### Oslo massacre – Surprise?

# **CBRNE-TERRORISM Newsletter** Volume 39 - 2011

Sensors printed on wetsuits detect explosives Chemical weapons terrorism on eBay Depleted uranium in Libya What next? A Sunni bomb? Bombs beneath the burga Obsession – the movie Nano detector spots deadly anthrax India to open Bio safety Level-4 lab Dangerous TB spreading at alarming rate in Europe Underwater nuke detecting drone Radiological Dispersal Device playbook A nightmare that could be worse than 9/11 RPG in a belly – an amazing story America's power grid too vulnerable to cyber attack

Stuxnet can morph into a new threat Qaeda's Zawahiri bigger threat than Osama?



EU terrorism situation and trend (EUROPOL) Norway: Lessons from a successful lone wolf attacker Piracy spreads to South New edition of Inspire America's next 12 terror threats Iran's Quds Force

AI



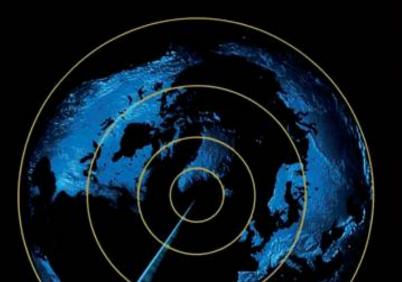
ISDS Headquarters Tel: 972-8-9227699 Fax: 972-8-9235104 P.O. Box 173, Nir Zvi, 72905, Israel ISDS@ISDS.co.il WWW.ISDS.co.il

#### ISDS offices around the world



Land and Sea Forces





ISDS is a multi-national security company with a global outlook.

Emergency units,

Government

institutions

Venues, Concerts, Delegations, and

Dignitaries

A worldwide influential, sophisticated security consultant and integrator in areas Such as Home land security (HLS), Defense, Maritime and Aviation security, Infrastructures, Multi-National Enterprises and the security of Mega-Events .

With a record of more than 27 years in planning, developing, integrating and operating large scale security projects in versatile environment, ISDS is a "one stop shop" for security projects of high complexity

Registered and certified by the Israeli M.O.D, and operates according to the Israeli M.O.D

#### Volume 39 (Autumn 2011)

Copyright© 2011

#### **Editor**

#### BG(ret'd) Ioannis Galatas, MD, MA(Terr), MC

Consultant in Allergy & Clinical Immunology Medical/Hospital CBRN Planner Senior Terrorism/WMD Analyst CBRN Scientific Coordinator @ RIEAS VC Greek Intelligence Studies Association (GISA) CEO CBRN Hydra Consultancy Athens, Greece Contact e-mail: igalatas@yahoo.com

#### **Associated Editor**

Panagiotis Stavrakakis Hellenic Navy Captain (ret'd) MEng, MBA, MSc PhD Student (Chemical Engineering School, NTUA)

#### **Co-Editors**

#### Steve Photiou, MD, MSc

Consultant in Internal Medicine & Emergency Medicine Senior Staff Member, Emergency Department. Ospedale Sant Antonio, ULSS 16, Padua, Italy EM/DM Alumni Association Treasurer. Chief, EuSEM Disaster Medicine Section

#### Nikolaos Kokkotas, MSc

Civil Protection Consultant Emergency Manager in General Secretariat of Civil Protection Athens, Greece

#### COVER

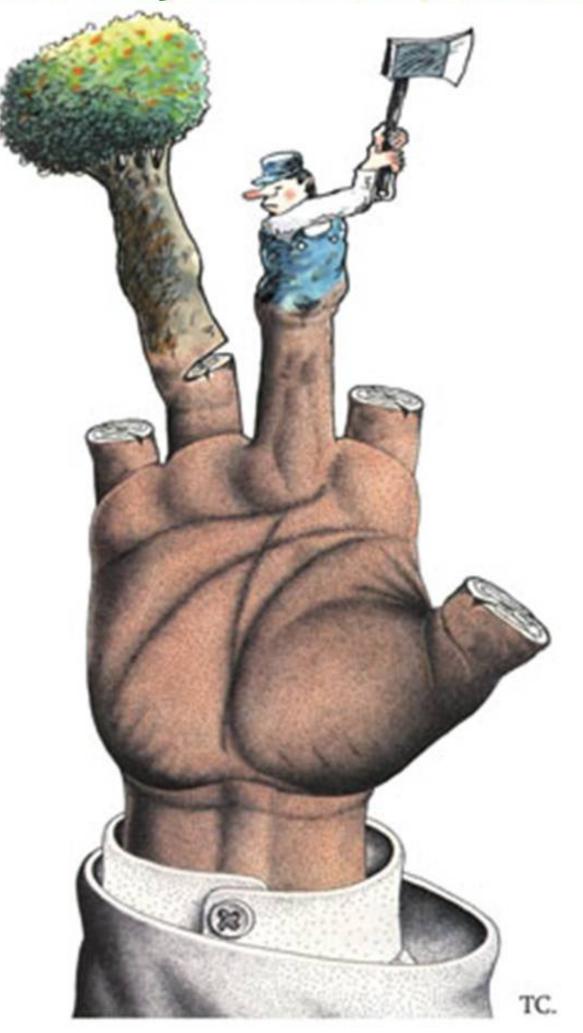
Dr. Ayman al-Zawahiri (top photo), Norway's massacre (bottom photo), Anders Behring Breivik (small insert)

#### DISCLAIMER

CBRNE-Terrorism Newsletter is a free on-line publication for the fellow civilian/military First Responders worldwide. The Newsletter is a collection of papers related to the stated thematology, relevant sources are provided and all info herein are solely from open Internet sources. Opinions expressed in original papers are those of the authors and do not necessarily reflect the mentality of the Editorial Group of the Newsletter.

2

# Climate change ... You are responsible too!



# Contents

#### **Reading Public**

• Who is reading the Newsletter

#### **Editor's Corner**

- Editorial
- Editor's choices

#### **Original Papers**

- Swiss CBRN protection goes national
- · Top ten reasons that hospitals are not prepared to evacuate in a large emergency
- Lessons from high reliability organizations
- Homegrown jihad in the United States

#### **Chem News**

- Two hood type NBC respirators
- Nanowire-based sensors detect volatile organic compounds
- Enzyme Might Hold Key to Countering Nerve Agents
- Directed evolution of hydrolases for prevention of G-type nerve agent intoxication
- WMD Central Five Years and Building
- · Sensors printed on wetsuits detect explosives, other hazards
- Natural enzyme can defend against terrorists' nerve agents
- School Safety Plans Must Include Terrorism Response Procedures
- New Multi-Threat Portable Gas-Detection Monitors Now Available Following Extensive Field Testing
- Chemical Weapons Terrorism on eBay
- US Department of Defense Contract Award for Avon Filters
- The Secret Behind NIST's New Gas Detector? Chirp Before Sniffing
- New chemical protection suit
- 1st Detect receives U.S. patent for chemical detector
- Libya: Securing Stockpiles Promotes Security
- Hospital Emergency Response Teams
- General Dynamics to integrate CBRN device in Army radios

#### **Bio News**

- Innovative duct tape strategy saves hospitals time, money; improves infection 173-222 prevention
- House introduces new biological weapons legislation
- Singapore Health Sciences Authority Approves Emergent BioSolutions Anthrax Vaccine, BioThrax
- New Discovery In Battle Against Plague And Bacterial Pneumonias
- How The Immune System Fights Back Against Anthrax Infections
- Nano detector spots deadly anthrax
- Natural antibody brings universal flu vaccine closer
- Satellites could predict next cholera outbreak
- Concerns over third outbreak of AIDS in Iran
- Global Bioterrorism Threat Analyzed For World Animal Health Office



12-120

121-142

143-172

- Protecting water utilities from terrorist attacks and contaminants
- Water purification unit generates its own energy
- Lung damage found in Iraq, Afghanistan veterans
- Engineering Innovative Hand-Held Lab-On-A-Chip Could Streamline Blood Testing Worldwide
- Portable detector can ID anthrax in one hour
- India to open Bio Safety Level-4 lab
- Five Joplin survivors die of mysterious fungal infection
- Gold nanoparticles help to diagnose flu in minutes
- CDC moves disease surveillance system to the cloud
- A natural food preservative kills food-borne bacteria
- · Innovative biosensor for rapid virus field tests
- Medical silver bullet: New drug cures most viral infections
- Qaeda Trying to Harness Toxin for Bombs, U.S. Officials Fear
- Software successfully predicted spread of West Nile virus in California
- How did H1N1 become an pandemic?
- Source of Haitian cholera outbreak identified
- Detecting bioterror attacks
- Experts anxious about appearance of a variant strain of Bird Flu
- How did the deadly plague bacterium develop?
- Hunting for a Mass Killer in Medieval Graveyards
- Anthrax-like Disease Caused by Bacillus cereus
- Dangerous TB spreading at alarming rate in Europe-WHO
- The Real Threat of 'Contagion'
- University lab focuses on deadly natural biological agents

#### **Dirty News**

- Flood waters threaten nuke plants along the Missouri River
- Jellyfish force Torness nuclear reactor shutdown
- Is NATO using dirty bombs in Libya?
- Depleted Uranium Found in Libya by Scientists
- Depleted uranium
- Gates and tactical nuclear weapons in Europe
- A Citizen's Radiation Dosimeter That Fits In The Wallet
- Strong reactions to assassination of another Iranian scientist
- China developing EMP weapons
- Funding To Develop Crystals For Detecting Nuclear Threats
- New radiation detector unveiled, does not rely on helium-3
- NYPD pioneers system to detect 'dirty bomb'
- Nuclear safety in Iran, post-Fukushima
- Swedish police arrest man for building nuclear reactor in his kitchen
- EMPACT America, Inc.
- Underwater nuke detecting drone
- Cheap radiation detector made of PET resin developed
- First quantitative measurements of Fukushima leakage
- What next: A Sunni bomb?
- A new way to detect secret nuclear tests: GPS
- Radiological Dispersal Device Playbook
- Iran runs nuclear missile payload tests, moves onto 60 pc fuel enrichment
- New materials hold promise for better detection of nuclear weapons
- Detecting contraband radioactive material



223-288

6

289-327

A Nightmare That Could Be Worse than 9/11

#### **Explosive News**

- Bomb-proof bag for planes' luggage compartment developed
- Militants may try bomb implants to attack
- Terrorists planning breast implant bombs
- TSA could begin searching for explosives hidden inside you
- Anti-Terror Sensor That Scans Crowds for Bombers Tested in U.K.
- Stand-Off Detection of Suicide Bombers and Mobile Subjects
- Terrorists in Drag: Bombs Beneath the Burga
- Roving robot can rescue people, detonate bombs
- Colombia rebels kill 2 police, set off "horse bomb"
- Beware of Dr. Jihad
- New software to improve explosive detection
- Animal kingdom's alternatives to full-body scanners
- Specialized Search Dog Add New Weapon to Fight
- Blast gauge gives medics, doctors critical information
- DHS slow to crack down on ammonium nitrate sales
- New device identifies unknown liquids instantly
- New material dramatically increases explosive force of weapons
- Sacramento Plastic Surgeon on the Possibility of Breast Implant Bombs
- Aussies to clone explosives sniffer dogs
- Marines deploy bomb-sniffing dog alternative
- Nanotechnologists Are Targets of Unabomber Copycat, Alarming Universities
- Bomb attack on beach in Antalya, Turkey: ten wounded in explosion
- Suicide Bombs In Iraq Caused 200 Coalition Soldier And 12,000 Civilian Casualties From 2003-10
- Suicide attacks—the rationale and consequences
- Taliban issue statement on use of child suicide bombers
- An amazing story
- Understanding the basics of IEDs
- Laser device detects IEDs

#### **Cyber News**

Study finds nearly 90 percent of businesses victim of cyber attacks

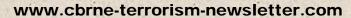
328-343

- · Google Ideas think tank gathering former extremists to battle radicalization
- Cybercrime statistics wildly inaccurate
- America's power grid too vulnerable to cyberattack, US report warns
- Detecting fake Web sites
- Al-Qaeda's cyber jihad on Facebook
- The top 10 Chinese cyber attacks (that we know of)
- Biggest-ever series of cyber attacks uncovered
- Stuxnet can morph into new threat
- Cyber Threat Resembles Pre-9/11 Terror Threat: Black Hat
- Why US Will Lose a Cyber War
- New Windows worm spreading by exploiting weak passwords
- Report warns U.S. unprepared for cyber attacks

#### **Terror News**

- Profile of Dr. Ayman al-Zawahiri, Osama bin Laden's Heir as Leader of Al-Qaeda1
- Al-Qaeda's Zawahiri, Bigger Threat Than Osama?

344-543



- Cash-Strapped Al Qaeda Turns to Kidnapping and Ransoms to Pay Operational Costs
- Somali Pirates Turn Violent
- Improved tracking system being developed for firefighters
- The al-Qaeda Crescent in Yemen
- Checkbook Jihad
- The United States and the Policy of Targeted Killing
- Israel drills for potential mass missile attacks
- Al-Qaeda and the Libyan Rebellion
- U.S. no longer mandating 100 percent screening of cargo containers
- Background Report on Suicide Attack on Intercontinental Hotel in Kabul, Afghanistan
- Taliban Hotel Attack: Low Death Toll, High Psychological Value
- The Seattle Plot: Jihadists Shifting Away From Civilian Targets?
- Questions arise surrounding the assassination of Ilyas Kashmiri
- Money, men in short supply to execute Al Qaeda's terror plans
- The Brutal Mind of Al-Qaeda's New Boss
- Belgium: Muslim extremists moving to the suburbs
- Russian Navy captures Somali pirates
- ICE lists Israel among countries that promote, produce, or protect terrorists
- Germany says Islamic terrorism still a threat
- Somali Piracy becoming an industry
- EUROPOL: TE-SAT 2011 EU Terrorism Situation and Trend Report
- Is Al Qaeda Planning Terrorist Attack on AeroVironment Inc? Here's the L.A. County Firm's 5 Coolest Spy Drones
- Al-Qaeda's Egyptian Ideologues Planning Caliphate's Return to Egypt
- Google Earth is Used by Terrorists
- Dewsbury, Bradford and Tower Hamlets ... where Islamic extremists want to establish independent states with sharia law
- Exploring Memories Of The London Bombing
- The Dog That Cornered Osama Bin Laden
- Trends in Global Violence and Norway's Peace Diplomacy
- EU: Jihadist calls for tourist Jihad
- The Third Jihad
- Norway's Terrorism in Context
- Norway: Lessons from a Successful Lone Wolf Attacker
- The Oslo massacre in pictures
- The 'Lone Wolf' Disconnect
- The Wide-Ranging Psychological Impacts Of The 9/11 Tragedy 10 Years Later
- The Killing Of Bin Laden Worsened Americans' Views Of US Muslims
- DHS unveils new Maritime security strategy
- Growing problem in Canada: stolen passports
- Full-body scanning for the shy
- Computational Models And Algorithms Cast Fresh Light On Terrorism In India
- Gaping Holes in Intelligence on Overseas Terrorists
- Securing critical infrastructure: portfolio based approach
- Getting Bin Laden
- A Portrait of Abu Bakr bin Abdul Aziz al-Athri: Salafi-Jihad's Emerging Internet Ideologue
- Al-Qaeda Uses Pakistani Intelligence Course to Train International Operatives
- Sovereign Citizens: A Homegrown Threat?
- Piracy Spreads to the South
- Mumbai Outraged Once Again: India Blinks, Blames Homegrown Terror



7

- Report warns Amtrak vulnerable
- Newly formed South Sudan joins Somalia, Pakistan, Iraq and Afghanistan at top of Maplecroft terrorism ranking – attacks up 15% globally
- Fighting Grassroots Terrorism: How Local Vigilance Can Help
- "Christian Terrorism"?
- Haqqani Network Growing Stronger at the Expense of the Tehrik-e-Taliban
- France: 100-150 mosques in progress
- Mumbai bombings tied to homegrown group
- Conspiracy of fire The Globalization Of Anarcho-Terrorism
- SAS scouts shopping centres as fears of London 2012 terror attack grow
- How to Forecast and Preempt al-Qaeda's Catastrophic Terrorist Warfare
- Piracy's Emerging Market: The Gulf of Guinea
- How Jihad Influenced the Norway Massacre
- Fort Hood Plots: Answering the Call of Individual Jihad
- Obsession The movie
- Bin Laden movie has King worried
- 10 Years and a Diagnosis Later, 9/11 Demons Haunt Thousands
- Indonesia's "Ghost Birds" Tackle Islamist Terrorists: A Profile of Densus 88
- Contemporary Maritime Piracy
- Counterstrike: The Untold Story Of America's Secret Campaign Against Al Qaeda
- How to Hijack an Airplane in 3 Seconds
- Has Al-Qaeda Opened A New Chapter In The Sinai Peninsula?
- Egypt's 5,000 troops take on 2,000 al Qaeda in Sinai
- Innovative disaster communication tech developed
- The Lone Wolf Jihad
- Implication of the Negev terrorist incident
- Attacks in Israel and New Militant Opportunities in Egypt
- New training facility features simulated bus, air, and rail stations
- An Emerging Threat: Al-Qaeda In The Sinai Peninsula
- Iran's Quds Force: Supporting Terrorism Worldwide
- Beyond Bin Laden: Global Terrorism Scenarios
- Why AI Qaeda is Unlikely to Execute Another 9/11
- NEW Edition of Inspire
- Study finds Somali piracy could cost global economy \$12 billion
- 1000 potential terrorists in Germany
- Jihadists in Syria: Myth or Reality?
- Inside the world of piracy
- Combating the financing of terrorism
- Parking attendants part of U.S. anti-terrorism effort
- America's Next 12 Terror Threats
- 9/11 legacy: more resilient skyscrapers
- The Evolution of a Pakistani Militant Network
- SGT. Dakota L. Meyer, USMC Medal of honor
- Hamas May Resume Suicide Bombings
- India has its own indigenous Islamist terrorist threat: US report
- Indians urged to buy terrorism insurance
- St. Andrews University promotes its certificate in terrorism studies

#### **New Upcoming Events**

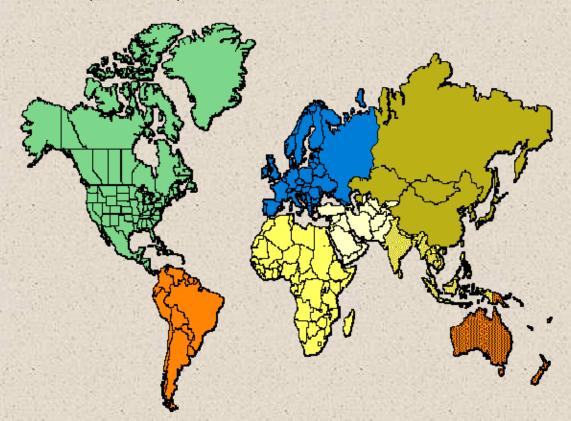
• 2011 - Conferences, workshops, training



8

# Reading Audience

Our reading audience comes from **65** countries all over the world and is constantly expanding. Currently colleagues and affiliates from **over 700** organizations, companies, institutions, ministries and the first responders are recipients of CBRNE-Terrorism Newsletter.



#### Europe

Greece – The Netherlands – Cyprus – Serbia – Romania – Slovak Republic – Monaco – Iceland – Sweden – Finland – Norway – Croatia – Italy – Belgium – Denmark – Switzerland – Estonia – Luxemburg – Germany – Austria – France – Portugal – Bulgaria – Spain – Poland – United Kingdom

#### Africa

South Africa - Kenya - Burundi - Nigeria

#### **Middle East**

Israel - Jordan - UAE - Saudi Arabia - Qatar - Kuwait - Bahrain - Oman - Iran - Iraq

#### Asia

Turkey – Russian Federation – India – Japan – China – Pakistan – Afghanistan – Azerbaijan – Singapore – Philippines – Malaysia – Indonesia – Uzbekistan – South Korea – Mongolia – Ukraine – Taiwan



### Oceania

Australia – New Zealand

#### North America United States of America – Canada

South America Argentina – Brazil – Peru – Colombia – Mexico – Trinidad & Tabaco

#### **CBRNE-Terrorism Newsletter Website's Follow-up**



#### Our Top-10 Visitors are coming from:

1	United States	6	Germany (new place)
2	Greece	7	Italy (new place)
3	United Kingdom	8	Canada
4	India (Эnew entry)	9	Belgium (Эnew entry)
5	The Netherlands	10	Switzerland
1 2 M 1 1 1 1 1 1 1	a find the same set that the same		Carl Provide State of the State





# Editor's Corner

#### **Editorial**

Dear Colleagues,

I hope you all enjoyed your summer holidays and fill your batteries for a difficult as always winter. The Norway Massacre upset the sleeping minds of our societies and reminded us once more that the uncexpected always happens! Then it was the enormous explosion at the naval base of Cyprus' armed forces that costed also lives and had big impact on strategic infrastructures on the island. This event was not very unexpected since it was there shouting that something will happen sooner or later but nobody was listening... And of course it is the coming anniversary of the 911 catastrophe that changed the world they way we used to know it.

Instead of writing my own thoughts about what happened in the years after the 9<sup>th</sup> of September 2001, I borrowed those of a US colleague who has better knowledge than me in this matter. Here is what he writes (source: www.abetteremergency.com):

"In light of the tenth year anniversary of the terror attacks of September 11, 2001 I thought it fitting to take a look at contributing factors leading up to that day and stimulate some discussion on how far we have or have not come to mitigate and respond to a similar attack.

According to the 9/11 Commission Report, they concluded the attacks revealed four kinds of failures on our part; in imagination, policy, capabilities and management.

Imagination – Imagination is not a gift associated with bureaucracies. If a contributing factor in the success of the attacks was the inability of our massive government machinery to fathom the threat from a band of tribal zealots in the mountains of Afghanistan, why would we conclude that the answer would be create an entirely new layer of bureaucracy called the Department of Homeland Security?

Policy – The existing mechanisms for handling terrorist attacks had been trial and punishment. The Actions of al Qaeda fit neither category. Our existing policy proved ineffective when we found the threat had no territory, citizens or assets that could be readily threatened, overwhelmed or destroyed. (Also a testament to lack of imagination within our bureaucracies) We knew the Taliban offered al Qaeda sanctuary in Afghanistan and the United States warned the Taliban in 1998, again late in 1999, once more in the fall of 2000 and in the summer of 2001 that they would be held responsible for further attacks by Bin Ladin on U.S. interests. Repeating a warning does not work raising children and obviously was a poor strategy against al Qaeda. It was concluded that killing Bin Ladin would have an impact on al Qaeda, but not stop the threat. The best option would be to end the Taliban's offer of Afghanistan as a base of operations for al Qaeda. Taking this type of military action against al Qaeda at this point was deemed disproportionate to the threat, especially in light of challenging domestic issues within the United States. If policy makers were distracted September 11, 2001 from making hard decisions, we can conclude the folly we witnessed in dealing with the financial security of the United States means they are similarly distracted today.

Capabilities – Government agencies sometimes display a tendency to match capabilities to mission by defining away the hardest part of their job. Identifying and trying to fix obvious (if imagination is encouraged) threats that are viewed as costly, controversial or disruptive are not wise to career longevity.



Management – Information was not shared, sometimes inadvertently and sometimes due to legal misunderstandings or lost in the divide between foreign and domestic agencies; analysis not pooled and effective operations not launched are symptoms of the government's inability to adapt how it manages new challenges of the 21st century. Imagine you check into a hospital for a bypass operation. You are surrounded by technology, extremely intelligent, skilled and well-meaning professionals that all understand how to do their piece of ensuring your stay goes well but the one piece missing is the attending physician to oversee your care. Think back to recent exercises you have attended with various branches of federal government; did they all seem to cooperate and work like a team to achieve the goal established by command?

I would like to think our preparedness has progressed over the last ten years, certainly we have seen huge sums of money spent, massive bureaucracies created, seen tons of toothpaste and other liquids and gels seized at airports and witnessed the best of our military and they have paid a precious price for all of us. My conclusion is that the old adage is true, all response is local and New York came up with the best terrorist disruption strategy with their if you see something say something campaign. I am curious if you think we are better off than we were ten years ago."

I think that we all agree with his thoughts and it is obvious that there are so many things to be done in all sectors of counterterrorism. What I would like to add is that medical/hospital CBRNE preparedness is still lacking the appropriate attention from state authorities worldwide. Officials in high places must realize that spending all that money for "Golden Hour" will not prevent a CBRNE terrorist attack while medical consequences of WMD agents' release will last for months and years. Following the triple catastrophe in Japan, no-one has the right to say that CBRNE threat is science fiction. What if it happens in your city or in your countrly?

Following a small poll at the website hosting the Newsletter, there was a majority request to change from quarterly to bi-monthly edition. There is no objection from our side since we understand that news should always be as fresh as possible. We will do that from the beginning of 2012. An alternative migh be to create a parallel blog where there will be daily information about what is happening in the CBRNE world around the globe and then put all these news in a .pdf format every two months for those not able to follow us on daily basis.

In this issue we are kind of short out of original papers – mostly due to summer activities of our reading audience. I always thought that summer is a good opportunity for writing – but we do not all share similar thoughts! Same applies for advertising – in that respect we reduced prices even more and if this does not work we will continue to incorporate ads from other sources as part of your information process. We stress once more that ads' money is not for profit but for expanding our activities in the area of CBRNE operations – i.e. conferences, visits, participation in forums etc.

From the above you realize that CBRNE-Terrorism issues are kind of a "passion" for us and not a main stream profession for profit. Even if the ads will not work out well, we will continue to edit the Newsletter even in its previous amateuristic format because it is the content that matters not how the whole thing looks like! It is self-evident that your remarks, comments and suggestions are more than welcomed and will be highly appreciated and incorporated in future issues!

Enjoy the CBRNE-Terrorism Newsletter and if you really like it, please feel free to pass it over to colleagues in your networks!

7he Editor

BG(ret) Ioannis Galatas, MD, MA, MC



#### **Islam in Greece**

By Ioannis Michaletos Source: http://www.drougos.gr/

#### Points of interest

Greece is an EU, NATO and Eurozone country which has traditionally strong links with the Islamic world due to the geographical proximity with the Middle East and North Africa and the Ottoman rule that lasted four centuries, along with numerous historical encounters with Islam since the Middle Ages.

Presently, the country hosts a Muslim minority which is a reminiscent of the Ottoman Empire, but also an expanding Islamic population from the Arab countries and Pakistan that enter Greece in significant numbers as illegal immigrants.Moreover, large corporations in the country, such as banking institutions, tourist companies and real estate ones are in control of Islamic funds, whereas countries such as Egypt, Saudi Arabia, Iran, Turkey and Libya, can be considered as significant trade partners of Greece.

In Athens Greece, the Iranian Saderat bank is hosted (1), which is a U.S black-listed institution due to alleged links with Hezbollah (2). Iran covers 25% of Greece's oil needs per annum and some 15% of its natural gas needs. Furthermore, there are indications that Hezbollah groups are operating in a logistic support basis in Athens by gathering funds through tobacco contraband over the past years (3).

In a broad sense, Greece due to a mixture of its geographical placement, history and business links, is considered as a gate-away for the Islamic element towards the EU and the Balkans and over the past 10 years it has become one of the main transit territories for Islamic-originating illegal immigration to Europe.

Until now Greece does not seem to have a particular issue of Islamic fundamentalism. Nevertheless as aptly described in a U.S State Department report on terrorism, "Greece is increasingly an EU entry point for illegal immigrants coming from the Middle East and South Asia and there was concern that it could be used as a transit route for terrorists travelling to Europe and the United States. The number of illegal immigrants entering Greece, especially through the Aegean Sea, increased dramatically in 2008 and 2009, with more than 100,000 illegal immigrants, nearly half of whom originated from North Africa, the Middle East, and South Asia, arrested each year" (4).

#### Islamist activity in Greece

Presently in Greece, there seems to be an activity within radical Islamic elements, as well as, gradual projection of Islamic political entities through the use of Greek nationals.

A revelation by the infamous Wiki Leaks US Dept of State telegrams, showed that, the ex-Ambassador of US in Athens, Mr. Daniel Speckhard, has noted the danger of the nexus between Greek domestic terrorist groups and Islamic groups, including those from Iran, as he was informed by the then Greek Minister of public Order, Mr. Chrysohoidis (5).

Furthermore, in a special report by the French daily "Le Figaro", on the 21st of December 2010, the case of the route of Islamic terrorists from Lebanon to Europe was noted with significant details (6).

The article titled "Liban-une filiere djihadiste vers l'Europe", clearly illustrated the perils involved for Greece as well. More specifically, the Lebanese Army Cornell Mahmoud Issa noted to the French journalists that since November 2010, some 20 extremists managed to escape from a camp where they were kept in Lebanon and found their way to the EU.

He stated that already the authorities were notified in an international level, although he admitted that this is a difficult task. From their part, the French security authorities believe that this is the case of a new Jihad mission heading towards European metropolises.

In classified documents that were in possession of radical groups in Lebanon, it was noted, that the individuals named: Karoum Imad Youssef, Ahmad Kayed and Sidawa, managed to leave the camp previously and through Syria and Turkey ventured up to Greece and Bulgaria with the assistance of illegal immigrant transport networks managed by Turks.

Moreover they managed to acquire fake ID's and they were finally caught by a common operation of the Bulgarian and Greek authorities. That case according to many reliable sources was closely monitored by the

British and French intelligence, due to the fact that these two countries was the ultimate destination of the Lebanese group. Mahmoud Issa, stated that more cases are to be found that evade the authorities so far. In the article Greece is mentioned as a traverse region from where potential terrorists travel on their way to other EU countries.

French intelligence sources dating back to the pre-9/11 period claimed that organized networks of radical Arab groups that have operated in Greece in the past have been used by al-Qaeda affiliates and other fundamentalist networks (7).

According to a pre-9/11 French intelligence report, American interests in Greece and Cyprus were considered by Osama bin Laden's network as targets. Citing a DGSE document, the newspaper "To Vima", reported that members of the bin Laden network in cooperation with Taliban officials and other armed groups were planning to hijack airplanes between March and September 2000, yet it was never carried out due to various logistical and operational disagreements (8).

In another notable case, in September 2005, the Moroccan Anwar Mazrar was arrested on the Greek-Turkey border while attempting to travel to Greece on the Istanbul-Thessalonica bus service . Mazrar had been accused of being a leading member of terrorist groups in Morocco and also of having ties with al-Qaeda (10).

European intelligence agencies have also reported that around 20 Arab fundamentalists have been arrested in Britain, Italy, Portugal, France and the Netherlands for having in their possession forged Greek passports (11).

Various intelligence sources conclude that the Greek immigration policy has deterred many radical Islamist networks from establishing permanent ties in the country. A security brief issued during the 2004 Olympic Games noted, "The legal environment was for many years an obstacle for the growth and development of organized networks that could operate overtly or covertly using religious and cultural organizations and NGOs as legitimate fronts." This policy, however, unintentionally leads many groups to go underground.

The Greek secret service has mapped a transnational network of radicals that has been developing in Greece over the years. Field informants indicate that this semi-legal web

spreads across five different communities, including:

Mosques and local Muslim communities

Humanitarian organizations and NGOs

Islamic cultural centres in Europe

• Foreign political, economic and religious elites

International Islamist terrorist organizations

The key members of this network (referred to as "The Union of Mosques" or "The Union of Imams") have military training and combat experience and are well connected with terrorist groups, foreign governments and the Muslim Diaspora in Europe (mainly in Britain, Italy and France). They use criminal activities to finance and facilitate their ideological objectives. The most noticeable illegal activities they conduct are passport forging, arms trafficking, people smuggling and drug trafficking. Finally, according to the same sources, the network has developed an internal structure to support fundraising, recruitment and counter intelligence activities (12).

Greece's rather recent encounter with domestic radical activities is getting stronger, as the data show regarding the spread of Islamic-driven NGO's and charity groups.

Al Jabbar, is a Islamic charity NGO active in Greece over the past five years. According to information of high value, the organization possesses funds in excess of 400,000 Euros and it is actively launching campaign for the raise of another 150,000 Euros in the near term. Furthermore, it has spent 550,000 Euros, in 2008 in order to buy a building in the Aeschilus Street, number 37 in the centre of Athens. In the nearby streets, over the past 24 months, there has been a notable increase of houses being bought by Pakistani nationals who pay in cash, although they tend not to reside there or open up businesses. Further, an undisclosed amount of capital, which is estimated at over 2 million Euros was invested between 2007-2009 for the construction of a "Islamic cultural centre" in the district of Moschato in Athens, by Al Jabbar, although details are in flux regarding the actual involvement. A Saudi financier was also involved into assisting this project. The organization claims unofficially to have as much as 45,000 members, although reliable information point out that the actual membership is a few hundred people. The vast majority of its members is illegally residing in Greece and is of Pakistani descent, although

the top members come from the Arab countries. There are no data, if there has been a thorough vetting process by the authorities regarding the transfer of these funds or if they derive from legal and taxed charity work. By taking into account the present state of affairs in the Islamic communities in Athens, there are strong indications that the capital was transferred from Arab countries. The AI Jabbar NGO is highly secretive; its members take measures as not to appear in public or have any kind of pubic contact with governmental authorities or the media (13).

Lastly, a case of interest was the arrest in 2009 of the Iraqi citizen named Abu Sanjad. In this case he was arrested in Athens in July 2009, and he was subsequently sent to Irbil-Iraq, when his identity as a wanted terrorist by the Iraqi government was established. He entered the country, as an illegal immigrant (14).

#### **Islamism and Society**

Estimates of the recognized Muslim minority, which is mostly located in Thrace, range from 98,000 to 140,000 (between 0.9% and 1.2%), while the immigrant Muslim community numbers between 200,000 and 300,000. Albanian immigrants to Greece are usually associated with the Muslim faith, although most are secular in orientation (15).

Greece's Muslim minority is to be found in Western Thrace, the province neighbouring with Bulgaria and Turkey. The first Muslim coming from Anatolia, settled there in 1363 along with the Ottoman Turks in the first European conquest endeavour.

In 1923 Greece and Turkey agreed to a mass exchange of populations and consequently Greeks resettled from Minor Asia to mainland Greece and vice versa (16). The Muslim minority in Thrace along with the Greek-Orthodox in Istanbul remained as a counterweight to its other and as a symbolic remembrance of the oldest Muslim settlement in Europe and the historical Byzantine -Christian presence in the East respectively.

The course of events though revealed a systematic extinction of the Greek-Orthodox Christians in Istanbul that number some 5,000 people down from 200,000 in the 1920's (17). In Western Thrace around 110,000 Muslims reside -45% Turks, 40% Pomaks, 15% Roma-, and constitute about 1% of the total population in Greece and a Quarter of the Western Thracian populous. The strategic importance of

the region has often attracted Turkish attention that the Greek government is accusing of sporadically trying to inflame nationalistic or religious divisions between the Muslim citizens and the Christian ones (18).

A major aspect into examining the present state of affairs in Greece regarding the Islamic element in the country is the influx of illegal immigration, which comes almost exclusively through Turkey.

Tens of thousands of illegal immigrants from the Middle East see Greece as their destination or point of entry into the EU. Only in 2010, their number was 128,000, the highest in all EU member states (19).

Moreover, Turkey does not maintain visa regime with Iran (20) and other Middle Eastern countries, thus promoting in effect the movement of Afghans and Pakistanis, as well as, Iranians into Europe.

The immigrants from the African countries (Somalia,Nigeria) travel to Smyrna, Istanbul and Mersina through vessels crossing the Mediterranean Sea, whilst Arabs come mostly through the Syrian-Turkish borders. The Asians (Pakistani, Bangladeshi, Kurds, and Afghani) pass through the Iranian-Turkish borders and it has to be noted that both countries do not have a visa regime, although Teheran is accused by the world community as a sponsor of terrorism. Therefore the flow of people from Iran to Turkey is in fact unconstrained and there has not been pressure to Ankara to alter this state of affairs with its neighbour.

Istanbul in particular is the undisputable centre where masses of illegal immigrants concentrate before they are transported to the West. In the Vefa neighborhood right beside the Süleymaniye Mosque, the Iraqi-Kurdish immigrants gather.

In the Laleli area the most immigrants come from the Caucasus. In the Aksaray and the Beyazit Meydani regions there are people from all corners of earth pilled in cheap hotels and in the Tarlabasi, African immigrants. In a city of almost 17 million people, it is roughly estimated that between 250,000 & 500,000 of those are illegally residing and waiting mainly to find a way reallocating towards Europe through Greece (21).

The first official mosque—officially named as: the Greek-Arabic educational and cultural centre—began operating in Athens in June 2007 following fierce opposition by political parties and the general public. The Saudic

sponsored mosque can accommodate more than 1,000 religious followers. The new mosque—which officially operates as a licensed cultural centre and school for Arabic language—was financed by the Saudi businessman El Faouza. The Egyptian imam, Omar Abde Kafi, was invited to be present at the opening of the mosque (22).

The Muslim Association of Greece (MAG) was founded in 2003 (23) . The MAG claims to represent all Muslims living in Greece. President of the MAG is Naim El-Ghandour an Egyptian born Muslim who lives in Greece since the early 1970s and has acquired Greek citizenship (24). His wife Anna Stamou a Greek convert to Islam is a member of the board of advisors of the MAG (25). She was also administrator of the islamfriends.gr website. Currently (March 2011), she is responsible for the MAG's public relations and she also works for the greeksrethink.com website (in Greek language) which appeals to Greek converts to Islam all over the world.

Another important member of the board of advisors of the MAG is Iman Sotiria Kouvali a Greek-Canadian convert to Islam (26). She was founder of the greeksrethink.com website and she is adviser for strategic planning for the MAG. MAG's official 'educational' website is ora-islam.gr. This website was created in early 2010 and seeks to spread knowledge about Islam in Greek language.

The website islam.gr has as an administrator who is Shadi Ayoubi, a Lebanese journalist and correspondent of the Al Jazeera media empire in Athens (27).

The Greek-Arabic Cultural Centre is situated in Athens (Moshato area). The Greek-Arabic Cultural Centre, better known as the Islamic Cultural Centre of Athens, was founded in 2001 in the Athens area of Ambelokipi and was relocated in 2007 in Moshato, an area close to Piraeus port. In December 2006 a Saudi businessman named Al-Fauzan bought an old textile factory building at the price of 2.5 million euros, in order to host the Greek-Arabic Cultural Centre. The building of 1,800 m2 also provides a place where Muslims can pray and serves as an informal mosque (28). The new building has a capacity to host 3,000 believers. The Greek-Arabic Cultural Centre is a member organization of the Federation of Islamic Organizations in Europe (FIOE) (29).

The main Dawah activity in Athens is coordinated by the Association named "El-

Rahman" which runs the islamforgreeks.org website (30). The association allegedly numbers 1,500 members (Real numbers of active members much less), mainly Greek converts to Islam. The founder and President of the association is Mohi Eldin Ahmed Ali. However, the brain of the association is his son Ahmed Eldin who serves as vice-president. Ahmed Eldin studied Islamic Theology in Cairo-Egypt as well as public relations and journalism in a private college.

In early February 2011 two Greek converts to Islam (Abu Jassir and Hamza) who are following the Salafi-Wahhabi strand of Islam joined Ahmed Eldin in the islamforgreeks.org website. Abu Jassir and Hamza, (before joining Ahmed Eldin), in partnership with Abu Alia another Greek convert to Islam were propagating the Wahhabi strand of Islam via the YouTube (31). Moreover, Abu Alia according to a report from Radio Free Europe was also actively propagating Wahhabi Islam in the Balkans. An international Wahhabi organization named "Poziv u Raj" (Invitation to Heaven) has launched a campaign in Bosnia-Herzegovina (March 2010) calling on non-Muslims to convert to Islam (32).

In overall, Greece and especially Athens, already hosts a number of Islamic organizations, which can be classified as NGO's and immigrant-support groups. They tend to keep a low profile and most of them do not retain a website or make their details publicly available (33).

#### Islamism and the State

Due to the fact that the majority of the Islamic population in Greece and especially the radicalized part of them are mainly interested into establishing themselves on a permanent basis in Western and Northern Europe, the situation is deemed as controllable by the local authorities, something that cannot be guaranteed in the long-term

Since late 2008, there have been three major cases that show the tendency of creating a rising network of a quasi-radical Islamic element in the Greek society. The first was in the December 2008 riots (34), were a large number of the people arrested were Pakistanis and Afghanis, some of them claiming to the authorities that were paid in order to participate in the violent demonstrations (35).

The second development was the May 2009 so-called "Koran demonstrations" (36), when a.

16

multicultural group of various Islamic communities in Athens took to the street allegedly claiming that the Police desecrated the Koran during a routine search in the pockets of a Syria street contraband vendor (37).

Bus stops, 5 shops, one bank and 57 cars, where smashed in and the city centre's main squares and streets were turned into battle zones for hours. 46 immigrants were arrested, 7 immigrants and 7 police officers were wounded during the clashes (38).

It was later revealed that this particular individual was lying to the authorities and the press and was involved in various illegal actions including armed robberies (39).

A third phase was the mass prayer of thousands of Muslims in the centre of Athens in October 2010, without attaining the necessary state permission for that (40). Amongst the organizers they were individuals associated with the Muslim Brotherhood and an Imam was brought by Egypt to commemorate the ending of the Ramadan.

Small-scale riots started the next few days when they were again false allegations for Koran desecration by the Greek police in the centre of the city (41). It was again proved to be false, but it is more than obvious that a "street mechanism" is being established in the country that facilitates the mobilization of a few hundred "angry Muslims", and the spread of these kind of news to the media through the use of Greek intermediates along with the umbrella of NGO's that operate by spending considerable amounts of capital (42).

In 2005, the "Pakistani abduction case," took place, in which 28 Pakistani immigrants were allegedly kidnapped by intelligence agents in Athens (43). That case was connected to the cooperation between the Greek and UK authorities following the July 2005 bombings in London, but was also the first notable case of accusation of the Greek state by Islamic organizations that Greece is actively turning against the Islamic element and takes harsh measures in the "war against terror". The Greek weekly newspaper, "Proto Thema" also disclosed the names of 15 alleged Greek agents and an MI6 spy chief allegedly involved with kidnapping and torturing the Pakistanis eight days after the London bombings of July 7, 2005 (44). There was widespread support by leftist groups mostly that demanded through a series of legal actions and demonstrations the

punishment of the Greek and UK security members involved.

In another case, which was the devastating wildfires in Greece in the summer of 2007 (45), a report, citing US intelligence channels, claimed that an Arabic-language jihad website has urged Muslims in Europe, America and Australia to use arson as a tool of terror. The website apparently cited imprisoned Al Qaeda "theorist" Abu Musab Al-Suri as the ideological progenitor of this plan. While Greece is not specified among the countries to be attacked, and while it is not a contributor of troops to the US-led coalition in Iraq, it has been vital to the war effort by allowing the Americans access to its island bases, transport and other logistical services (46).

Further evidence attests to a possible connection between Islamists and the forest fires in Greece. A type of improvised explosive device used in setting off the fires was ignited with a mobile phone (47). By calling the phone's number, the device exploded, sparking a blaze that soon grew out of control. The advantage for the perpetrators is that this result can be achieved from a safe distance- even from abroad. Significantly, it is similar to one of the methods used in the Madrid bombing in March 2003 and frequently used in IED's in Iraq and Afghanistan.

Further, a ranking Greek intelligence officer that spoke on the condition of anonymity stated that during the height of the summer fires a Saudi national equipped with such a device was arrested by Greek border police in the north of Greece, in the company of several Kosovo Albanians. It is no secret that the latter consider Greeks to be an enemy, in light of the latter's historic support for the Serbian point of view regarding the Kosovo issue. Nevertheless, there is evidence, some of it gathered in an August 2007 Jamestown Foundation report, of Greece being used as a transit zone and even potential target for al Qaeda and related groups (48).

The Greek state authorities have numerously in the recent past, been called upon, to investigate potential Islamic terrorist activity in the country. A warning from Serb intelligence about the mobilization of an extremist Islamic organization in Greece has put the Greek authorities on high alert in 2007. The Serb intelligence briefed a Serb parliamentary Committee that a group of extremists Islamists who are part of the Islamist organization Selar.

have become active near Serbia's southern border.

"There is no organized Salaf camp in Greece," claimed an EYP [Greek National Intelligence Service] official responsible for preventing the mobilization of Islamic organizations domestically. Greece, he revealed, "has been used as a crossing for terrorists headed either for the West for the former Eastern Bloc. We also have information that Greece has been used to support Islamic terrorist networks" (49). In 2005, immediately after the capture of Anwar Mazrar, who was linked to Al-Qaeda, Europol asked Greece to intensify its investigations into the potential activities of Muslim extremists. As a result, dozens of them, the majority from Pakistan and North African countries, were placed under continuous surveillance. Sources report the authorities are focusing on two North African imams suspected of membership in extremist Islamist organizations in Algeria. Furthermore, US, British, Italian and French intelligence have informed the Greek authorities that members of extremist Islamic terrorist organizations have used Greece as a "support country" (50).

Towards the end of 2010, various press reports, claimed that radical Islamic action was increasing in the centre of Athens and the issue became widely publicised after it was brought to the Parliament via the LAOS political party that demanded state explanations upon the issue and the proper notification of the security forces (51).

About 290 mosques operate in Western Thrace and on the islands of Rhodes and Kos. The only Muslim cemeteries are in Western Thrace. Although they formally have the right to use municipal cemeteries, this practice is reportedly discouraged, and few have done so. A Muslim cemetery is being developed currently in the outskirts of down town Athens. The Greek Orthodox Church has also donated 300,000 square feet (28,000 m2), worth an estimated \$20 million, in west Athens for the purpose of a Muslim cemetery (52). The Greek state pledged it will provide 15 million Euros for the construction of the Mosque.

Generally, Muslims in Greece must pursue burials either in Thrace or other countries. The Treaty of Lausanne also provides powers over some aspects of civil law to muftis in Thrace. These provisions have been respected by the Greek government (53).

Moreover, there are various evidence that around 120 non-classified or known officially to the authorities, Mosques operate in Athens (54). According to sources of the Greek daily "Kathimerini" newspaper, the number of unofficial mosques operating in Greece are 75 unofficial mosques (compared to 68 in June 2009), 23 of which have been founded by Pakistani and 15 by Bangladeshi immigrants. According to the same newspaper there are indications that the number of Muslim extremists reaching Greece through illegal immigration is also increasing (55).

The Greek state, with the Law 3512 of 2006, agreed for the construction of an "Official Mosque" near the city centre. According to the legislation, the Mosque will be classified as an entity administered by a seven-member board that will be composed by state, municipal officials and representatives of the Muslim communities, residing legally in the country. The Mosque has not yet to be constructed due to a variety of bureaucratic, political and social reasons (56).

#### Notes:

1) in.bsi.ir/Greece/default.bsi

2)http://news.bbc.co.uk/2/hi/business/5329326.stm

3)"Transnational Threats", Edited by Kimberley L. Thachuk, Page 92, Praeger Security International, London, 2007

4)http://www.state.gov/s/ct/rls/crt/2009/140885.htm

5)http://www.tovima.gr/politics/article/?aid=377454 (To Vima daily newspaper : Wikileaks revelations for Greek security", 11th of January 2011)

6)http://www.lefigaro.fr/international/2010/12/21/01003-20101221ARTFIG00563-liban-une-filierediihadiste-vers-l-europe.php

7) Greek weekly newspaper "To Vima, April 22, 2007

8)http://www.jamestown.org/single/?no\_cache=1&tx\_ttnews%5Btt\_news%5D=4347

9)http://www.iss.org.za/pgcontent.php?UID=19716

10)Greek daily newspaper, "Ta Nea", May 15, 2007



11)Ibid.

12)Jamestown Foundation, Islamist Terrorism in Europe: Could Greece Be Next? 4 October 2010, by Panos Kostakos, Terrorism Monitor Volume: 8 Issue: 37, available at: http://www.unhcr.org/refworld/docid/4caabf092.html

13)"Terrorism & Organized Crime Database" service, by the faculty of Security Studies of the University of Belgrade and the George C. Marshall Center for Security Studies, accessed at 19th of March 2011 14)http://news.kathimerini.gr/4dcgi/\_w\_articles\_politics\_100056\_20/03/2011\_436444 (Kathimerini daily newspaper : "Illegal immigration & terrorism; revelations of the Greek Wikileaks", 20th of March 2011) 15)http://www.state.gov/g/drl/rls/irf/2006/71383.htm

16)http://www.hri.org/docs/straits/exchange.html

17)http://www.answers.com/topic/greeks-in-turkey

18)http://www.unhcr.org/refworld/country,,,CHRON,GRC,,469f3890c,0.html

19)http://www.novinite.com/view\_news.php?id=126456

20)http://www.nytimes.com/2010/06/13/world/middleeast/13turkey.html?\_r=1

21) http://www.worldsecuritynetwork.com/showArticle3.cfm?article\_id=17798

22) Greek daily newspaper, "Eleftherotypia", May 15, 2007

23)http://www.equalsociety.com/

24)http://www.setimes.com/cocoon/setimes/xhtml/en\_GB/features/setimes/articles/2011/01/03/reportag e-01

25)http://www.greeksrethink.com/tag/anna-stamou/

26)http://www.greeksrethink.com/tag/iman-sotiria-kouvalis/

27)http://news.kathimerini.gr/4dcgi/\_w\_articles\_ell\_100062\_13/09/2008\_284648 (Kathimerini daily newspaper :The unknown Islam in a webpage in Greek", 13th of September 2008)

28)http://archive.enet.gr/online/online\_text/c=112,dt=22.06.2007,id=45124756 (Elefherotypia daily newspaper: "Saudi Arabian funds finance Mosque in Athens", 22nd of June 2007)

29)http://www.euro-muslim.com/En\_u\_Foundation\_Details.aspx?News\_ID=211

30)http://islamforgreeks.org/

31)http://www.youtube.com/watch?v=EPtJ10QYPXg&feature=related

32)http://www.rferl.org/content/Wahhabi\_Group\_Launches\_Conversion\_Campaign\_In\_Bosnia/2001137. html

33)http://www.islamicfinder.org/worldIslamicCountry.php?more=more&startPoint=0&endPoint=50&coun try=greece&lang=

34)http://en.wikipedia.org/wiki/2008\_Greek\_riots

35)Interview by Ioannis Michaletos to Polish Times on the Greek riots, English version: http://www.analyst-network.com/article.php?art\_id=2653

36)http://www.enet.gr/?i=news.el.ellada&id=47040 (Elftherotypia daily newspaper : "Clashes with Muslim immigrants", 23rd of May 2009)

37)http://www.setimes.com/cocoon/setimes/xhtml/en\_GB/features/setimes/newsbriefs/2009/05/31/nb-06

38)http://www.enet.gr/?i=news.el.ellada&id=47040

39) http://www.analyst-network.com/article.php?art\_id=3722

40)http://archive.ekathimerini.com/4dcgi/\_w\_articles\_politics\_100006\_17/11/2010\_121222

41)http://www.enet.gr/?i=news.el.ellada&id=225466 (Eleftherotypia daily newspaper : "Muslims clash with riot Police because of the Koran, 19th of November 2010)

42)Ibid.

43)http://news.bbc.co.uk/2/hi/europe/4763777.stm

44)http://www.worldsecuritynetwork.com/showArticle3.cfm?article\_id=15586

45)http://www.guardian.co.uk/world/2007/aug/28/helenasmith.international

46)http://www.worldsecuritynetwork.com/showArticle3.cfm?article\_id=15586

47)http://wn.com/Forest\_Fires\_Suspected\_arson\_Athens,\_Greece

48)http://www.worldsecuritynetwork.com/showArticle3.cfm?article\_id=15586

49)Greek daily newspaper "Ta Nea" on 30 November 2007:"Greece Servers As Transit Country for Islamists"

50)Ibid



51)http://www.epikaira.gr/epikairo.php?id=2682&category\_id=0 (Epikaira weekly political magazine: "Preparations for urban Islamic uprising", 24th of November 2010)

52)http://www.islamicpopulation.com/Europe/Greece/Islam%20in%20Greece.html

53)http://www.euro-islam.info/country-profiles/greece/

54)http://www.inews.gr/116/i-lista-me-ta-paranoma-tzamia-stin-athina.html, "The list with the illegal mosques in Athens"

55)http://news.kathimerini.gr/4dcgi/\_w\_articles\_ell\_1\_24/04/2010\_398765 (Kathimerini daily newspaper : "The process for the construction of the Mosque in Athens is accelerating", 24th of April 2010)

56)http://www.npr.org/2011/01/21/133121680/Greeks-Divided-On-Mosque-Construction

#### Greece and the extremist trends of Islam

#### **By Ioannis Michaletos**

Source: http://www.drougos.gr/

Greece is an E.U., NATO and Eurozone



country that has traditionally strong links with the Islamic world due to the geographical proximity with the Middle East and North Africa and the Ottoman rule that lasted four centuries, along with numerous historical encounters with Islam since the Middle Ages. Currently the country faces a debt crisis that, apart from its obvious disastrous financial consequences both in a domestic and in a global scale, also raises security concerns related to terrorist



networks of Islamist origin. Recent upheavals in Maghreb

and the Middle East pertain to Greek and European security as well.

Presently, the country hosts a Muslim minority

(map – dark grey areas) that is a remnant of the Ottoman Empire, but also an expanding Islamic population from the Arab countries and Pakistan that enter Greece in significant number as illegal immigrants. Corporations in the country, such as banking institutions, tourist companies and real estate firms are in control of Islamic funds, whereas countries such as Egypt, Saudi Arabia, Iran, Turkey and Libya can be considered significant trade partners of Greece.

In Athens; Greece, the Iranian Saderat bank is hosted, (25-29 Panepistimiou Str., 10564 Athens) which is a U.S black-listed institution due to alleged links with Hezbollah. Iran covers 25 percent of Greece's oil needs per annum and segments of its natural gas needs. There are indications that Hezbollah groups are operating in a logistical-support basis in Athens by gathering funds through tobacco contraband over the past years, as a 2007 report by American collective security research outlined. In a broad sense, Greece, due to a mixture of its geographical placement, history and



business links, is considered a gateway for the Islamic element in close proximity to the European Union and the Balkans, and over the past 10 years it has become one of the main transit territories for Islamic-originating illegal immigration to Europe.

Until now Greece does not seem to have a particular issue of Islamic fundamentalism. Nevertheless, as aptly described in a 2009 U.S. State Department report on terrorism,

"Greece is increasingly an E.U. entry point for illegal immigrants coming from the Middle East and South Asia, and there was concern that it could be used as a transit route for terrorists travelling to Europe and the United States. The number of illegal immigrants entering Greece, especially through the Aegean Sea, increased dramatically in 2008 and 2009, with more than 100,000 illegal immigrants, nearly half of whom originated from North Africa, the Middle East and South Asia, arrested each year."

Presently in Greece, there seems to be activity within radical Islamic elements as well as gradual projection of Islamic political entities through the use of Greek nationals. weekly To Proto Thema reported that Greek leftist terrorists seem to have been trained in Lebanon in paramilitary camps operated by Islamists.

In a special report by the French daily Le Figaro, on December 21, 2010, the case of the route of Islamic terrorists from Lebanon to Europe was noted with significant details. The Lebanese Army Cornell Mahmoud Issa (photo –right) noted to the French journalists that since November 2010, some 20 extremists managed to escape from a camp where they were kept in Lebanon and found their way to the European Union. He stated that already the authorities had been notified on an



A revelation by the infamous WikiLeaks telegrams showed that the ex-U.S. ambassador in Athens, Daniel Speckhard, has noted the danger of the nexus between Greek domestic terrorist groups and Islamic groups, including those from Iran, as he was informed by the then-Greek minister of public Order, Michalis Chrysohoidis. The leaked telegram was presented by the Greek weekly paper To Vima along with further analysis that points out that the fears expressed are of valid nature.

In 2007 a rocket launch attack with an RPG against the American Embassy in Athens (site of broken window at picture) was carried out by the Greek group Revolutionary Struggle, which stated in its proclamation note support for Hezbollah in Lebanon. In 2009 the Greek



international level, although he admitted that this is a difficult task. The French security authorities believe that this is the case of a new jihad mission heading towards European metropolises.

In classified documents that were in possession of radical groups in Lebanon, it was noted that three men managed to leave the camp through Syria and Turkey and up to Greece and Bulgaria with the assistance of illegal immigrant transport networks managed by Turks. They managed to acquire fake IDs and were finally caught by a common operation of the Bulgarian and Greek authorities. That case was closely monitored by British and French intelligence due to the fact that these two countries were the ultimate destination of

the Lebanese group. Mahmoud Issa stated that more cases are to be found that evade the authorities so far.

#### Incidents of interest

According to the pre-9/11 French intelligence report, American interests in Greece and Cyprus were considered by Osama bin Laden's network as targets. Citing a DGSE document, To Vima reported that members of al Qaeda, mostly located in Beirut, in cooperation with Taliban officials and other armed groups, were planning to hijack airplanes between March and September 2000, yet it was never carried out due to various logistical and operational disagreements.

European intelligence agencies have also reported that about 20 Arab fundamentalists have been arrested in Britain, Italy, Portugal, France and the Netherlands for having in their possession forged Greek passports, according to a 2007 revelation by the Greek daily Ta Nea and for the period 2001-2006.

In another notable case, in September 2005 Moroccan Anwar Mazrar— one of the leading Al Qaeda operational terrorists in Europe—was arrested on the Greek-Turkey border while attempting to travel to Greece on the Istanbul-Thessalonica bus service. Mazrar had been accused of being a leading member of terrorist groups in Morocco and also of having ties with al Qaeda. It was revealed that Mazrar was planning to stay in Greece for a while as an illegal immigrant and then move on to Italy and plan two bombing attacks.

Mazrar regularly travelled from Milan, Italy, to Algeria, Syria and Turkey. Greek authorities suspected that he was interested in setting up a base of support in Greece and use the country as a safe haven between Italy and the Middle East. In 2005, immediately after the capture of Mazrar, there was a boost in surveillance by the Greek authorities of suspected Islamist radicals in the country. Cooperation between Greece, the United States, France, Italy and the United Kingdom intensified in that sector.

Towards the end of 2010, various press reports claimed that radical Islamic action was increasing in the center of Athens, and the issue became widely publicized after it was brought to Parliament via the LAOS political party, which demanded state explanations on the issue and proper notification of security forces. According to statements by several Greek politicians, the country hosts amongst its illegal immigrant population radical cells and quite possibly "al Qaeda sleeping cells."

In another case in 2005, the so-called "Pakistani abduction case," 28 Pakistani immigrants were allegedly kidnapped by Greek intelligence agents in Athens. That case was connected to the cooperation between Greek and U.K. authorities following the July 2005 bombings in London, but was also the first notable case of accusation of the Greek state by Islamic organizations that Greece is actively turning against the Islamic element and taking harsh measures in the "war against terror." The Greek weekly newspaper Proto Thema



disclosed the names of 15 alleged Greek agents and an MI6 spy chief allegedly involved with kidnapping and torturing the Pakistanis eight days after the London bombings of July 7, 2005. There was widespread support by leftist groups that demanded through a series of legal actions and demonstrations the punishment of the Greek and U.K. security members involved. According to all data up to now, the Pakistani immigrants were somehow connected. probably via mobile phone SMS texting and conversations, with the terrorist group responsible for the July 2005 bombings in London. Although six years have passed, Greek and U.K. authorities have not revealed the extent of the involvement of these immigrants.

In early 2011, the Greek media revealed information mainly derived from WikiLeaks that U.S. diplomats in Athens had since 2006 information that there is a nexus between illegal immigrant trafficking networks from Pakistan and terrorists groups in that country that profit from that illicit market. American diplomats at that period in Athens met with their Pakistani counterparts and then provided to Greek authorities several names of traffickers suspected with links to terrorists.

According to the State Department, the Greek authorities didn't take any action, and one Pakistani diplomat who served in Athens at that period, in a conversation with an American officer, commented that he suspects "Greek security officials may be involved in covering the traffickers."

In July 2009 Abu Sanjat, am Iraqi citizen wanted by Interpol due to his involvement with terrorist attacks in Baghdad, was arrested in Greece. His arrest was a joint Greek-American-Iraqi operation. According to media reports, he was one of the main ringleaders of al Qaeda in Iraq who wanted to expand the network into Europe. He came to Greece as an illegal immigrant by crossing the borders with Turkey and joined a team of another 20 immigrants. When he was arrested he had forged papers identifying him as a Palestinian refugee



claiming political asylum.

In 2006 another case of interest took place in the Athens international network. According to reportage by the Greek daily paper Kathimerini, an imam and

Pakistani citizen wanted for terrorist attacks and homicide was arrested as he was flying from the United Kingdom, where he lived in a provincial town. The police investigation revealed that his purpose of visiting Athens was to enact a series of religious seminars for the expanding community of Pakistani immigrants in the city. Although there was an international arrest warrant against him by authorities of Pakistan, he was able to pass through the airport controls in London before taking his flight to Athens. That particular incident alarmed the Greek authorities who surprisingly were able to map an emerging social network of Pakistani radical Islamists in Greece before they were able to commit illegal activities or terrorist actions.

#### Overall

Greece's geographical placement, in addition to the wider culminations in the Mediterranean that have unfolded over the past year, has sounded alarm bells over the peril of the country being used as a regional logistics hub for international Islamic terrorists and a breeding ground of radicals amongst the communities of illegal immigrants from Islamic countries.

A Greek intelligence service report that was leaked in April 2011 in the Greek daily paper Ethnos points to a definite nexus between international organized crime, illegal immigration trafficking, and the communities of Islamists in the country who in their turn finance and form NGOs in order to attain influence in the local society. The danger of infiltration of terrorists in all of the above is also highlighted.

The main known countermeasures that have been taken by the Greek authorities include increased exchange of intelligence with partner countries, technological upgrade of surveillance equipment, and infiltration of suspected radical and terrorist cells.

#### The threat of Electro Magnetic Pulse

Source:http://www.publicbroadcasting.net/wbfo/news.newsmain/article/1/0/1822497/

A businessman man in Elma is leading the fight against a major threat to the nation's electrical grid. WBFO news contributor Rich Kelmman and senior correspondent for WGRZ-TV tells us about Electro Magnetic Pulse or EMP.

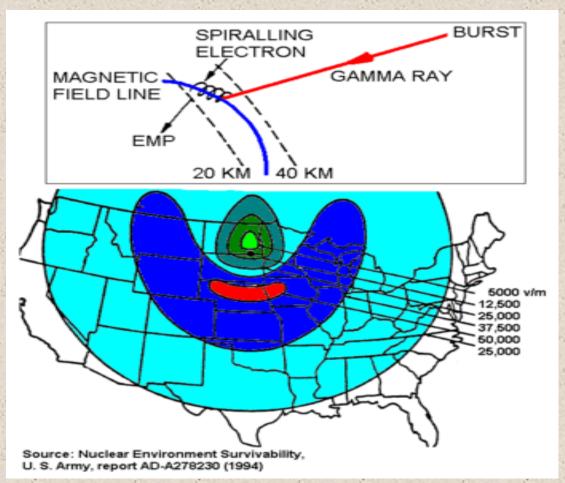
Have you ever considered what would happen if one day all electricity just stopped. Local businessman Henry Schwartz thinks about it a lot.

"You'd get up and none of the lights would work. Your radio wouldn't work, the car wouldn't start, your water system would stop. Go to the food store and there wouldn't be any. Everything that we know in the modern world would grind to a halt," said Schwartz. In 2008, an independent congressional commission warned that an electromagnetic pulse generated by a nuclear blast high above the earth could critically damage or destroy our electric grid.

Henry Schwartz's business runs on electricity. He owns Steuben Foods in Elma and employs some 500 people. They manufacture and package food and medical supplies. About three years ago, he became deeply concerned about EMP and formed a not-for-profit organization called EMPact America.

"(EMP is) more of a threat than nuclear devices exploded in 10 of our cities at the same time," he said.





The sun can also generate emp through solar storms. UB physics professor Dr. Will Kinney shows us video of the sun spewing a geyser of superheated gas in early June. "Blammo," said Kinney. "And that was just last Tuesday. That material travels outward in space and can affect things like communications and the infrastructure on the earth."

At risk are more than 200,000 miles of transmission lines across North America. In 1989, a blast of hot solar gas knocked out power for six million people in and around Quebec for about 9 hours.

"It's entirely possible that we could see large outages again from these kinds of solar storms," said Kinney. "But those regional outages didn't result in cascading failures."

But back in 1859, a huge supersolar storm, far bigger than the one that caused the Quebec blackout, shorted out telegraph wires in the United States and Europe and caused fires. The northern lights were seen as far south as Rome, and the world was not wired then as it is today.

What are the odds of that happening again? Will Kinney said,"Nobody really knows for sure."

Anthony Caruana is Town Supervisor of Tonawanda. "The likelihood may be rare," said Caruana. "But we need to be prepared just in case."

Caruana is a retired Army brigadier general. "I don't think anybody ever believed that 9/11 could happen with airplanes going into massive buildings using our own planes and our own fuel to hit it."

"A lack of imagination," said Caruana.

In 2008 after eight years of study, the Congressional EMP Commission issued its final report, which focused on EMP as a weapon. We reach senior staff member Dr. Peter Pry in Washington and asked whether the commission considers nuclear EMP a clear and present danger.

"Yes, that's correct. the commission did judge that it was a clear and present danger now," said Pry.

Pry envisions an attack by an enemy that explodes a nuclear bomb in space, 300 miles above the United States. The resulting EMP destroys our entire electrical system. Everything shuts down. "North Korea has the bomb now." he said, "and North Korea will sell anything to anybody."

As for Iran, Pry said, "The Federation of American Scientists put out an estimate that Iran could have enough fuel for several nuclear bombs within five months."

There is debate among some experts about the actual likelihood of the nightmare scenario foreseen in the Commission report. "I certainly think they have the desire and motivation to do what they say," said UB physics professor Dr. Dejan Stojkovic.

"Right now, I don't think they have the capabilities to do what they say, but that may change in the near future," said Stojkovic.

"We are in a very critical position here in our town," said Caruana. "We have a water treatment plant, we have a wastewater plant, we have emergency services, hazardous materials and critical infrastructure."

Tonawanda has a backup generator at its wastewater treatment plant. good for a few weeks, till the fuel runs out. "So if we're doing things protecting our own equipment things here," says Caruana, If it's not done at the next level, we may not even be able to continue to function."

In response to the threat, Congress is considering a bill called the Shield Act to strengthen the nation's electric grid. "I think everybody should get to their congressman and tell them this is a high urgency," said Schwartz.

Caruana calls Schwartz a good neighbor and a patriot. "He's dedicated, it looks like, this part of his life, to making sure we're protected."

Henry Schwartz is the sole funder of EMPact America. With its mission of informing the public about EMP, we ask why he is doing that. "What's in it for me?" he said. "Well,I have a family just like you probably do, and I'd like them to live. I also have another family, and that's the employees that I work with everyday. I have a community, and I have the United States of America, and I want to hold onto them with all my heart and soul.

"My life wouldn't be worth living if we had an EMP event and we're not prepared. So it's everything," said Schwartz.

## The Powers of Manipulation: Islam as a Geopolitical Tool to Control the Middle East

#### By Mahdi Darius Nazemroaya

Source: http://www.globalresearch.ca/index.php?context=va&aid=25199

As Washington and its cohorts march towards the Eurasian Heartland, they have tried to manipulate Islam as a geo-political tool. They have created political and social chaos in the process. Along the way they have tried to redefine Islam and to subordinate it to the interests of global capital by ushering in a new



generation of so-called Islamists, chiefly amongst the Arabs.

### The Project to Redefine Islam: Turkey as the New Model and "Calvinist Islam"

Turkey in its present form is now being presented as the democratic model for the rebelling Arab masses to follow. It is true that Ankara has progressed since the days it used to ban Kurdish from being spoken in public, but Turkey is not a functional democracy and is very much a kleptocracy with fascist tendencies.

The military still plays a huge role in the affairs of the state and government. The term "deep state," which denotes a state run secretly from the top-down by unaccountable bodies and individuals, in fact originates from Turkey. Civil rights are still not respected in Turkey and candidates for public office have to be approved by the state apparatus and the

groups controlling them, which try to filter out anyone that would go against the status quo in Turkey.

Turkey is not being presented as a model for the Arabs due to its democratic qualifications. It is being presented as the political model for the Arabs, because of a project of political and socio-economic "bida" (innovation) involving the manipulation of Islam.

Although very popular, the Turkish Justice and Development Party or JDP (Adalet ve Kalkinma Partisi or AKP) was allowed to come into power in 2002, without opposition by the Turkish military and the Turkish courts. Before this there was little tolerance for political Islam in Turkey. The JDP/AKP was founded in 2001 and the timing of their founding and their electoral win in 2002 was also tied to the objective of redrawing Southwest Asia and North Africa.

This project to manipulate and redefine Islam seeks to subordinate Islam to dominant World Order capitalist interests through a new wave of "political Islamism", such as the JDP/AKP. A new strand of Islam is thereby being fashioned through what has come to be called "Calvinist Islam" or a "Muslim version of the Protestant work ethic." It is this model that is been nurtured in Turkey and now being presented to Egypt and the Arabs by Washington and Brussels.

This "Calvinist Islam" also has no problem with the "reba" or interest system, which is prohibited under Islam. It is this system that is used to enslave individuals and societies with the chains of debt to global capitalism. It is in this context that the European Bank of Reconstruction and Development (EBRD) is calling for so-called "democratic reforms" in the Arab World.

The ruling families of Sauda Arabia and the Arab petro-sheikhdoms are also partners in the enslavement of the Arab world through debt. In this regard Qatar and the Arab sheikhdoms of the Persian Gulf are in the process of creating a Middle East Development Bank that is intended to give loans to Arab countries to support their "transition towards democracy". The democracy promotion mission of the Middle East Development Bank is ironic because the countries forming it are all staunch dictatorships.

It is also this subordination of Islam to global capitalism that is causing internal friction in Iran.

## Opening the Door for a New Generation of Islamists

The hope in Washington is that this "Calvinist Islam" will take root with a new generation of Islamists under the banner of new democratic states. These governments will effectively enslave their countries by placing them further into debt and selling national assets. They will help subvert the region extending from North Africa to Southwest and Central Asia as the area is being balkanized and restructured in the image of Israel under ethnocratic systems.

Tel Aviv will also wield wide influence amongst these new states. Hand-in-hand with this project, different forms of ethno-linguistic nationalism and religious intolerance are also being promoted to divide the region. Turkey also plays an important, because it is one of the cradle for this new generation of Islamists. Saudi Arabia too plays a role in supporting the militant wing of these Islamists.

#### Washington's Restructuring of the Geo-Strategic Chessboard

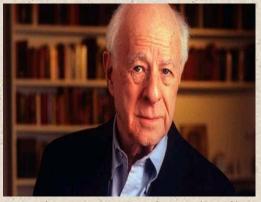
Targeting Iran and Syria is part of the larger strategy of controlling Eurasia. Chinese interests have been attacked everywhere on the global map. Sudan has been balkanized and both North Sudan and South Sudan are headed towards conflict. Libya has been attacked and is in the process of being balkanized. Syria is being pressured to surrender and fall into line. The U.S. and Britain are now integrating their national security councils, which parallels Anglo-American bodies from the Second World War.

Targeting Pakistan is also connected to neutralizing Iran and attacking Chinese interests and any future unity in Eurasia. In this regard, the U.S. and NATO have militarized the waters around Yemen. At the same time in Eastern Europe, the U.S. is building its fortifications in Poland, Bulgaria, and Romania to neutralize Russia and the former Soviet republics. Belarus and Ukraine are being -put.

under increasing pressure too. All these steps are part of a military strategy to encircle Eurasia and to either control its energy supplies or the flow of energy towards China. Even Cuba and Venezuela are under increasing threat. The military noose is globally being tightened by Washington.

It appears that new Islamist parties are being formed and groomed by the Al-Sauds with the help of Turkey to take power in Arab capitals. Such governments will work to subordinate their respective states. The Pentagon, NATO, and Israel may even select some of these new governments to justify new wars.

It has to be mentioned that Norman Podhoretz (photo), an original member of the



Project for a New American Century (PNAC), in 2008 suggest an apocalyptic future scenario in which Israel launches a nuclear war against Iran, Syria, and Egypt amongst its other neighbouring countries. This would include Lebanon and Jordan. Podhoretz described an expansionist Israel and even suggested that the Israelis would militarily occupy the oil fields of the Persian Gulf.

What came across as odd in 2008 was the suggestion by Podhoretz, which was influenced by the strategic analysis of the Center for

Strategic and International Studies (CSIS), that Tel Aviv would launch a nuclear attack on its staunch Egyptian allies ruling Cairo under President Mubarak. Despite the fact that the old regime still remains, Mubarak is no longer in power in Cairo. The Egyptian military still gives orders, but Islamists may come to power. This is occuring despite the fact that Islam continues to be demonized by the U.S. and most of its NATO allies.

#### **Unknown Future: What Next?**

The U.S., the E.U., and Israel are trying to use the upheavals in the Turko-Arabo-Iranic World to further their own objectives including the war on Libya and the support of an Islamic insurrection in Syria. Along with the Al-Sauds, they are attempting to spread "fitna" or division amongst the peoples of Southwest Asia and North Africa. The Israeli-Khaliji strategic alliance, formed by Tel Aviv and the ruling Arab families in the Persian Gulf, is crucial in this regard.

In Egypt the social upheaval is far from over and the people are become more radical. This is resulting in concessions by the military junta in Cairo. The protest movement is now starting to address the role of Israel and its relationship to the military junta. In Tunisia too, the popular stream is headed towards radicalization.

Washington and its cohorts are playing with fire. They may think that this period of chaos presents an excellent opportunity for confrontation with Iran and Syria. The upheaval that has taken root in the Turko-Arabo-Iranic World will have unpredictable results. The resilience of the peoples in Bahrain and Yemen under the threats of increased state-sponsored violence indicates the articulation of more cohesive anti-US and Anti-Zionist protest movement.

Mahdi Darius Nazemroaya specializes in the Middle East and Central Asia. He is a Research Associate of the the Centre for Research on Globalization (CRG).

#### U.S. cost of war at least \$3.7 trillion and counting

Source: http://www.rawstory.com/rs/2011/06/29/u-s-cost-of-war-at-least-3-7-trillion-and-counting/

When President Barack Obama cited cost as a reason to bring troops home from Afghanistan, he referred to a \$1 trillion price tag for America's wars.

Staggering as it is, that figure grossly underestimates the total cost of wars in Iraq, Afghanistan and Pakistan to the U.S. Treasury



and ignores more imposing costs yet to come, according to a study released on Wednesday.

The final bill will run at least \$3.7 trillion and could reach as high as \$4.4 trillion, according to the research project "Costs of War" by Brown University's Watson Institute for International Studies. (http://www.costsofwar .org)

due to an aging American population and skyrocketing healthcare costs.

It also raises the question of what the United States gained from its multitrillion-dollar investment.

"I hope that when we look back, whenever this ends, something very good has come out of it," Senator Bob Corker, a Republican from

Other War Costs in Pentagon Base Budget, Interest Payments, Veterans' Care, Homeland Security, and War-Related Aid

Pentagon War Appropriations \$1.3 Trillion

\$1.9 to \$2.7 Trillion

In the 10 years since U.S. troops went into Afghanistan to root out the al Qaeda leaders behind the September 11, 2001, attacks, spending on the conflicts totaled \$2.3 trillion to \$2.7 trillion.

War Costs

to Date:

\$3.2 to \$4 Trillion

Those numbers will continue to soar when considering often overlooked costs such as long-term obligations to wounded veterans and projected war spending from 2012 through 2020. The estimates do not include at least \$1 trillion more in interest payments coming due and many billions more in expenses that cannot be counted, according to the study.

In human terms, 224,000 to 258,000 people have died directly from warfare, including 125,000 civilians in Iraq. Many more have died indirectly, from the loss of clean drinking water, healthcare, and nutrition. An additional 365,000 have been wounded and 7.8 million people -equal to the combined population of Connecticut and Kentucky -- have been displaced.

"Costs of War" brought together more than 20 academics to uncover the expense of war in lives and dollars, a daunting task given the inconsistent recording of lives lost and what the report called opaque and sloppy accounting by the U.S. Congress and the Pentagon.

The report underlines the extent to which war will continue to stretch the U.S. federal budget, which is already on an unsustainable course Tennessee, told Reuters in Washington. Sept 11, 2001: The damage continues

In one sense, the report measures the cost of 9/11, the American shorthand for the events of September 11, 2001. Nineteen hijackers plus other al Qaeda plotters spent an estimated \$400,000 to \$500,000 on the plane attacks that killed 2,995 people and caused \$50 billion to \$100 billion in economic damages.

What followed were three wars in which \$50 billion amounts to a rounding error. For every person killed on September 11, another 73 have been killed since.

Was it worth it? That is a question many people want answered, said Catherine Lutz, head of the anthropology department at Brown and codirector of the study.

"We decided we needed to do this kind of rigorous assessment of what it cost to make those choices to go to war," she said. "Politicians, we assumed, were not going to do that kind of assessment."

The report arrives as Congress debates how to cut a U.S. deficit projected at \$1.4 trillion this year, roughly a 10th of which can be attributed to direct war spending.

What did the United States gain for its trillions? Strategically, the results for the United States are mixed. Osama bin Laden and Saddam Hussein are dead, but Iraq and Afghanistan are far from stable democracies. Iran has gained influence in the Gulf and the Taliban; though ousted from government, remain a viable military force in Afghanistan.

"The United States has been extremely successful in protecting the homeland," said George Friedman, founder of STRATFOR, a U.S.-based intelligence company.

"Al Qaeda in Afghanistan was capable of mounting very sophisticated, complex, operations on an intercontinental basis. That organization with that capability has not only been substantially reduced, it seems to have been shattered," Friedman said.

Economically, the results are also mixed. War spending may be adding half a percentage point a year to growth in the gross domestic product but that has been more than offset by the negative effects of deficit spending, the report concludes.

#### **Comprehensive study**

Some U.S. government reports have attempted to assess the costs of war, notably a March 2011 Congressional Research Service report that estimated post-September 11 war funding at \$1.4 trillion through 2012. The Congressional Budget Office projected war costs through 2021 at \$1.8 trillion.

A ground-breaking private estimate was published in the 2008 book "The Three Trillion Dollar War," by Linda Bilmes, a member of the Watson Institute team, and Nobel-winning economist Joseph Stiglitz. That work revealed how much cost was added by interest on deficit spending and medical care for veterans.

The report draws on those sources and pieces together many others for a more comprehensive picture.

The report also makes special note of Pakistan, a front not generally mentioned along with Iraq and Afghanistan. War has probably killed more people in Pakistan than in neighboring Afghanistan, the report concludes. Politicians throughout history have underestimated the costs of war, believing they will be shorter and less deadly than reality, said Neta Crawford, the other co-director of the report and a political science professor at Boston University.

The report said former President George W. Bush's administration was "shamelessly politically driven" in underestimating Iraq war costs before the 2003 invasion.

Most official sources continue to overlook costs, largely because of a focus on just Pentagon spending, Crawford said.

"Over the last decade, we have spent a trillion dollars on war," Obama said in last week's speech on reducing U.S. troop levels in Afghanistan. At the very least, he was rounding down by \$200 billion to \$300 billion, when counting U.S. congressional appropriations for the post 9/11 wars.

"I don't know what the president knows, but I wish it were a trillion," Crawford said. "It would be better if it were a trillion."

#### Elusive number

In theory, adding up the dollars spent and lives lost should be a statistical errand. The U.S. Congress appropriates the money, and a life lost on battlefield should have a death certificate and a casket to match.

The team quickly discovered, however, the task was far more complicated.

Specific war spending over the past 10 years, when expressed in 2011 dollars, comes to \$1.3 trillion, the "Costs of War" project found. When it comes to accounting for every dollar, that \$1.3 trillion is merely a good start.

Since the wars have been financed by deficit spending, interest must be paid -- \$185 billion of accumulated so far.

The Pentagon has received an additional \$326 billion to \$652 billion beyond what can be attributed to the war appropriations, the study found.

Homeland security spending has totaled another \$401 billion so far that can be traced to September 11. War-related foreign aid: another \$74 billion.

Then comes caring for U.S. veterans of war. Nearly half of the 1.25 million who have served in uniform in Iraq and Afghanistan have used their status as veterans to make health or disability claims at an expense of \$32.6 billion to date.

Those costs will soar over the next 40 years as veterans age. The report estimates the U.S. obligations to the veterans will reach \$589 billion to \$934 billion through 2050.

So far, those numbers add up to a low estimate of \$2.9 trillion and a moderate estimate of \$3.6 trillion in costs to the U.S. Treasury. No high estimate was offered.

"We feel a conservative measure of costs is plenty large to attract attention," said report contributor Ryan Edwards, an economist who studied the war impact on deficit spending. Those numbers leave out hundreds of billions

in social costs not born by the U.S. taxpayer

but by veterans and their families: another \$295 billion to \$400 billion, increasing the range of costs to date to some \$3.2 trillion to \$4 trillion.

That's a running total through fiscal 2011. Add another \$453 billion in war-related spending projected for 2012 to 2020 and the total grows to \$3.668 trillion to \$4.444 trillion.

#### The human toll

If the financial costs are elusive, so too is the human toll. The report estimates between 224,475 and 257,655 have been killed in Iraq. Afghanistan and though those Pakistan, numbers give a false sense of precision. There are many sources of data on civilian deaths, most with different results.

The civilian death toll in Iraq -- 125,000 -- and the number

of Saddam's security forces killed in invasion --10,000 -- are loose estimates. The U.S. military does not publish a thorough accounting.

"We don't do body counts," Tommy Franks, the U.S. commander in Iraq, famously said after the fall of Saddam in 2003.

In Afghanistan, the civilian death count ranges from 11,700 to 13,900. For Pakistan, where there is little access to the battlefield and the United States fights mostly through aerial drone attacks, the study found it impossible to distinguish between civilian and insurgent deaths.

The numbers only consider direct deaths -people killed by bombs or bullets. Estimates for indirect deaths in war vary so much that researchers considered them too arbitrary to report.

"When the fighting stops, the indirect dying



continues. It's in fact worse than land mines. The healthcare system is still in bad shape. People are still suffering the effects of malnutrition and so on," Crawford said.

Even where the United States does do body counts -- for the members of the military -- the numbers may come up short of reality, said Lutz, the study's co-director. When veterans return home, they are more likely to die in suicides and automobile accidents.

#### Interview with former Foreign Secretary of Pakistan

#### By Hubertus Hoffman

Source: http://www.worldsecuritynetwork.com

Riaz Khokhar, Foreign Secretary of Pakistan from 2002 to 2005, former Ambassador to China and the USA as well as High Commissioner to India, discussed with Dr. Hubertus Hoffmann, President of the World Security Network Foundation, the nature of extremism, Osama bin Laden, the Taliban, the army, and politics in Pakistan. Khokhar also commented on the U.S. strategy in Afghanistan, explained the relation between India and Pakistan after the Mumbai terror attacks and Islam in Pakistan.

Hubertus Hoffmann: Aatish Taseer complained in a well received Financial Times article on May 5, 2011: "There has also been, since Benazir Bhutto's assassination, a campaign to silence dissent in Pakistan. Earlier this year, my father, the governor of Punjab, was killed by his own guard. The act was put down to the actions of a single man. But later that week there were vast demonstrations of support for my father's killer - rallies of 40,000.

and more - and leading them was Lashkar-e-Taiba, a group created and nurtured by the Pakistani army, which is loath to put it out of business due to its special hatred of India. Its leader, Hafez Saeed, was also the man conducting prayers for bin Laden this week. There is such a climate of fear and violence in Pakistan at the moment that only a fraction of what happens gets reported." What is the situation in Pakistan now and are radicals



winning step by step while the majority stays silent?

**Riaz Khokhar:** Aatish is the son of very notable parents. He is a brilliant young man and has a great future in the world of literature. I share his grief and wish him well.

I knew Salman Taseer, we were class mates in school. He was a fabulous person, who did not deserve a tragic end. Yes, it is indeed abominable that some people supported the killer's act, but the large majority of the people in Pakistan were shocked and saddened by the heinous act. There was no justification whatsoever for killing Salman Taseer.

Salman Taseer was principally let down by his own political party, the Pakistan Peoples Party (PPP). The President of Pakistan, also the Chairperson of the PPP, should have attended Taseer's funeral, which would have given the clearest signal to the extremist elements that the President was going to deal with them with a firm hand. Instead the Prime Minister attended the last rites, a person who is a political light weight and not taken seriously by any one, let alone the extremists. After the murder, the PPP government should have launched an aggressive campaign to deal with the extremists, but instead it pursued a policy of appeasement. Extremism has been on the march since the days of President Zia UI Haq, who was the darling of the West, especially close to the U.S. Zia's rule was a curse for Pakistan, but his patrons were successive US Presidents. It was the US that had encouraged the Jihadi culture in Pakistan for the struggle against the Soviet Union. How can anyone forget that President Reagan had embraced the Afghan Mujahideen leaders in the Oval Office.

One of the principal reasons for the growth of extremism is that the secular and moderate political forces conceded too much political space to the extremists. The secular political forces have failed to deliver a social and economic program the masses of Pakistan, which would bring about a change in the quality of life of the people. In the last four years the situation has worsened. More than half of Pakistan's population (ca. 180 million people) has fallen below the poverty line. Because of the dire economic situation and worsening condition law and order, the country is slowly moving towards an anarchical situation, something the extremists would welcome.

There is no doubt that the culture bred by Zia ul Haq is still flourishing, including to some extent in the Armed Forces. The infection in the army is limited and is being rooted out.

The best and most effective way to deal with extremism is not through military means, but by presenting to the people of Pakistan a more powerful and promising message of hope. This is the responsibility of political parties. Today, Pakistan has the poorest and most incompetent political leadership, which is incapable of providing good governance. If this political dispensation continues, radicalism will gain strength.

Hubertus Hoffmann: Taseer continued on Osama bin Laden: "Let us be clear about what happened last week: Osama bin Laden was not just found living in Abbottabad, there out of some inverse logic of his own. He was found in this garrison town because he was the guest of the army. And now the charges against this army and its agencies are manifold". When asked for his opinion by the World Security Network Foundation, a respected head of a Western intelligence agency stated: "The

Director of the ISI and the Chief of Staff indisputably knew about Osama bin Laden's residence, while a separated group of the ISI was in charge. They feared that to hand him over to the U.S. and having him imprisoned in Guantanamo Bay would produce an outcry in Pakistan. Moreover, they could have continued to ask for more support by the US against Al Qaeda". The Pakistani Parliament condemned the killing of bin Laden as well as the air strikes against terrorists in the tribal areas. Is the military playing a double game with the US and the West? What is Pakistan's position?

**Riaz Khokhar:** Yes, indeed Osama was found in Abbottabad, which is strictly speaking not a garrison town. The town hosts the Pakistan Military Academy, which is the equivalent to Sandhurst in England and West Point in the US. No combat or special action troops are stationed in Abbottabad.

The jury is still in the dark about who knew about Osama's presence in Abbottabad and who provided him the support system. Without a doubt, the government of Pakistan has to investigate and provide credible answers to very valid and critical questions. To date, it is a matter of record, that the President of the United States and some seniors officials have implied, that government leaders and senior official in Pakistan were not aware of Osama's presence in Abbottabad. Clearly, Osama had some support system, probably provided by some extremist groups, which were linked to Al Qaeda. Pakistan has conceded that we have to satisfy the international community on a host of issues arising from the Abbotabad incident.

Osama was not living in a \$ 10 Million mansion or a state owned safe house. From the TV clips and films it is evident, that he was living in penury and squalor. There were no security guards to protect him. The 79 Navy Seals actually killed an unarmed Osama. There was no exchange of fire. He was not surrounded by scores of highly trained loyal guards as was the ten years old myth created by the western media. It would have been better if he had been captured alive, and faced a trial, for the world could have discovered the truth about the attack on the US in 2001. Osama"s burial at sea was also controversial as it raised many questions. Hubertus Hoffmann: Concerning Afghanistan, some in ISAF and Kabul blame the Pakistani Army to play both sides of the fence, including secret support for the Afghan Taliban and protection of the Pakistani Taliban. What is the truth?

**Riaz Khokhar:** The US and ISAF have failed in Afghanistan and will probably face a Vietnamlike defeat. An illegal occupation force cannot win against person that is fighting for the freedom of their motherland. Afghanistan is a poor country and stands devastated. A quisling and corrupt regime has not only failed its people but has also taken the US and its allies for a huge ride. The regime has succeeded in one area, which is corruption on a monumental scale.

The real test for Afghanistan will come when the occupation forces leave the country to its own device. There is no military solution to the Afghan tangle. It has to be an Afghan solution, which reflects the ethnic mosaic of Afghanistan. Any outside sponsored solution would not work.

Any attempt to divide Afghanistan on ethnic lines, a proposal floated by Ambassador Blackwell will be a recipe for a civil war. Furthermore, any attempt to neutralize Afghanistan will not be acceptable to the proud Afghan people. The US exit plan has no sustainable political solution. It also seems that the US has no sincere desire to leave Afghanistan. It wants to retain and use the huge military bases against China, Iran, Russia and central Asian states. The US has also set its vision on the vast oil and gas resources of central Asia and the Caspian region. In sum, the US presence in Afghanistan is a factor of instability in the region.

Hubertus Hoffmann: Should the Taliban again take over control in the national interest of Pakistan in the Pashtun part of Afghanistan or was this time of cooperation from 1989 to 2001 more of a burden and disaster for Islamabad? What is the best design for Pakistan of Afghanistan?

**Riaz Khokhar:** The Tehrik-i-Taliban Pakistan (TTP) has declared war on Pakistan. Clearly, the TTP is sponsored by some forces, which.

are inimical to Pakistan. The key questions are: who is funding the TTP and who is providing highly sophisticated weapons and modern communication equipment to the TTP? It does not stand to reason, that the ISI is supporting the TTP to attack the Pakistan Army and security forces. The TTP does not enjoy the support of the tribes in the FATA region. In comparison, the Afghan Taliban has roots among the people because they are seen as fighting foreign occupation forces. This is consistent with centuries old Afghan tradition and culture.

As for Pakistan, it is not seeking an Islamabadmade solution to the Afghan problem. Pakistan has to take into account the sentiments of the 26 millions Pakhtuns in Pakistan and 12 million in Afghanistan. Pakistan cannot afford to earn the generational enmity of the Pakhtuns for the sake of American interests. Pakistan would not be able to recover from any military misadventure in the FATA region.

Hubertus Hoffmann: How should negotiations with the Taliban be done best?

Riaz Khokhar: The US has no choice but to talk to the Taliban directly and immediately. The US-Taliban talks at the lower levels, sponsored by the Germans, are showing some hopeful signs. All the countries directly bordering Afghanistan, including Russia and China should also be involved in the talks. If asked, Pakistan can assist in setting up these talks, but the US must not insist on keeping military bases in Afghanistan. It seems that the Taliban would give up their links with Al Qaeda and would not have any problems in renouncing violence, provided the US ends its military occupation. However, asking the Taliban to accept a highly flawed constitution makes no sense. The US would also be making a huge mistake in targeting and killing Mullah Omar, the one person who holds overwhelming influence over the various Taliban groups, and who could help in bringing about peace and stability in Afghanistan.

**Hubertus Hoffmann:** The most influential German Forces, the Wehrmacht, had some sympathies with the Nazis from 1918 until 1939, but in the end only proved to be a puppet of Adolf Hitler and his totalitarian Nazi regime.

Hitler promised to revitalize Germany after the shame of Versailles, but in the end produced 50 million dead, millions of Germans killed and all cities in ruins - could this become the fate and misperception of the Pakistani army? Will the terror monsters that it created finally destroy their masters and its homeland?

Riaz Khokhar: The comparison with Nazi Germany is not relevant. Pakistan has suffered mainly, because it got sucked into a war against terrorism, which it had not initiated. The overwhelming view in Pakistan is that it is not our war. There is a major gap between the opinions of the pro US government and the majority of the Pakistani people. Pakistan has sufferered from huge casualty numbers: 35000 innocent people killed, 5000 soldiers and 3000 paramilitary casualties and thousands disabled. Every city of Pakistan has faced bombing incidents. Pakistan's economy has endured huge losses to the tune of \$ 68 Billion. No county in the world has paid such a high price in blood and treasure. The people of Pakistan are asking why we should make more sacrifices? They are just fed up with the arrogant and imperialistic attitude of the USA.

**Hubertus Hoffmann:** Concerning India: is terrorism still a means in the toolbox of Pakistan? What should be done to ease the Kashmir issue?

**Riaz Khokhar:** Terrorism is not an instrument of Pakistan's policy towards India. The Bombay incident was a horrendous act. It was widely condemned by the government and the people of Pakistan. There is no reason to believe that Pakistan will not honor its commitment to carry out a free and fair trial. India has to cooperate with Pakistan in providing solid evidence, which will stand up in a court of law. It seems that the judicial process is moving in the right direction.

As for Kashmir, India is in illegal occupation. It has committed over 700,000 troops to bludgeon the Kashmiris into submission, who are only demanding the right of selfdetermination, a right conceded to them by Pandit Nehru, the first and the most well known Indian Prime Minister. It is shameful that India has been in gross violation of the UN resolutions for decades. Why is it that the US and the West have adopted double standards

in regard to Kashmir? Over 100,000 Kashmiris have been killed, several thousands disabled and thousands of women raped. Human rights violations are rampant, but the international community is blind to the happenings in Jammu and Kashmir. It is a reality that India has failed in suppressing the will of the people of Jammu and Kashmir over six decades even with the help of several hundred thousand Pakistan and India should sit across a table and find a peaceful solution to the oldest problem at the United Nations. War is neither an option for India nor for Pakistan, both have nuclear capabilities. Pakistan would like to live in peace and harmony with India. Our salvation lies in peace and stability, enabling both countries to divert precious resources to cater for the well-being of the teeming millions who



troops. Today, Kashmir is one huge armed military camp.

Timor got its independence through the right of self-determination, because the population was Christian. Similarly, South Sudan is being created and given independence, because the population is Christian in large parts. Why is it that the people of Jammu and Kashmir are not being allowed to exercise their right of selfdetermination? India claims to be largest democracy in the world and yet it is afraid of giving the Kashmiris the democratic rights to determine their own future. Pakistan would accept any solution that is acceptable to the people of Jammu and Kashmir as long as they are able to exercise their right in a free and fair manner without the presence of 700,000 troops.

are living in abject poverty.

Hubertus Hoffmann: Why do so few openly and aggressively defend the Prophet and the Koran against radicals? The true teaching of Islam is peace, understanding and tolerance towards Christians and Jews - why do we hear almost nothing to oust the extremists, why do the the totalitarian preachers of hate control the media and public attention? Is the silent majority in Pakistan paralyzed and scared or full of cowardice?

**Riaz Khokhar:** The majority of the people of Pakistan are deeply committed to Islam, but are moderate Muslims who firmly believe in and revere the Holy Quran and love and adore the Holy Prophet. The bulk of the people of Pakistan are too preoccupied with the daily life in search of bread and butter issues. They are also concerned about extremism and deport

acts of terrorism. The civil society in Pakistan has been at the forefront, challenging the wrongful interpretation of the Koran and promoting the true spirit of Islam.

Islam is a religion of peace and emphasizes respect for other religions. Muslims hold all Prophets in high esteem and accept them without any prejudice. Tolerance and understanding should guide people of all religions for the world to become a harmonious place.

The reality is ugly. Muslims have been following the massacred break-up of Yugoslavia. Over a million Iragi's died in a war which was based on utter lies and deceit. 500,000 Afghans have been killed in a war for which they were not responsible. The Islamic world is faced with many problems begging for solutions, namely the Arab-Israel problem, the Kashmir problem between India & Pakistan and several other issues. Today, Western countries are interfering in some Arab countries on the basis of highly dubious principles. There are some hardliners in the US who are suggesting that the US should also take military action against Syria and Iran.

There is immediate need for a serious dialogue between the Islamic World and the West, to develop a harmonious working relationship for the sake of future generations.

#### **Operation Smoking Dragon**

Source: http://www.fbi.gov/news/stories/2011/july/dragon 070511/dragon 070511

The judge who recently sentenced Yi Qing Chen noted that the smuggler "never saw a criminal scheme he didn't want a part of." The Southern California man was convicted last October of distributing methamphetamine, trafficking approximately 800,000 cases of counterfeit cigarettes, and conspiracy to import Chinese-made shoulder fired missiles into the U.S. Chen is now serving a 25-year prison sentence, and his case marks the end of a long-running investigation called Operation Smoking Dragon.

Smoking Dragon and a related case in New Jersey called Operation Royal Charm led to the indictment of 87 individuals from China, Taiwan, Canada, and the U.S. The investigations uncovered-and dismantled-an international smuggling ring that could have threatened the country's national security. Charges against the subjects included



The smugglers offered a variety of Chinese military-grade weapons, including surface-to-air missiles.

smuggling real and phony drugs and other contraband into the U.S. along with counterfeit \$100 bills-believed to have been produced in North Korea-that were so nearly perfect and so much more sophisticated than typical counterfeit currency they were dubbed "Supernotes."

"One of the most important things about Operation Smoking Dragon was that it demonstrated the broad range of international criminal activity conducted by today's Asian organized crime groups," said Special Agent Bud Spencer, who worked the case in our Los Angeles office.

The eight-year investigation began when FBI undercover agents, posing as underworld criminals, helped make sure that shipping containers full of counterfeit cigarettes made it past U.S. Customs officers undetected. Over time, as undercover agents won the smugglers' trust, they were asked to facilitate other illegal shipments such as narcotics and millions of dollars in Supernotes. Later, the smugglers offered a variety of Chinese military-grade weapons, including the QW-2 surface-to-air missiles.

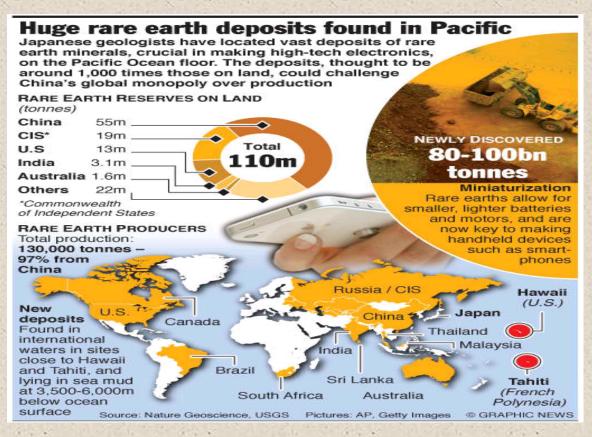
Some of the drugs-including methamphetamine and fake Viagra-were hidden in large cardboard boxes with false bottoms that contained toys. The Supernotes were placed between the pages of books or lined in large bolts of rolled-up fabric. All of the items were smuggled into the U.S. in 40-foot shipping containers.

Between Smoking Dragon and Royal Charm, some \$4.5 million in counterfeit currency was seized, along with more than \$40 million worth of counterfeit cigarettes, drugs, and other real and phony items. The smugglers were also forced to forfeit a total of \$24 million in cash, along with real estate, cars, and jewelry.

Most of the defendants were indicted in 2005 and have since pled guilty or been convicted. Chen was the final defendant to be sentenced relating to Operation Smoking Dragon. His was the nation's first conviction under a 2004 antiterrorism statute that outlaws the importation of missile systems designed to destroy aircraft.

"There is only one purpose for shoulder-fired missiles like the QW-2, and that is to bring down aircraft," said Special Agent Omar Trevino, who worked the case from the beginning. "Smoking Dragon dismantled an international smuggling ring, and it illustrated that organized crime groups will stop at nothing to make a profit."

Mark Aveis, an assistant United States attorney in Los Angeles who prosecuted the Chen case, agreed with Agent Trevino. "Chen and his associates didn't care what they smuggled as long as they made money," he said. "This case highlights the FBI's ability to carry out successful long-term undercover investigations—and the continuing need for such investigations."



# Japanese discovery could undermine China's rare earth dominance

Source: http://www.homelandsecuritynewswire.com/japanese-discovery-could-undermine-chinas-rare-earth-dominance

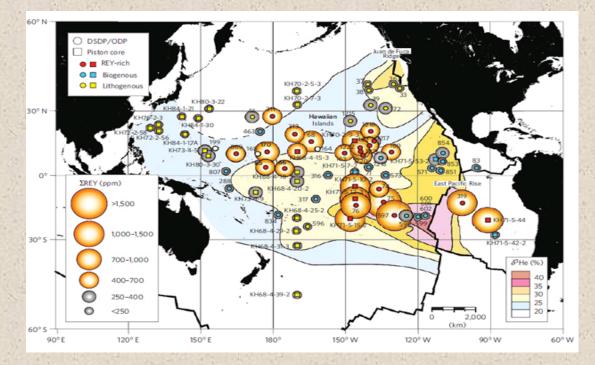
A new discovery by Japanese researchers could break China's stranglehold over rare Earth metals. Japanese geologists say they have found large deposits of rare Earth minerals on the floor of the Pacific Ocean. It is estimated that the mud of the Pacific Ocean contains 100 billion tons of rare Earth elements.

If geologists are able to mine for the minerals in a cost effective way, analysts believe this discovery could undermine China's dominance. Currently, 97 percent of rare Earth metals, and

36

produced in China, but in recent years the country has imposed strict quotas and limited exports disrupting the global supply chain. Yasuhiro Kato, an associate professor of earth science at the University of Tokyo and the leader of the team thatdiscovered the rare earth stores, said, "The deposits have a heavy concentration of rare earths. Just one square kilometer (0.4 square mile) of deposits will be The discovery has already touched off a race as companies scramble to obtain licenses to mine for these minerals deep below the Pacific Ocean. So far Nautilus, a mining company, has been the first to obtain a license to mine the ocean floor around Papua New Guinea.

The latest discovery has also caused concern among environmentalists as mining for rare Earth metals is an environmentally damaging



able to provide one-fifth of the current global annual consumption."

The minerals were found in sea mud in seventy-eight locations at depths of 11,500 to 20,000 feet below the ocean's surface. The deposits are primarily located in international waters east and west of Hawaii and east of Tahiti.

process that results in millions of tons of toxic waste laced with corrosive acids. "There's not one step of the rare Earth mining process that is not disastrous for the environment. Ores are being extracted by pumping acid into the ground, and then they are processed using more acid and chemicals," said Jamie Choi, an expert on toxics for Greenpeace China.

#### Democracy's Cradle, Rocking the World

#### By Mark Mazower

Published: June 29, 2011 Source: http://www.nytimes.com/2011/06/30/opinion/30mazower.html?\_r=2

On June 28th, the whole world was watching Greece as its Parliament voted to pass a divisive package of austerity measures that could have critical ramifications for the global financial system. It may come as a surprise that this tiny tip of the Balkan Peninsula could command such attention. We usually think of Greece as the home of Plato and Pericles, its real importance lying deep in antiquity. But this is hardly the first time that to understand Europe's future, you need to turn away from the big powers at the center of the continent and look closely at what is happening in Athens. For the past 200 years, Greece has been at the forefront of Europe's evolution.



In the **1820s**, as it waged a war of independence against the Ottoman Empire, Greece became an early symbol of escape from the prison house of empire. For philhellenes, its resurrection represented the noblest of causes. "In the great morning of the world," Shelley wrote in "Hellas," his poem about the country's struggle for independence, "Freedom's splendor burst and shone!" Victory would mean liberty's triumph not only over the Turks but also over all those dynasts who had kept so many



Europeans enslaved. Germans, Italians, Poles and Americans flocked to fight under the Greek blue and white for the sake of democracy. And within a decade, the country won its freedom.

**Over the next century**, the radically new combination of constitutional democracy and ethnic nationalism that Greece embodied spread across the continent, culminating in "the peace to end all peace" at the end of the First World War, when the Ottoman, Hapsburg and Russian empires disintegrated and were replaced by nation-states.

In the aftermath of the **First World War**, Greece again paved the way for Europe's future. Only now it was democracy's dark side that came to the fore. In a world of nation-states, ethnic minorities like Greece's Muslim population and the Orthodox Christians of Asia Minor were a recipe for international instability. In the early 1920s, Greek and Turkish leaders decided to swap their minority populations, expelling some two million Christians and Muslims in the interest of national homogeneity. The Greco-Turkish population exchange was the largest such organized refugee movement in history to that point and a model that the Nazis and others would point to later for displacing peoples in Eastern Europe, the Middle East and India.

It is ironic, then, that Greece was in the vanguard of resistance to the Nazis, too. In the **winter of 1940-41**, it was the first country to fight back effectively against the Axis powers, humiliating Mussolini in the Greco-Italian war while the rest of Europe cheered. And many cheered again a few months later when a young left-wing resistance fighter named Manolis Glezos climbed the Acropolis one night with a friend and pulled down a swastika flag that the Germans had recently unfurled. (Almost 70 years later, Mr. Glezos would be tear-gassed by the Greek police while protesting the austerity program.) Ultimately, however, Greece succumbed to German occupation. Nazi rule brought with it political disintegration, mass starvation and, after liberation, the descent of the country into outright civil war between Communist and anti-Communist forces.

Only a few years after Hitler's defeat, Greece found itself in the center of history again, as a **front line in the cold war.** In 1947, President Harry S. Truman used the intensifying civil war there to galvanize Congress behind the Truman Doctrine and his sweeping peacetime commitment of American respurces.

to fight Communism and rebuild Europe. Suddenly elevated into a trans-Atlantic cause, Greece now stood for a very different Europe — one that had crippled itself by tearing itself apart, whose only path out of the destitution of the mid-1940s was as a junior partner with Washington. As the dollars poured in, American advisers sat in Athens telling Greek policy makers what to do and American napalm scorched the Greek mountains as the Communists were put to flight.

European political and economic integration was supposed to end the weakness and dependency of the divided continent, and here, too, Greece was an emblem of a new phase in its history. The fall of its **military dictatorship in 1974** not only brought the country full membership in what would become the European Union; it also (along with the transitions in Spain and Portugal at the same time) prefigured the global democratization wave of the 1980s and '90s, first in South America and Southeast Asia and then in Eastern Europe. And it gave the European Union the taste for enlargement and the ambition to turn itself from a small club of wealthy Western European states into a voice for the newly democratic continent as a whole, extending far to the south and east.

And now today, after the euphoria of the '90s has faded and a new modesty sets in among the Europeans, it falls again to Greece to **challenge the mandarins of the European Union** and to ask what lies ahead for the continent. The European Union was supposed to shore up a fragmented Europe, to consolidate its democratic potential and to transform the continent into a force capable of competing on the global stage. It is perhaps fitting that one of Europe's oldest and most democratic nation-states should be on the new front line, throwing all these achievements into question. For we are all small powers now, and once again Greece is in the forefront of the fight for the future.

Mark Mazower is a professor of history at Columbia University.

# World Alamanac of Islamism

Source: http://almanac.afpc.org/

The World Alamanac of Islamism is a new site by The American Foreign Policy Council, devoted to



mapping out the various Islamist movements around the world. They have a section on Europe, with details on different countries.

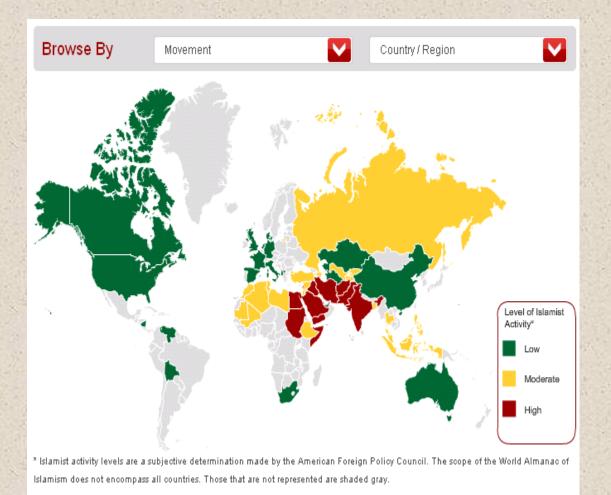
#### From their main Europe page:

Buoyed by steady immigration from the Middle East and North Africa, as well as negative native demographics among continental states, the Muslim communities in Europe are becoming larger, more complex and more vocal. Within these communities,

the past year saw Islamism continue to grow in strength as a political phenomenon.

The dominant mode of Islamist activism in Europe remains to operated within the parameters of existing political systems. Some groups, such as the Union of the Islamic Communities and Organizations of Italy, confine themselves to expanding the participation of Muslims in national politics, while others, like the Muslim Association of Britain, work to promote Islamist political thought, as well as the message and appeal of foreign Islamist groups such as the Muslim Brotherhood. Only a small minority—exemplified by England's al-Muhajiroon, among other fringe elements—has advocated violence against, and the overthrow of, European governments. Those elements are closely monitored and proscribed by the authorities in question.





# **2012 WMDFZ Conference: Assessments from Track II** Discussions Source: http://www.inss.org.il/publications.php?cat=21&incat=&read=5354

The recommendation for a conference in 2012 on a weapons of mass destruction free zone (WMDFZ) in the Middle East, included in last year's NPT Review Conference Final Document, has thus far not produced tangible progress at official levels. A facilitator has yet to be named, and more important, there is no indication of substantive progress on forging a common understanding in the region and beyond on the immediate goal of this meeting, its format, and its subject matter. The political turmoil in the Middle East over the past six months, including governments and regimes in a number of Arab states that are in a state of flux, has raised additional questions about the viability of convening such a meeting.

In contrast to the foot dragging and problems at the official level, the recommendation to hold the conference has already generated much discussion at unofficial levels, both in Israel and in broader regional frameworks. Over the course of 2010-2011 a number of meetings in the context of Track II and Track one-and-ahalf initiatives have sparked a debate over the prospects of convening this conference and a discussion of its conceptual guidelines. Some telling insights into the thinking among the different parties can be gleaned from these discussions, including the EU seminar held in Brussels in early July. Due to its broad regionwide participation, this meeting provided a good opportunity to assess an array of state approaches.

What emerges most clearly from these unofficial debates is the longstanding gulf between the positions of the two major protagonists: Israel and Egypt. Egyptian participants continue to highlight the nuclear issue almost exclusively, pointing to Israel's non-party status to the NPT as the primary – if not only – constraint to achieving a WMDFZ in the Middle East. For their part, Israeli participants continue to underscore the importance of the regional realities. that,

40

characterize the Middle East and the poor quality of inter-state relations in this region. They stress that the starting point for a WMDFZ discussion must be an effort to improve these relations, and in the first place, the ability to rely on the commitments that states make. Hence their emphasis on initiating a regional security process that draws on the notion of confidence building and step-by-step progress. Egyptian participants do not accept this logic, and the opposing positions continue to present as zero sum.

While this ongoing divide perhaps comes as no surprise, it nonetheless underscores the degree to which familiar positions have become entrenched and static, even in the face of new realities in the region, first and foremost the rapidly developing nuclear capability of Iran. There is no indication at these meetings that the highly negative regional implications of Iran's nuclear progress over the past decade have driven home to Egyptian experts where the real danger in the nuclear realm lies, or have led them to reconsider previous Egyptian positions. Amr Moussa, one of Egypt's presidential hopefuls, has stressed that there will be no change in attitudes toward Israel. In an interview with Lally Weymouth in early May he asserted, "The nuclear issue in the Middle East means Israel and then Iran."

The new factor in this round of discussions as opposed to the ACRS dynamic of the early 1990s - is no doubt the presence of Iran. At the July Brussels meeting, Iranians were not only present at the discussions, but proved to be very active participants. If this is any indication of what can be expected for 2012, it means that Iran will not stay away because of Israel's presence at the table. Indeed, the primarily bilateral dynamic that characterized the ACRS talks could turn into a trilateral Israel-Egypt-Iran dynamic this time around, with Egypt and Iran cooperating on the basis of a mutual tactical interest to focus all attention on Israel. While in one sense Egypt would no doubt draw comfort from Iran's support in finger pointing at Israel, in another sense Iran's activism would also present a challenge to Equpt, fueling the implicit general Equptian-Iranian rivalry over prominence and influence in the Middle East. Thus some of the major energy Egypt is already exerting in its campaign to have Israel join the NPT could be doubling as a message to Iran, namely, that it should take the back seat in this campaign.

If Iran joins the prospective 2012 meeting, this would create another framework for discussing its nuclear program. Thus, the "conversation" that the international community is currently having with Iran regarding evidence of its military intentions in the nuclear realm and its broken commitment to remain non-nuclear according to its NPT membership would be joined by another dialogue: a regional discussion of ridding the Middle East of all WMD. If Iran overcame its aversion to sitting at the same table with Israel, it would be in its interest to cooperate with the WMDFZ idea, as this would enable it to capitalize on the "all against Israel" dynamic, while deflecting attention from itself. One of the challenges of a WMDFZ conference in 2012 will be to keep these conversations separate and not allow Iran to hijack the 2012 format for its own agenda - namely, deflecting any plans to deal harshly with Iran's violations of its international commitments.

41

The identity of the facilitator for the 2012 conference has generated much focus at the unofficial meetings. Great expectations are being pinned to this announcement, as if it will be a concrete achievement in itself. Clearly, those who are most interested in the 2012 conference being convened need this emphasis on naming the facilitator and the host country as a means of creating an ongoing sense of activity and forward motion.

A final observation regards the puzzle of US commitment to the 2012 conference. While official statements broadcast "yes, the US is committed," US behavior on the ground, including its low profile at the Brussels meeting, seems to convey a less than enthusiastic approach. The reasons for this could have something to do with the dilemma that the conference poses as far as the strong US commitment to Israel's continued strategic advantage in light of the security challenges that it faces. The US might also be considering what the conference could mean as far as efforts to stop Iran from attaining a military capability. In addition, the turmoil in the Middle East may underscore that the region's volatility must ebb somewhat before such a discussion can be broached. At the same time, the US knows that it needs evidence of activity before the next NPT Review Conference in 2015, so it cannot entirely ignore the issue. The result of the dilemma is the ambivalence that is guite noticeable on the ground.

# Climate change ... You are responsible too!

S. M.

# BLIND DATE

BT.

## To Pay or Not to Pay? The French Hostage Dilemma

By Pascale Combelles Siegel Source: http://www.jamestown.org

After 18 months in captivity, the Taliban released Hervé Ghesquière and Stéphane Taponier on June 29. The two journalists from the French public television channel France Télévision were taken hostage on December 30, 2009 as they were working on a documentary on reconstruction in Afghanistan. The French press and the political establishment greeted the news with obvious elation. [1] The two journalists were not party to the conflict and were simply documenting history in the making. As such, the press described them as innocent pawns in a broader grand strategic game and as victims who should not be sacrificed.

However, after the relief and the selfcongratulation, the central question of "why did the Taliban release the hostages" and "what did they get in return" quickly came to the forefront of the debate.

Weary of fueling the "kidnapping-for-ransom business model," French Government officials repeatedly denied the payment of any ransom. "France does not pay ransoms." claimed Alain Juppé, the French Foreign Minister, echoed by the Elysée Palace and the Minister of Economy and Finance François Baroin (L'Express, June 30). The trouble is, nobody really believes the official version. Security expert Gérard de Villiers said that the government would deny it, but "I don't know of any hostage liberation without the payment of a ransom" (Atlantico.fr, June 30). Frédéric Helbert, a security consultant for the private channel BFM TV. went even further. Based on unnamed sources, he described in great detail how an envelope containing "several million dollars" was handed over to the kidnappers as they released the two journalists to the French authorities, exchanged into local currency and sent back to the Taliban's Quetta Shura in Pakistan (BFM TV, June 29; L'Express, June 30).

It was not the first time that France has been rumored to pay a ransom in exchange for its citizens. The London *Times*, citing Baghdad security officials "who played a crucial role in the negotiations," claimed the French government paid \$15 million to obtain the liberation of Christian Chesnot and George Malbrunot in Iraq in December 2004 and another \$10 million to obtain the liberation of Florence Aubenas in Iraq six months later in June 2005 (*Times*, May 22, 2006).

However, after his election in 2007, President Sarkozy clearly indicated that he wanted to distance his government from such practices, advocating instead a resolute opposition to paying ransoms or exchanging prisoners. In August 2009, he declared: "Paying ransoms and swapping prisoners for harmless innocents is no strategy at all," adding that France must "refuse the terrorists' diktat" (Rue89.com, January 15).

However, a closer look at the French government's practices since his election shows that the government's actions are less resolute than its words and that different circumstances yield different remedies.

- In April 2008, Somali pirates seized a French luxury cruise yacht, the *Ponant*, off the coast of Somalia. The owner of the yacht, GMA-CGM of France, paid a ransom of over \$2 million for the 30 crew members, part of which was recovered in Opération Thalatine, a raid on the pirates in the north-central Mudug region of Somalia by French Commandos marine (Naval Commandos) based in Djibouti. Six pirates were captured in the helicopter raid and brought to France for trial.
- A year later, the French government launched a successful assault on the *Tanit*, a luxury sailboat also taken off the coast of Somalia, after the pirates refused the offer of a ransom (*Times*, April 12, 2009). One hostage was killed in the crossfire during the assault by the Commando Hubert, the frogman unit of the Commandos marine, supported by French and German warships. Three pirates were arrested in the operation.
- Denis Allex is one of two Direction Générale de la Sécurité Extérieure (DGSE – French external intelligence) agents kidnapped from a Mogadishu hotel in July, 2009 (see Terrorism Monitor, July 30, 2009). Though his colleague escaped from his Hizb al-

Islam captors only a month later, Allex continues to be held by al-Shabaab somewhere within Somalia. Al-Shabaab has released two videotaped sets of demands, as read by Allex himself. In both cases the demands were political (prisoner release, cessation of French support for the Transitional Federal Government, withdrawal of African Union peacekeepers. etc) rather than financial (al-Qimmah.com, July 18, 2009; AFP, June 9, 2010). [2]

In July 2010, Al-Qaeda in the Islamic Maghreb (AQIM) announced that it had killed hostage Michel Germaneau in retaliation for a Franco-Malian raid against one of its camps in northwestern Mali (al-Jazeera, July 26). In that case, Defense Minister Hervé Morin indicated that the French Government "didn't have the slightest discussion with the kidnappers... We never had any specific claims" (La Dépêche du Midi, January 10, 2010; AFP, August 1). However, AQIM chief Abdulmalik Droukdel claimed the raid was launched while negotiations for Germaneau were underway (see Terrorism Monitor, September 23, 2010).

Finally, in January 2011, the government launched a raid to free two French citizens, Antoine de Léocour and Vincent Delory, who were kidnapped in Niamey, capital of Niger. Both were killed in northern Mali during an assault on the AQIM convoy transporting the prisoners by French and Nigérien troops (see *Terrorism Monitor*, January 28).

In contrast, the French government's attitude toward the September 2010 kidnapping of seven employees and sub-contractors of AREVA by AQIM in Niger is much more ambivalent. In that case, contacts have been established between the government and the kidnappers and a mediation team has been set up (*La Dépêche du Midi*, January 10, 2010). There are also reports that a ransom paid by AREVA secured the liberation of three of the seven hostages (Radio France Internationale, February 25). Most recently, in March 2011, AQIM released new demands asking for 90 million Euros and a prisoner swap in exchange for the four remaining hostages. The French Foreign Minister immediately rejected the ransom demand on the grounds that "we don't negotiate on that basis," indicating that the price rather than the principle of ransom is the problem (*La Dépêche du Midi*, January 10). The DGSE special fund allocation for hostage rescue operations amounts to \$53.9 million Euros for the fiscal year 2011 (*Paris Match*, July 1).

Based on this recent history, the French government does not seem to have a consistent position on negotiating the release of hostages taken by pirates or terrorist groups. Nevertheless, the French government is equipped with a dedicated bureaucratic structure, a budget, and a strong political will to engage in negotiations to secure the release of French citizens. There is little doubt that French officials do not want to encourage hostage-taking by paying ransoms - President Sarkozy has made his feelings clear in that regard. However, the collective desire to spare the lives of innocent victims taken hostage and/or to protect the economic and professional interests of large corporations clearly continues to push the government toward negotiating the release of French hostages.

In the Taliban's release of Ghesquière and Taponier in June, as well as the 2005-2006 cases of Chesnot, Malbrunot and Aubenas in Iraq, there was acknowledgement in the press that money was paid to either the hostage takers or intermediaries. There was, however, virtually no debate on the potential impact of paying ransoms to terrorist groups. The absence of discussion about the impact of paying ransoms to terrorist groups or intermediaries indicates that President Sarkozy faces a steep uphill battle if he truly wants to end French practice of paying ransoms. There remain nine French nationals held hostage in the world.

#### Notes:

1. See Prime Minister François Fillon before the National Assembly (French lower house of Parliament), 29 June 2011. Available at <u>http://www.bfmtv.com/video-infos-actualite/detail/taponier-et-ghesquiere-liberes-annonce-fillon-1426267/</u>.



The second video is available at http://www.youtube.com/watch?v=YKLtO7Zj7dw.

Pascale Combelles Siegel is President of Insight Through Analysis, a consultancy firm specializing in strategic communications, military-media, and civil-military relations research, analysis, planning, and assessment.

# Tiny flying machines revolutionize surveillance work

Source: http://www.homelandsecuritynewswire.com/tiny-flying-machines-revolutionize-surveillance-work

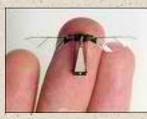
Tiny aerial vehicles are being developed with innovative flapping wings based on those of



reallife insects. Incorporating microcameras, these revolutionary insect-size vehicles will

be suitable for many different purposes ranging emergency situations from helping in considered too dangerous for people to enter, to covert military surveillance missions.

Supported by the Engineering and Physical Sciences Research Council (EPSRC),



research at the University of Oxford is playing a key role in the

vehicles' development.

Dr. Richard Bomphrey, from the Department of Zoology, is leading this research, which is generating new insight into how insect wings have evolved over the last 350 million years. "Nature has solved the problem of how to design miniature flying machines," he says. "By learning those lessons, our findings (will make it possible to aerodynamically engineer a new breed of surveillance vehicles that, because they're as small as insects and also fly like them. completely blend into their surroundings."



An **EPSRC** release reports currently that the smallest of state-of-the-art fixed-wing unmanned surveillance

vehicles are around a foot wide. The

incorporation of flapping wings is the secret to making the new designs so small. To achieve flight, any object requires a combination of thrust and lift. In manmade aircraft, two separate devices are needed to generate these (that is, engines provide thrust and wings provide lift), this limits the scope for miniaturizing flying machines.

An insect's flapping wings, however, combine both thrust and lift. If manmade vehicles could emulate this more efficient approach, it would be possible to scale down flying machines to much smaller dimensions than is currently possible.

"This will require a much more detailed understanding than we currently have of how insect wings have evolved, and specifically of how different types of insect wing have evolved



for different purposes," Bomphrey "For savs. instance, bees are load-lifters, a predator such

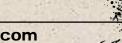
as a dragonfly is fast and maneuverable, and creatures like locusts have to range over vast distances. Investigating the differences between insect wing designs is a key focus of our work. These ecological differences have led to a variety of wing designs depending on the task needing to be performed. It means that

vehicles new could be customized to particular suit ranging uses exploring from hostile terrain,



collapsed buildings or chemical spills to providing enhanced TV coverage of sports and other events".

Bomphrey and his team lead the world in their use of both cutting-edge computer modeling capabilities and the latest high-speed, high-



resolution camera technology to investigate insect wing design and performance.

Key to the work is the calculation of air flow velocities around insect wings. This is achieved

placing bv insects in a wind tunnel, seeding the air with a light fog and illuminating the particles with pulsing laser light - using a technique called Particle Image Velocimetry. The release notes that the team's groundbreaking has work attracted the attention of the perfect way of exploring all kinds of dark, dangerous and dirty places."

Bomphrey is using his EPSRC-funded Fellowship to pursue this research. The



NATO, the U..S Air Force, and the European Office of Aerospace Research and Development. The research is expected to produce findings that can be utilized by the defense industry within three to five years, leading to the development and widespread deployment of insect-sized flying machines within twenty years.

"This is just one more example of how we can learn important lessons from nature," says Bomphrey. "Tiny flying machines could provide fundamental aim of the work is to explore how natural selection has impacted on the design of insect wings and how these designs have been affected by the laws of aerodynamics and other physical constraints.

"Evolution hasn't settled on a single type of insect wing design," says Bomphrey. "We aim to understand how natural selection led to this situation. But we also want to explore how manmade vehicles could transcend the constraints imposed by nature."

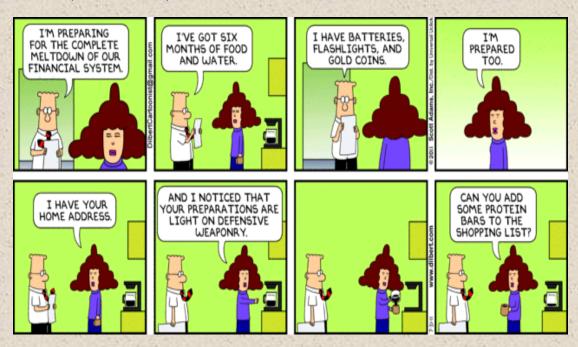
Particle image velocimetry (PIV) is an optical method of flow visualization used in education and research. It is used to obtain instantaneous velocity measurements and related properties in fluids. The fluid is seeded with tracer particles which, for sufficiently small particles, are assumed to faithfully follow the flow dynamics (the degree to which the particles faithfully follow the flow is represented by the Stokes number). The fluid with entrained particles is illuminated so that particles are visible. The motion of the seeding particles is used to calculate speed and direction (the velocity field) of the flow being studied. Other techniques used to measure flows are Laser Doppler velocimetry and Hot-wire anemometry. The main difference between PIV and those techniques is that PIV produces two dimensional or even three dimensional vector fields, while the other techniques measure the velocity at a point. During PIV, the particle concentration is such that it is possible to identify individual particles in an image, but not with certainty to track it between images. When the particle concentration is so low that it is possible to follow an individual particle it is called Particle tracking velocimetry, while Laser speckle velocimetry is used for cases where the particle concentration is so high that it is difficult to observe individual particles in an image. Typical PIV apparatus consists of a camera (normally a digital camera with a CCD chip in modern systems), a strobe or laser with an optical arrangement to limit the physical region illuminated (normally a cylindrical lens to convert a light beam to a line), a synchronizer to act as an external trigger for control of the camera and laser, the seeding particles and the fluid under investigation. A fiber optic cable or liquid light guide may connect the laser to the lens setup. PIV software is used to post-processes the optical images.



46

# Preparedness

Source: http://dilbert.com/strips/comic/2011-07-31/



### Growing menace: animal-rights terrorism

Source: http://www.homelandsecuritynewswire.com/growing-menace-animal-rights-terrorism

The phenomenon of increased violence committed by some extremists in the name of



animal rights is a growing cause for concern. In a major conference organized by Europol and Eurojust, fifty-eight experts from law enforcement and prosecution authorities, plus representatives from thirty-five private sector organizations, met last week at Europol's new headquarters in The Hague to discuss the issues behind this new trend.

Europol says that while the defense of the rights of animals and their welfare is legitimate and fully supported by European Union institutions, the increase in violence by extremists remains a concern for all of the conference participants. An example is the increased use of Improvised Explosive Devices (IEDs) and Improvised Incendiary Devices (IIDs).

Violent animal rights extremists do not hesitate in sending threatening e-mails or making warning phone calls to their targets, often intimidating their family and committing physical assaults on their property, in so-called home visits. This has resulted in arson attacks on cars and property.

Single-issue extremist groups are also actively targeting the fur and pharmaceutical industries. This has included the mass release of animals and the destruction of feeding and water installations for the animals. Another tendency is that single-issue extremist groups (including anarchist groups) are supporting each others' causes more and more.

"The conference at Europol's new headquarters was an important milestone in these efforts." says Rob Wainwright, director of Europol.

Together with a tactical meeting held at Eurojust in April 2011 on the same topic; the

47

conference clearly identified the need for a wider exchange of information to provide the member states' authorities with a clear picture of ongoing criminal activities. There is a tendency to underestimate the importance of the phenomenon and of the links between criminal actions committed in different countries. Forensic analysis clearly demonstrates that some attacks committed in

the EU have used the same modus operandi and that the devices used are similarly manufactured.

From the discussions at the conference, it became obvious that the violent criminal activities are often orchestrated at an international level. To this end, speakers said there was a need for increased law enforcement coordination at an international level, as well as more awareness on a local police and judicial level.

The conference recommendations include:

- Encouraging member states' authorities to prevent and fight all forms of violent criminal extremism and developing, at an EU level, a renewed dialogue on animal protection and animal welfare to allow all concerned parties to express their needs and concerns in a democratic way
- Exploring the possibility of sharing technical data with the relevant parts of the

corporate security community and their branch organizations, respecting the data protection regulations within Europol and Eurojust's existing legal frameworks

• Developing a common strategy with the corporate security community to further cooperation between EU institutions and the relevant parts of the private sector.

The above recommendations were supported



by a conclusion that called for increased information exchange with Europol and Eurojust on attacks, prosecutions and convictions in animal rights extremism cases. This will lead to the identification of good practice, increased sharing of experience and ultimately a more efficient and coordinated approach in tackling the phenomenon.

# **OBL planned to kill Obama on 9/11**

Source:http://www.dailymail.co.uk/news/article-2014988/Bin-Laden-planning-shoot-Air-Force-One-Obama-inside.html

Osama Bib Laden was putting together a team of al Qaeda operatives whose mission was to use a shoulder-fired missile to bring down Air



Force One or Marine one -- the president's helicopter - on the anniversary of the 9/11 attack; the plot was gleaned from digital

storage media picked up on 2 May at OBL's compound in Pakistan; other plots were discussed, among them flying an explosives-filled plane into a sports stadium on 4th July, and killing General David Petraeus

Targets: President Obama boarding Marine One // Source: trendite.net

Osama Bib Laden was putting together a team of al Qaeda operatives whose mission was to use a shoulder-fired missile to bring

down Air Force One or Marine one — the president's helicopter - on the anniversary of

One reason the plan was slow to go into effect was that bin Laden had been having



### the 9/11 attacks.

The Daily Mail reports that the information was gleaned from the many storage devices picked up by the Navy SEALs team that raided bin Laden's compound on 2 May. American intelligence sources said that the plan was still in the discussion phase when bin laden was killed. disagreements with his operations chief Attiyah Abd al-Rahman, on who should be included in the attack team, the Wall Street Journal reported.

This disagreement and others, intelligence officials say, painted a picture of a leader who was losing his grip over the organization he had created, with his lieutenants openly defying



his instructions.

Another plan found in the documents and digital data at the compound was to use a celebration day in the United States — for example, the 4th of July — to create a mass-casualty event by flying a small jet into a stadium during a sport even, creating a mass explosion.

Former FBI agent Brad Garrett told the Mail that despite improvements in security, the plan to hijack a small jet and fly it into a sports stadium could work.

"We have so many small airports, you could fly below radar," he said. "hat's possibly doable."

Al Qaeda's Ominous Silence

Source: http://www.thedailybeast.com/articles/2011/07/10/al-qaeda-s-ominous-silence-and-zawahiri-s-big-challenge.html

There is a puzzling silence in the global jihad that may portend a lack of confidence in al Qaeda's new leader, Ayman al-Zawahiri. side, so it often speaks out late in the game.

It's been several weeks now since Al Qaeda's core leadership in Pakistan and Afghanistan



announced that the Egyptian doctor and longtime second-in-command Zawahiri is the new emir of the terror gang. Individual Qaeda figures have come out and praised the choice. But only one of Al Qaeda's regional affiliates or franchises has publicly hailed it. Only the Shabaab al Mujahedin in Somalia has publicly signed on as a group to the decision to make Zawahiri the new No. 1.

Al Qaeda's much more important affiliates in Iraq, Yemen, and North Africa have remained mute on the choice. They have released other news bulletins, so we know they haven't suddenly come down with laryngitis. Individual members have made favorable noises, but silence has been the group response.

Al Qaeda is not collapsing; indeed, strategic patience has long been one of its strengths. The terror cell believes time is on its side, so it often speaks out late in the game. This quiet certainly does not mean there is a rebellion against the doctor. No one in Al Qaeda is publicly contesting his selection or denying his authority. And endorsements may yet come.

The newspaper notes that although at the

embryonic stage, the details of the plot lead

CIA acting director Michael Morell to tell staff that one of their top priorities was to ensure

Another plan was aimed at killing General

such an attack never took place.

David Petraeus.

Ayman al-Zawahiri has called on Americans to embrace Islam to overcome its financial crisis, which he said was a consequence of the 9/11 attacks and militant strikes in Iraq and Afghanistan., AP Photo

But there does seem to be a distinct lack of enthusiasm. Zawahiri has seemed old and tired in most of his statements this year, and he has never been a charismatic figure. He can be deadly dull when he tries to explain why Pakistan is not Islamic enough or how Napoleon tried to create Israel in 1798. Yet Zawahiri is also a ruthless killer. According to Al Qaeda, he ordered the murder of Benazir Bhutto in 2007. He helped kill seven CIA officers and a Jordanian prince in 2009 in Afghanistan using a triple agent. No one should underestimate his ideological role in Al Qaeda or his operational command.

Maybe his fellow terrorists are hedging their bets a bit, waiting to see if Zawahiri is up to the challenge of filling bin Laden's role. They've heard the Americans say Al Qaeda's core is on the ropes. Perhaps they are looking for it to strike back.

Bruce Riedel, a former longtime CIA officer, is a senior fellow in the Saban Center at the Brookings Institution. At President Obama's request, he chaired the strategic review of policy toward Afghanisten and the strategic review of policy toward Afghanisten and the strategic review of policy toward and the strategic revie

and Pakistan in 2009. He is author of the new book <u>Deadly Embrace: Pakistan, America and the</u> <u>Future of the Global Jihad and The Search for Al Qaeda: Its Leadership, Ideology and Future.</u>

# Terror cult's persistence key to WMD attack

Source: http://kstc45.com/article/stories/S2218667.shtml?cat=11584

Experts argue over how hard it is for terrorists to make weapons of mass destruction, but a new study of the doomsday cult that carried out the Tokyo subway nerve gas attack says that even seemingly marginal groups can succeed with persistence and luck.

A report on the Aum Shinrikyo cult by ex-Navy Secretary Richard Danzig and colleagues at the Center for a New Security describes the cult's often bumbling efforts to make biological and chemical weapons in the 1980s and 1990s. But the report says that the cult's persistence was key to its success in making sarin nerve agent, which it used in its deadly 1995 attack on Tokyo commuters that killed 13 and injured more than 6,000. "Terrorists need time; time will be used for trial and error ...; trial and error entail risk and, in this case, provoked disruption; but Aum found paths to WMD, and other terrorists are likely to do the same," said the report.

Japanese authorities granted Danzig and his co-authors rare access to senior cult members being held in a Tokyo prison during a series of interviews that began in 2008. Danzig told terrorism experts and others gathered to discuss the report Thursday that experts needed to understand the cult's quest for WMD in order to learn how to prevent others from doing the same thing.

Terror groups can seem "almost laughable" when they fail, Danzig said, and Aum Shinrikyo had many failures and setbacks. He cited one case where a cult devotee fell into a fermenting tank full of the bacterium that produces the botulinum toxin and nearly drowned. He was unharmed.

There was of course nothing funny about the group's successes, which included the subway attack and an earlier effort to use sarin gas to kill the judges in a commercial dispute involving the cult. The judges survived but eight people died in a nearby apartment building when the wind shifted.

Danzig compared the situation to Russian roulette. Terror groups trying to make WMD can keep shooting blanks, he said, "and then one of the chambers turns out to be loaded."

Danzig said the miniaturization of chemical equipment and the new synthetic biology, capable of producing disease-causing organisms, have only raised the risk that small groups can manufacture weapons capable of killing thousands.

But the report also said that the cult was never able to devise a way of disseminating its chemical and biological arsenal with any precision. Producing large quantities of these materials probably also remains a challenge.

The authors reported that the group struggled to make bioweapons, and it still isn't clear if it succeeded in producing deadly forms of anthrax or other pathogens. As a result, they concluded that it is probably much harder for terrorists to make biological arms than chemical weapons. "As a rule of thumb, we think that conventional bomb makers who manufacture their weapons need days, chemists need weeks, biologists need months and nuclear terrorists need years," the study said.

#### Turning sport vehicle into military machine

Source: http://www.homelandsecuritynewswire.com/turning-sport-vehicle-military-machine

Devon, U.K.-based Supacat is launching a military variant of the Rally Raid-proven Wildcat into the global defense market "to offer a high performance, off road vehicle for special forces, border patrol, reconnaissance, rapid intervention or strike roles," the company says. The company says the Wildcat will fill a significant gap that currently exists between lightweight and less expensive high mobility platforms such as quad bikes and the heavier, more specialized Jackal.



Supacat's militarized version of the Wildcat // Source: businessinsider.com

The teaming of Supacat and QT Services aims to provide race-bred capability in a fully integrated military variant of the race car at an affordable price. The transfer and modification of an entire U.K. vehicle from the motorsport



industry into a military role by Supacat may well be an industry first.

Supacat has partnered with Wildcat Design Authority and manufacturer, QT Services, to deliver a military variant of Wildcat 500 DKR, which boasts high speed performance in harsh environments for a vehicle in its size and weight class. Supacat is responsible for

militarizing the vehicle. including systems integration and volume production. A variety of lightweight solutions, armor weapons, and communications systems can be fitted to meet each customer's requirements. Supacat will be displaying a militarized variant of Wildcat at DSEi in September. "Wildcat's rugged and high performance profile is an ideal fit with Supacat, given our unrivalled pedigree in high mobility military vehicles with outstanding off road performance, such as Jackal, Coyote and the SPV400", said Jamie

Clarke, Sales and Marketing Manager, Supacat. He continued:



"Compared to other 'Modified Off The Shelf' vehicles, the Wildcat is on a different level in terms of performance and durability. It has the race results to prove it can perform in the desert and other environments, it is light and agile yet big enough to carry the sub-systems required on operations. As military vehicles have become heavier and more expensive due to increased protection requirements, we perceive that there is a gap in the market for a platform like the Wildcat. We have a history of successfully using the motorsport industry to enhance our current products, hence Jackal has over 14 motorsport companies in its supply chain. However this is the first time we've taken an entire platform from the racing sector and marketed it into defense. It's very exciting!".

The Wildcat has a tubular space-frame chassis and state of the art suspension with a reputation for rugged reliability. With a Gross Vehicle Weight of 2580kg and size (3800mm x 1755mm) it is air portable. Maximum speed is 106 mph (170km/h) and range is 2000km. The Wildcat is available with specially developed air conditioning to reduce crew fatigue. It also shares some parts with Land Rover so the logistic footprint is reduced for any military



customer who already has Land Rovers in service.

QT Services's Managing Director, Dave Marsh commented, "we are delighted to have reached this agreement with Supacat. We are two U.K. companies based in the South West who share a similar ethos; our companies are a good cultural fit. The Wildcat fits in well with Supacat's existing product range of high performance vehicles and we're very much looking forward to tackling new markets with a well-proven product".



Climate change ... You are responsible too!

# Preparing for the worst

Source: http://www.homelandsecuritynewswire.com/preparing-worst

Nearly three quarters (73 percent) of companies surveyed by AT&T are calling business continuity a priority in 2011, and almost half of them are seriously thinking about using cloud technology to help them deal with terrorism threats, security breaches, the problems that come when the power goes out or the weather turns extreme.

The business continuity survey results were released yesterday, and AT&T conducted its first ever London-based Network Disaster Recovery (NDR) Exercise – which the company said allowed it to practice and share its know-how in handling network and customer disruptions. Télécoms Sans Frontières, the leading international humanitarian organization specializing in emergency communications, also demonstrated its equipment and best practices, deployed in response teams to disasters around the world.

The survey shows that such preparedness is not just for theoretical threats – almost a third (27 percent) of the firms surveyed said they have had to use their own disaster plans for real to deal with such diverse threats as power outages, extreme weather events or IT failures. In major cities like London, the threat posed by natural disaster, terrorism, and security threats is never far from executives' minds.

The survey of London businesses reveals an increasing role for cloud technologies as a way of delivering business continuity:

• Business continuity is seen as a priority for 73 percent of IT executives in the London area and 85 percent plan to invest in new technologies in 2011.

- 45 percent of executives use or are considering cloud computing as a means of delivering improved business continuity – and another 21 percent are planning to invest in cloud computing this year
- Investment in new technologies is motivated by business growth (27 percent), increasing productivity (25 percent) and reducing costs (21 percent)

AT&T's NDR exercise demonstrates its business continuity and disaster recovery services. Through simulating the response to large-scale disasters and network service disruptions, the NDR workforce test processes, skills, and technologies – improving best practice for restoring critical communications. Onsite will be a command and control center and mobile disaster recovery units designed to replicate the AT&T network. The equipment is designed to be deployed by air or ground transport.

"AT&T believes it is important to run these disaster recovery demonstrations in the field and we also take the time to understand what customers' concerns are around network readiness and preparedness," said Mark Francis, vice president, AT&T Global Network Operations and Network Disaster Recovery. "We've found that U.K. enterprises appreciate the need to invest in preparedness and are realizing that cloud computing will play a vital role in delivering this without compromising performance."

# **IACSP CD High Risk Environments Survival Checklist**

Source:http://www.iacsp.com/pay\_pal/fax/payment.php?id=IA302

As U.S. and coalition forces, corporate employees, and contractors continue to surge overseas for both operational and commercial trips, there is an urgent need for up-to-the minute, validated, credible personal security and survival information on what to do and how to get ready. Seven years in the making, the High Risk Environments Survival<sup>™</sup> (HRES) Checklist is an electronic reference document providing information, resources, and inputs covering all of the key areas for taking a trip overseas to a high-risk area.

What you need to know, where to get more information, what to train on and where, and what to bring are all covered in this resource document. Over 40 pages of pertinent information culled from nearly 20



years of experience and research from a variety of sources and IACSP hands-on professionals to include Tactical Trainers, Special Forces Soldiers, who have served in the Global War on Terrorism, Corporate Security personnel, etc. Every inch of this document is packed with information. It can be pocket pc/PDA, or printed in color as a complete manual. We viewed on your computer or

much of this as possible in one place, having at your fingertips what you need to "know before you go."

Equipment, clothing, how to make a "go bag", medical prep, security preparations, personal protection items, open source intel resources, excellent reading, where to obtain free antiterrorism/personal protection manuals, weapons accessories, recommended personal training, complete

listing of driving/shooting/fighting/protection schools, and how to prepare for the culture and situations you about to visit ....

Sent to you as a ready to use PDF file, the checklist includes over 200 hundred website links that you can

on immediately, taking you directly to the services, products, training, downloadable manuals, information resources that you need to plan

for and prepare for your trip.

have gathered as

are

click

This checklist is designed to save you many hours of time, much effort, money, and even possibly your life.

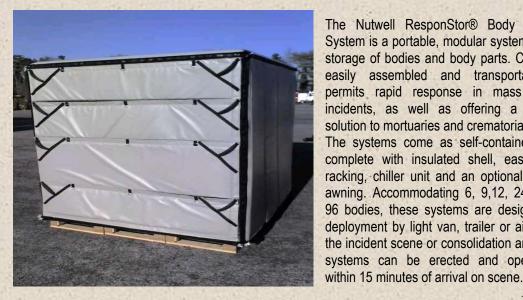
#### Intended Audience / Who This Material Is Applicable To:

The IACSP HRES Checklist applies to all of the following: military personnel, security professionals, contractors, government civilian and law enforcement, NGO's, and journalists. Business persons and vacation travelers will also find much in this checklist that will make their trip safer, healthier, and more successful.

Whether you have advanced skills or experience in operating overseas, or are preparing for your first trip. or are getting ready to head to a hostile area overseas, the positive feedback from users of this document is a testimony to the importance and urgency of acquiring the IACSP HRES Checklist before you head out.

# Nutwell ResponStor® Body Storage System

A portable, modular system for the storage of bodies and body parts Source: http://www.responstor.com/index.html



The Nutwell ResponStor® Body Storage System is a portable, modular system for the storage of bodies and body parts. Compact, easily assembled and transportable, it permits rapid response in mass fatality incidents, as well as offering a storage solution to mortuaries and crematoria. The systems come as self-contained units complete with insulated shell, easy clean racking, chiller unit and an optional privacy awning. Accommodating 6, 9,12, 24, 48 or 96 bodies, these systems are designed for deployment by light van, trailer or aircraft at the incident scene or consolidation area. The systems can be erected and operational



www.cbrne-terrorism-newsletter.com

55

#### Advantages of this system:

- ☑ 6/9/12-body units expandable to 96 bodies
- ☑ Climate controlled, energy efficient
- ☑ Space-saving, flat-pack storage
- ☑ 15-minute assembly, no tools needed
- Ergonomic design meets NIOSH lifting standards
- Exerts a small, low-pressure footprint
- ☑ 100% safety margin on sprung flooring
- Highly mobile, lightweight and resilient
- ☑ Cost effective purchase or lease



#### **Fifteen Million Plastic Bags**

Source: http://www.cbrneworld.com/pdf/cbrne-world-spring-2011-fifteen-million-plastic-bags.pdf

www.cbrne-terrorism-newsletter.com

Once upon a time the issue of contaminated body disposal was a very real concern for governments, faced with the possibility of even limited nuclear strikes there had to be some form of solution, even if only to ensure that 'the radiation won't spread.' Yet post-Cold War, along with the bunkers, this issue just went away, as it was no longer going to be a problem. Except that was not the case... Many terrorist attacks across the world had never really stretched the system, tens or even a hundred fatalities could be absorbed by the system, and all the emphasis looked to the first parts of the problem, the prevent and protect part. Even the prepare element didn't like to focus on the issue of mass fatalities because it was seen as too pessimistic and moribund. The alarm went off on Boxing Day 2004 for many countries, when the Aceh Tsunami hit the major tourist resorts of South East Asia (as well as the non-tourist resorts), and many nations suddenly found that they had a large amount of bodies coming in-country, in various states. Suddenly there was a modern need for



the sorts of facilities that had once been in place, cold storage, forensic identification, psychological counselling etc., and it was needed NOW!

Following this was the Hurricane Katrina disaster, which also drilled home the same lesson – but albeit a lower priority one in that it was a localised disaster, and there is no doubt that the same lesson is being learned in Japan. Yet while the template for natural disasters, terrorist attacks and CBRN incidents overlap to

need to enhance what was there, and we provided a two year study to the point where there was a concept demonstrator of the module: to allows for autopsies to be conducted, where body bags can be opened in a negative pressure environment and safely stored. When you need to close the bag then it and the operator have to undergo thorough decontamination before it can be safely stored, and you need the ability to check that the bag is as clean as it can be, that it is not going to



a large extent, they are important differences. Natural disasters rarely have the encumbrance of evidence, while CBR fatalities have both the evidential requirement and a far higher contamination concern than conventional attacks. While biological attacks are a concern, in terms of large amounts of fatalities, the attendant problems diminish when compared to the challenges of radiological or even chemical incident.

Following on from the Aceh Tsunami, the UK government placed a contract with Kellogg Brown and Root (KBR) as part of the National Emergency Mortuary Arrangement (NEMA) to be able to provide a turnkey capability, as Dave Butler, KBR's CBRN Technical Delivery Manager, explained, "KBR have the ten year contract for NEMA, they manage the arrangement on behalf of the Home Office and as part of that we conducted a piece of our own work to look at a CBRN module to complement the NEMA arrangement; a KBR initiative with no requirement from the Customer. We identified what we saw as a capability gap, a cross contaminate. We needed the system to be mobile and modular and to be set up in a street in London, as opposed to a greenfield site." Mr Butler suggested it was this need to have evidence that was a game-changer for the forensic community as it meant that they could not rely on the traditional computerised tomography (CT) scan that they usually do. "What we have seen previously is that contaminated bodies are wrapped in bags at the scene, decontaminated and then brought in from there," he said. "From that moment on the concept is that the bag is not opened, it undergoes the CT scan inside the bag. There are differing opinions as to whether all the Disaster Victim Identification (DVI) can be acquired from a CT scan, and the pathology world has different opinions on that. In terrorist incidents there may be a requirement to open the bag again to either take samples for further analysis or evidence, you may want to remove contaminated shrapnel from the body for example - so there are various reasons why you may want to open the bag while

previously there was no capability to do this. So we came up with a negative pressure autopsy suite, whereby the bags can be opened, the pathologist can work there in suitable PPE and then do the bag up again, and the pathologist and the bag can undergo a thorough decontamination.

The question came up about crematoriums with suitable filters to dispose of CBR bodies. So we took part of the study to a technical specification level, a mobile crematorium, housed in 5 ISO containers which has the capability to cremate the body, filter the fumes and render the ash clean. We concluded that it may be possible to provide the ashes of the person to their next of kin. There were some concerns after London's 7/7, from the next of kin, about whether they could see their loved ones and say goodbye, take their ashes etc., and with a CBRN event that becomes even more difficult." Yet while the UK is still at the technology demonstrator stage, the US has actually rolled out a capability.

The US operates the Disaster Mortuary (DMORT), a DHHS Response Team programme designed to assist local authorities in a mass fatality incident which has overwhelmed their capability. The DMORT consists of three core groups, the Disaster Portable Morgue Unit, Family Assistance, and the WMD Team, and the core component of these teams are: Medical Examiners, Pathologists, Funeral Directors, Mental Health specialists, Evidence Specialists, Technical Specialists (Fingerprints, DNA, Odontologists, Photographers, etc.), as well as admin support. The DMORT is a specialised turnkey capability, including personnel and materiel, and within this perhaps the most specialised is the WMD Team, led by Dale Downey. Much like the UK system it became apparent to the DHHS that there would be capabilities that were needed for a CBRN attack that would be unique and perhaps outside the normal remit of both the The Joint Program Executive Office for Chemical and Biological Defense (JPEO CBD), in the US, did have an ambitious programme for fatality decontamination - the human remain decontamination system. This came in three parts, the contaminated human remains pouch, the remains decontamination system and the transportation and storage container. Elements of this were supposed to be completed in a 2008-2010 timeframe, especially the human remains pouch, which

local authorities and the normal DMORT. "The idea was that if there was a CBRN event, there could be fatalities involved," said Mr Downey. "Given the need for special handling of the dead, i.e., chain of possession, evidence retrieval, etc., people trained in the proper and legal handling of the deceased should be the ones who decontaminate them as well. DMORT is usually called out when the community is overwhelmed by the number of dead. The same holds true for DMORTWMD as well. With CBRN, however, the numbers do not have to be large to overwhelm the 'capabilities' of the community. DMORT-WMD has the same disciplines as a regional DMORT, but with extra training in CBRN and HazMat etc. The National Medical Response Teams (NMRT) have also been crossed trained with DMORT-WMD so that in the event of a huge scale event, or a multiple location event, they can be assigned to DMORTWMD and function alongside the fatality subject matter experts to decontaminate and recover remains. " Decontamination and human remains is always a tricky subject as the natural putrification is in itself a bio-hazard, so how do DMORT classify decontamination? "There is only one way to truly decontaminate the inside of a human and that is by embalming, which is possible for this team to perform, but not really necessary," explained Mr Downey. "All remains are always handled for burial or cremation as if they are contagious already - universal precautions - and our level of clean for radiation is twice background or less, while for chemicals it is to a degree where they would not cause any issues with a person using proper PPE. Most chemicals are easily neutralized, and our team has the experts to determine what agent we use to decontaminate according to the contaminant; we do not practice 'cookie cutter decontamination." Yet these are both civilian systems, what about the military? Sadly they are not so forthcoming. was looking at some military off the shelf solutions (MOTS). In fact there are already some products out there that claim to do this -Remploy Frontline, for example, have one - yet despite this there has been no procurement. Indeed JPM Decontamination have dropped the other two elements of the programme and only the pouch remains - still touted as a potential MOTs solution. We put a request for information into the JPEO in February but they were unable to provide a response in the four

weeks before print – so exactly why the DoD cannot provide a system analogous to ones already existing in the civilian field is not known. With past, present and future operations likely to be in a high threat CBR environment it is worrying to know that there seems to be a low priority for the potential repatriation of fatalities. One thing is for certain, as 'Public Enquiries' become the norm for any terrorist attack there will be greater scrutiny on the elements that the public are going to be concerned about. Much of the Prevent work – the legislation, the intelligence operations – is going to be behind closed doors, and their emphasis is going to be on the protect piece –

# Hospitals in the Holy Land

# By Dorit Zimerman

Source: CBRNe WORLD "Summer-2011" issue

Hospitals in Israel have always been prepared for large scale terrorist events as well as fullscale war, but since Saddam Hussein threatened Israel with biological warheads on ballistic missiles in 2001, hospitals have been preparing for CBRN situations as well. This is something that has been taken very seriously, and as a country that not only runs emergency training sessions for the public, but also



provides its entire population with gas masks, we can be sure that Israel has a handle on CBRN events.

Dr Meir Oren, Director General of the Hillel– Yaffe Medical Center in Hadera and Chairman of the National Advisory Committee for Extraordinary Biological Events within the Ministry of Health,

explains that hospital preparedness is part of the over-arching Israeli 'all-hazards' approach, building on the conventional mass casualty incident as the basic model of preparedness. As such, all decontamination takes place at what happened immediately before, during and after the attack. End Ex usually happens once the last person has cleared decontamination (the protection of the living takes priority), yet for many the care for the deceased is going to be a prime concern (this is currently a #1 Priority in the aftermath of the recent tsunami). Not only is this event not being practised for, in many cases it does not exist – it will try to be put together on the day. The US, as they often do, is leading the way in this, as their experience of natural disasters is making it a prerequisite, but quite how many will heed their lessons is another matter.

hospitals, rather than setting up facilities at an incident site. Almost every hospital in Israel has fixed decontamination facilities for both small scale incidents, like hazmat and industrial chemical accidents, as well as for full-blown CBRN warfare. The same facilities will serve for decontamination no matter what is the offensive agent - chemical, biological or radiological. CBRN events obviously pose a more complicated challenge for hospitals, from ensuring that personnel are always on a high level of alert to identify the agent used, to dealing with the 'worried well,' but this ability to have everything on the ready and under one roof diminishes what could be a logistical nightmare. Hospital decontamination takes place outside, generally in the hospital parking lot, with about 20-30 decontamination showers, however, this can be increased



tremendously in case of chemical warfare. All patients are decontaminated in these showers, using detergents, and with the help of PPE clad



hospital staff. After transport and decontamination, the clean patients will be brought inside and start a one-way path to complete assessment and care. The aim is for patients not to return to the emergency department, but rather flow forward to discharge.

#### Triage

As Professor Shmuel Shapira, Deputy Director General of the Hadassah Hospital in Jerusalem and Director of Military Track Medicine at the Hebrew University Hadassah School of Medicine, explains, generally the triage for such events are very simple: three classes; first the ambulant, who are able to walk (meaning only mildly affected): second the non-ambulant. that need to be carried on stretchers; finally those who need airway maintenance and Ultimately, moderate ventilator support. casualties have the highest priority for evacuation to hospitals, followed by severe casualties. According to the standard operating procedure, death is only declared after decontamination, but Professor Shapira feels that in reality this will not be feasible during a major incident and death will be declared beforehand. A greater dilemma, however, is performing 'triage' on self-referrals at the front gate. As a result, a Home Front Command military unit, also incorporating paramedics, would be present at the gates of the hospital campus to perform an initial triage to stop the 'worried well' taking over precious hospital resources as well as issuing antidotes to those who are only mildly injured. A minute number of victims will, however, manage to penetrate this barricade, especially at the start of the crisis, before hospitals have been informed of the situation. Professor Shapira explains that when this happens, one should either take them outside and decontaminate them as usual, or place them in an isolated department for immediate decontamination with water and sponges. If, however, they are suspected to be contaminated, even before the hospitals are aware of the situation, they won't be allowed in and a decontamination team will be sent outside to deal with them. Ultimately, the speedy self-arrival of mildly wounded will be the first indication that a CBRN agent has been used, which is why it is so important that hospital staff are trained and able to perform a near instant identification of agents. This, however, is not always easy, especially if

victims are not displaying classic chemicalbased symptoms, or if wounds are masking the signs, so working on suspicion and gutfeeling is important. Once ambulances start arriving en masse at hospitals with the victims, there is a fear of a 'bottleneck' scenario, but Professor Shapira explains that there are protected medical teams in the areas of patients' downloading before decontamination, and these teams provide initial treatment and help to control the inflow for decontamination. Furthermore, as with conventional attacks, hospital staff is comprehensively trained in evacuating emergency rooms of those with non-related minor injuries, so there is sufficient space for those requiring hospitalisation post decontamination. Coupled with this, if there is a huge surge in patients or the need to increase the size of the ICU, hospitals are equipped to treat patients in the corridors, admission areas and lobbies, through the use of extra plug sockets and emergency equipment stores. These events also require the maximum efforts of the entire hospital staff at very short notice, so pre-designed contact and recruitment systems; including personal data, contact details and pre-determined roles in various situations is mandatory. Furthermore, the Hadassah Hospital, for example, has an official volunteer organisation consisting of retired people with both medical and non-medical backgrounds, who are trained to perform a variety of hospital tasks, from administration to changing bed linen and refreshing supplies.

#### Security

The Israeli response. including decontamination in hospital parking lots is very well known; as a result, much is done to protect the area from the possibility of a secondary attack and the possibility of IEDs and small arms being smuggled in. Generally, hospitals in Israel are guarded by security officers, and surrounded by fences and security cameras, each person who enters the hospital is inspected, checked and walked through a magnetometer. Even arriving ambulances are searched at the entrance to the hospital campus and at the entrance to the emergency department. During mass casualty events these security conditions still occur and there is even further police reinforcement. As such, hospital staff has a close working relationship and understanding with security personnel.

#### **Psychological Issues**

Israel is a place steeped in religious sentimentality, with a population of roughly 74 million Jews, Muslims and Christians sharing various degrees of orthodoxy. A question of major concern then is how to deal with the issues of disrobing and showering. In this situation, however, the notion of a religious divide is set aside and the concern is only for gender; where the men and women will be decontaminated separately. Furthermore. victims are not left to self-decontaminate, and will have staff members with them guiding them on what to do, which helps with any uncertainty. Teams consisting of psychologists, psychiatrists and social-workers will further provide support immediately following the acute stage, and a public communications centre will be erected away from the site to provide information to victim's families, help with the identification of unknown patients, and act as an information conduit between different hospitals involved.

perception of threats, preparation, including drills, are the cornerstones of dealing with CBRN events. CBRN drills are carried out once or twice a year, varying from chemical warfare drills with over 100 volunteers, to small simulations. The army is usually brought in the act as simulated casualties, but 'smart' simulated casualties are also used. These are paramedics, medical students and physicians who are spread amongst the simulated casualties and are able to give enhanced and insider information on the level of triage, transport and care. Coupled with this, some volunteers also act as bystanders at the scene of an incident, who then help ambulance staff with simple tasks like loading patients into ambulances and keeping onlookers away. Furthermore, much time is spent working out different methods of communications between agencies involved in case mobile phone networks fail, like volunteers used to run messages and instructions. If asked to give advice to other countries, Dr Oren insists that



#### Training

Israeli hospitals are not only well prepared for conventional attacks, but also well rehearsed in real-life instances. Although they possess the right equipment, unconventional attacks are more constraining due to the extra pressures of decontamination and identification of agents. As a result, Professor Shapira insists that amongst commitment and the correct effective preparedness for emergencies including CBRN necessitates awareness, constant alertness, determination, ambition, leadership and building capacity in advance at national, local and hospital level. This includes integrative operations, preplanning and continuous debriefing and learning. There are many logistical advantages to having fixed decontamination sites at hospitals, from easy access of skilled personnel, to the immediate.

availability of decontamination equipment with a secure water supply and instant access to hospital facilities post decontamination. The level of security also makes it a safe place to decontaminate, as opposed to the threat of secondary attacks on an incident site. Complexity does lie, however, in dealing with existing hospital patients, ensuring that the inside of the clean hospital is not contaminated, dealing with both a surge and bottleneck of incoming victims and ensuring that the hospital

### Medical complications Source: CBRNe WORLD "Autumn-2009" issue

Hospitals are very complex and robust organisations, usually very busy with day-today activity and acting under remarkable pressure from many areas, such as patients and their families, shortness of budget and limited manpower. These challenges must be met at the clinical, as well as at the organisational and economic, level; elective

activity must be performed and integrated with unexpected and unplanned emergency activity, and performance should be maintained at the highest standards. On the top of these challenges, hospitals, as well as other components of the healthcare system, must be prepared to cope successfully with various emergency scenarios. The various threats are complicated to deal with, and range from the thwarting stage at the pre-event phase through comprehensive the to response in the event and post-event phase. These scenarios may be natural, accidental or intentional, and

may be caused by terrorists. Among all these challenges, CBRN devices pose a very complicated challenge for hospitals, raising operational, ethical, medical and other issues. All these challenges are affected by the choice of agent, whether chemical, biological, radiological or nuclear. This paper will not concern itself with hospital preparedness for nuclear scenarios, however. In order to achieve a satisfactory level of preparedness, and an is prepared for all these complexities at any point of time, days, nights, religious holidays and weekends. Ultimately, Israel does have practice in mass casualty events, lots of it, as well as the confidence to assure that their way is the correct way; as Professor Shapira stated when asked about Europe's Orchids Project, "I am not aware of the Orchids project, but certainly it would be wise to consult with Israeli experts, who have years of experience with preparations and drills."

appropriate response for every scenario, the hospital management and the staff must be committed to achieving that goal, and investing in the necessary resources. Since hospitals are just one component of the healthcare system (which also includes primary care, public health, first responders, etc) they are one module among many other external "actors",



including agencies like police, fire brigade, EMS, military, media and risk communication. Hospital preparedness and successful performance is highly dependent on very close co-operation and coordination among all parties.

Hospital approach to CBRN incidents The various scenarios are so different from each other that they pose their own difficulties.



For example, there is the challenge of instilling basic knowledge among staff of the scenarios, such as chemical or biological agents and radioisotopes, as well as the organisational plan for every scenario. Maintaining a high level of constant alert at the personal level and the organisational level is also very challenging. The Israeli approach in general is an "all-hazards" approach. We tried to formulate our doctrine of hospital preparedness on a generic universal approach as much as possible. The basic module for emergency scenarios is the conventional mass-casualty incident. On that module we built the doctrine for the various scenarios: toxicological (hazmat), chemical, biological and radiological events. Regarding the biological scenario, the generic approach is preparedness for noncontagious agents, contagious agents and toxins. The doctrine for a bio event is formulated by a multidisciplinary team - the National Advisory Committee for Extraordinary Biological Events - within the Ministry of Health, and a top-down process is introduced and integrated at the hospital level, where every hospital formulates its own standard of procedures for the scenarios. Specific national advisory committees implement the same concept for chemical, toxicological and radiological scenarios. Each hospital has an emergency committee headed by the deputy director of the hospital, or one of the heads of a clinical department, who is experienced in emergency medicine and has also organisational capabilities. Other members of the committee are the deputy chief nurse, the deputy administrative director, the head of trauma unit and the chief of security. According to the specific scenario, other participants, like infectious disease consultants, epidemiological nurses and the head of the microbiology laboratory, may join the committee to deal with the event. In Israel, the hospital directors are board-certified in medical administration: they are also boardcertified in one of the clinical fields and hold either a Masters degree in economics, business administration or public health. The Emergency Committee directly reports to, and is supervised by, the CEO and Medical Director (in essence the Hospital Director). A remarkable challenge is to have the hospital staff familiar with all kinds of scenarios, agents, doctrine, standard of procedures, and achieving constant alert and readiness. In order to meet that challenge there

is a well- designed apparatus of building capabilities and assessing readiness.

### Lockdown of hospitals

Hospitals are open to the public and freely accessible to everyone during most of the day, while assuring that patients' treatment or rest is not disturbed. Mass-casualty incidents, regardless of their type, cause an extreme and outstanding situation in which we will encounter panic and extreme anxiety among families looking for relatives who maybe injured in the incident, or who are looking to receive the best possible treatment within the hospital, regardless of the number of casualties. Is it the right thing to lock down the hospital in that very special situation? Does locking down the hospital increase the already heightened level of uncertainty and anxiety of the patients and their families, or would it contribute to calming them? Is it practically possible to lock down a hospital in that situation when the level of tension is so high? Can we isolate the hospital and direct patients or casualties to alternate triage centres, such as anxiety centres or resilience centres, for example? In the case of an outbreak caused by an infectious pathogen that requires the quarantining of staff and patients, how do we manage and plan it in advance? In any case, whatever the approach, close co-operation and collaboration of the management and the security staff of the hospital, with police forces and their highest command, are mandatory in order to enable hospitals to function in these complicated scenarios. Surge capacity In Israel, every acute care general hospital is designed and planned to have a 20 per cent surge capacity of its licensed number of beds. Most acute care hospitals are public. CBR scenarios, being by nature scenarios that might engage a large number of staff from various disciplines of medicine - including nursing, paramedical professions and others - challenge us with many problems. These include: what standard of care should be provided given shortness of staff; limited availability of Intensive Care Unit (ICCU) beds and medical equipment, etc; who is in charge of taking care of patients and treating them; what capabilities are needed; whether authorisation of some procedures can be extended to medical students or nurses: who is in charge of decision-making and setting priorities - politicians, professionals at the national level, hospital CEOs or heads c

departments; who will be mechanically ventilated if there is a shortage of respirators. Who makes these decisions?

#### Manpower at the hospital level

Mass-casualty incidents require a maximisation of the efforts of the whole hospital staff, at very short notice, to perform at their best while under extreme stress with a high degree of uncertainty. Emergency events may occur at the most inconvenient time, such as during the weekend, a holiday, during the evening or at night. In that case, regular staff numbers are reduced and recruiting staff might be very difficult. Sometimes critical key persons - such surgeons, interventional as vascular radiologists or anaesthetists - may be missing, leading to "bottle neck" problems or

incompetence, and limiting the provision of comprehensive care to some casualties. It is mandatory, therefore, that at the hospital level a pre-designed recruitment system is available with updated lists and employee data and their roles in each of the various scenarios. It is critical that the communication systems, cellular phones, SMS, beepers, etc are backed up and that there is a possibility of backup manpower from hospital to hospital. In conclusion, not all problems are solved:

there are not always good or reasonable solutions. But effective preparedness for emergencies at the national level, as well as at the local and hospital level, necessitates constant alertness, control, co-ordination and co-operation, integrative operations, capacity building and pre-planning.

# Tottenham Riots: It's Time for England to Confront its Race-Related Issues



# By Lola Adesioye

Source: http://www.huffingtonpost.co.uk/lola-adesioye/tottenham-riots-its-time-\_b\_920542.html

In 2011, it's shameful that any of England's citizens feel that violence is the best way in which to express frustration. Watching live online footage of yesterday's rioting in Tottenham from America, I was thrown back to yesteryear.

This is what happened in Tottenham in 1985. Then, it was the Broadwater Farm riots which came about as a result of the death of a black woman, Cynthia Jarrett, who suffered a stroke while police conducted a search of her home. It was also what happened in Brixton that same year, shortly before the Broadwater Farm riot, when Jamaican Dorothy Groce was also shot (and subsequently paralysed) by police. I was five years old, but I remember watching the riots on TV at the time.







One would have expected that, over 25 years on, there would be more effective ways of dealing with such tensions and frustrations. The trouble is, there aren't. And while it is shameful that some of Tottenham's residents responded to the shooting of Mark Duggan by rioting, it's also disappointingly unsurprising. the police in the inner cities have not dissipated. On the contrary, suspicions are endemic. Black leadership is desperately lacking, and the country refuses to tackle these major challenges in any substantive way.

Black people - youth especially - around the country are being left high and dry. The result?



Although I am a black Britain who is based in the US, I continue to be concerned about the future of the black population in my home country. In 2011, as in 1985, the underlying issues - in particular a sense that black Britons are routinely ill treated by the establishment, the police especially - still have not been resolved. Tensions between black youth and Growing violent crime (with black men being overrepresented as both perpetrators and victims) and increasing social and political disaffection. If you re-read reports from the riots of the late 70s and 80s, the very same factors are still at work. The bottom line is that the UK still does not take its issues related to



its black British citizens seriously and it is

## paying the price.

An example of the unwillingness to confront what's really going on here is evident in the commentary that has been provided about last night's Tottenham riots. Many have talked about social disadvantage, disenfranchisement and dissatisfied youth. While that's important, they have however, missed a vital element. These riots were about more than that. These riots were about the social disadvantage, disenfranchisement and disaffection of black specifying which community they are talking

about. And while understand that "community" is a broad term, let's be straight - this riot relates mostly to Tottenham's black community, а disproportionate minority of which is, as we saw last night, enough to cause significant trouble for the rest.

Tottenham - one of England's most deprived areas - is a troubled area with high rates of violent

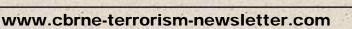
crime and poverty. But it's not just Tottenham that fits that profile. There are several parts of London that fit this type, and several parts of other English cities that do the same. This unwillingness to deal with deep rooted challenges will continue to undermine England's very progress as a supposedly melting pot nation.

Considering that black Britons have now moved from being recent immigrants to Britishborn and -raised nationals, these are not



#### people in particular.

Mark Duggan was not just another man - he was yet another black man who was shot and killed by the police. The commentators keep on talking about "the community" without issues that will go away anytime soon. For as long as England continues to be ignore or really deal with the serious issues regarding its black inhabitants, its disenfranchised ones



especially, there will be more Tottenham-like riots.

The English - and Londoners in particular prefer not to talk about race. Little weight is given to the experiences of being black in Britain, nor is racism or the intersection of race



and class discussed in any meaningful way. Many find race-related topics uncomfortable and believe them to be unnecessary. After all, England does not have US-style segregation. This ignores however, the very real and shocking statistics about what it means to be black and British today. Black children - boys in particular - continue to be at the bottom of the ladder when it comes to education. They are over represented in crime statistics and in prisons. The majority of black populations live in the UK's most deprived areas. It should not take extreme incidents like this for people to wake up to what's happening under their very noses.

This is not just an issue for the government either. As I said, black leadership has failed massively. Apart from a few like MP's David

Note: Photos were not part of the article.

# London violence raises 2012 Olympic concerns

#### By Stephen Wilson

Source:http://www.google.com/hostednews/ap/article/ALeqM5itkT8zdvH2wyJC7gWHTo7KjdaSFg?docl d=f339143394ad417abb37063a799acec1

Less than a year before London hosts the 2012 Games, scenes of rioting and looting a few miles from the main Olympic site have raised concerns about security and policing for the event. Images of buildings and vehicles in flames broadcast around the world are also Lammy and Diane Abbott, those at Operation Black Vote and some notable others, many black people are simply silent on these issues. Where are the young people coming up and saying they will not stand for this? Who are we expecting to repair this damage? Who are we

> expecting to deal with our frustrated youth? Who is setting out and outlining a vision for the future of our young people and holding anyone accountable?

> One of the things that I like most about the US something that stems from their history of having to be self reliant and fight against segregation - is that there is a willingness and a sense of duty and responsibility in some circles for black people to stand up and take

ownership and make a difference for their own. Consequently, there are prominent black leaders - activists, intellectuals, politicians and even vocal entertainers like Bill Cosby - who can be counted on to take issues to task. This is a vital, yet missing, facet among black Britons - young ones especially - that is hindering us collectively. We seem to be afraid, perhaps ashamed, disinterested or just plain unwilling to take any ownership which leaves me to ask "if not you or I, then who?"

There are some deep issues which must be handled here if we are to avoid a repeat of this type of violence. Hopefully we can use this as a teachable moment. We don't seem to have learned much since 1985. The only question is, what will be different this time around?

poor publicity for the capital as it prepares to stage the games for a third time.

The unrest, which started Saturday night in the Tottenham area of north London after a police shooting, spread closer to the Olympic complex Monday when scattered violence broke out in the Hackney area of east London. "You, can

imagine how stretched the police would be if this were to occur during the Olympics," said Tony Travers, a local government expert at the The park includes the Olympic Stadium, which will host the opening and closing ceremonies and track and field competition, as well as the



London School of Economics. "So I think this will create a worry within City Hall and the Home Office. "It's not so much that this might happen again — unlikely — as that it reminds the people in charge that while the Olympic Games are going on, any other major event is going to be complicated."

Groups of youths, many wearing hoods and masks, attacked shops and windows in Hackney. Police in riot gear were pelted with pieces of wood and other objects.

The government said more than 200 people had been arrested and more than two dozen charged over three days of trouble. Police said at least 35 police officers were injured.

Sports also felt the impact, with two soccer matches called off because police needed to focus its resources on the violence. East London's West Ham said police told it to postpone the League Cup match against Aldershot on Tuesday because "all major public events in London were to be rearranged," while south London side Charlton said its cup match against Reading was being called off "on safety grounds" on advice from the police.

Hackney is one of the five boroughs encompassing the Olympic Park, a 1-squaremile site that will be the centerpiece of the games, which start on July 27, 2012. Monday's violence took place about 4 miles from the park. velodrome, aquatics center, basketball arena, handball arena and main press and broadcast center.

Other Olympic venues are located at various sites around the capital, including Hyde Park (triathlon), Horse Guards Parade (beach volleyball), Wembley Stadium (football) and Wimbledon (tennis). There has been no violence in those areas.

For civic leaders and Olympic organizers, the violence was an unwelcome reminder of London's volatility, less than two weeks after the city celebrated the one-year countdown to the games with great fanfare.

The International Olympic Committee said it had confidence in British authorities. "Security at the Olympic Games is a top priority for the IOC," spokesman Mark Adams said. "It is, however, directly handled by the local authorities, as they know best what is appropriate and proportionate. We are confident they will do a good job in this domain."

The London organizing committee for the Olympics, declined to comment on the trouble, in what appeared to be an attempt to avoid making any links between the violence and the games.

Two police cars and a double-decker bus were set on fire Saturday, stores were looted and several buildings along Tottenham's main

street — five miles from the Olympic Park — were reduced to smoldering shells.

The unrest was sparked by a police shooting, but some blamed unemployment, insensitive policing and opportunistic looting for the worst violence the city has seen in years.

Police and politicians insisted the disorder was the work of a criminal minority and not a sign of social tensions or security lapses ahead of the 2012 Games. Britain was already preparing a massive security operation for the Olympics, but most of the attention has been on the threat of international terrorism. About 12,000 police officers will be on duty each day of the games, which have a security budget of at least \$770 million.

69

A day after London was awarded the games in 2005, suicide bombers attacked London's



The O2 arena is seen as smoke continues to rise from a Sony Warehouse, which was destroyed by arsonists in Enfield, in north London. REUTERS transport network, killing 52 people. The British government is planning for the national terror threat to be "severe" during the Olympics, meaning an attempted attack is highly likely.

Associated Press writers Jill Lawless, Meera Selva and Danica Kirka contributed to this report.

# London riots: how BlackBerry Messenger has been used to plan two nights of looting

Source:http://www.telegraph.co.uk/technology/blackberry/8688651/London-riots-how-BlackBerry-Messenger-has-been-used-to-plan-two-nights-of-looting.html

This weekend's disturbances in parts of London have again raised questions about the role technology can play in helping crowds to gather and organise. During the Arab revolutions earlier this year, attention focused on Facebook and Twitter, but for the looters and rioters of Tottenham, Enfield and Brixton, the communications tool of choice has apparently been BlackBerry Messenger (BBM). It appears to have acted as their private, encrypted social network over the past two nights' violence. RIM's BlackBerry smartphones are very popular among inner city youths on both sides of the Atlantic. The devices themselves are typically cheaper than Android models and the iPhone, particularly on pay-as-you-go packages. But it is software that central to BlackBerrys' success in this market. BBM is an instant messaging application, allowing users to communicate in a similar way to text messaging, but effectively for free, as traffic is exchanged via the internet. According to analysts it is replacing text messaging among young people. "We've seen SMS usage fall among young people and the main driver is



ISTOCIENT OF ASSAULT

BlackBerry," said Graham Brown of Mobile Youth, in April.

Each user has a unique PIN that allows other BBM users to contact them. BBM PINs are typically shared more readily than phone numbers, which means news can spread through the network more quickly than via text

messages. For authorities aiming to track disturbances this via technology, it presents problems particular compared to public social networks like Facebook and Twitter. While chatter in public can be monitored in real time using fairly simple software - and the Met has such capabilities - BBM conversations are more secure.

Messages are strongly encrypted using an algorithm called Triple-DES, which makes them unintelligible to observers. BBM can be intercepted and deciphered more easily than say, BlackBerry email, however, because all devices share the same cryptographic key. In the words of Crackberry.com, "although PIN-to-PIN messages are encrypted using Triple-DES, the key used is a global cryptographic 'key' that is common to every BlackBerry device all over the world". "This means any BlackBerry device can potentially decrypt all PIN-to-PIN messages sent by any other BlackBerry device, if the messages can be intercepted and the destination PIN spoofed."

Within the British security apparatus, such technically-challenging spy work is carried out by GCHQ in Cheltenham and requires a warrant from the Home Secretary. Whether authorities would consider using such a resource – normally concerned with international terrorism and espionage – to spy

on youths looting Foot Locker seem unlikely.

RIM Alternatively. can be legally compelled to hand over decrypted versions of BBM conversations, but it would be too slow a process to be useful while disturbances were ongoing. Finally, and perhaps

most likely, police could go "undercover" on the BBM network, aiming to befriend ringleaders and gather intelligence. At time of writing, evidence for the use of BBM, a legitimate technology, by rioters in London is anecdotal. But given its popularity among the relevant section of society, and that the attention now focused on it seems fair. Facebook and Twitter have meanwhile played their usual role in major events in Britain, that of forums for breaking news, rumour and instant reaction. While Arab youth used them to spread ideas of openness as well as organise their actions, the mindless destruction and theft in London is orchestrated away from public view.

# Islamic extremists seek to use U.K. riots as distraction for terror attack

Source:http://www.canada.com/news/canada-in-afghanistan/Islamic+extremists+seek+benefit+from+ Britain+riots+Watchdog/5236593/story.html

Islamist extremists are trying to capitalize on the riots engulfing Britain, calling on their followers to help incite further violence so that a terror attack can be launched amid the chaos.

Via "jihadist" websites, the extremists say English-fluent Muslims should infiltrate social media with messages that encourage the rioters so that the police remain "preoccupied" by the disturbances, according to the Washington-based monitoring group SITE. The extremists are characterizing the violence as "useful" for London-based terror cells, saying the rioters are young and impressionable, and can be easily manipulated if the messages appear to be the sort of things they would write.

The extremists reason that by extending the violence, the police will drop their guard against jihadist terror planning.

The increased chaos could also force the British government to withdraw troops from Afghanistan, some of the sites say.

"The events in London are an opportunity for the mujahedeen to make a move in London and attack," says one prominent entry, adding that continued violence "may weaken the position of (the British) staying in Afghanistan, because the soldiers will be needed in London."

The riots spread after Saturday night when a small protest over the police shooting of Mark Duggan, a 29-year-old suspected gang member, escalated into violence.

"We are all Mark Duggan" and "The people want punishment for the killers of Mark Duggan" are among a string of slogans another jihadist site provides as examples it is seeking from English-speaking Muslims. want a dignified life." Yet another — "A call for free people of Britain to stop racism" — is a clear reference to the fact Duggan was black. "We ask the brothers who are fluent in the English language to write a number of inciting sentences (at least ten sentences or phrases) and post them here in the subject," the site says. "We will do the rest with permission from Allah."

Other sites call for English-speaking followers to post slogans directly, with one providing a list of Facebook addresses, mainly of prominent English soccer clubs, including Manchester United, Chelsea and Liverpool, and also of British universities.

One site expresses the hope that the riots will



Smoke billows from a Sony Centre warehouse in Enfield, north London in this still image taken from footage, August 9, 2011. Thousands of policemen prepared to deploy on London's streets on Tuesday night to head off rioters and looters who have rampaged through parts of the British capital virtually unchecked for the past three nights. REUTERS/BBC/ITN Helicopter via Reuters TV - Photograph by: REUTERS/BBC/ITN Helicopter via Reuters TV

Other examples mimic typical slogans of the political left in Britain, such as "No to favouritism and austerity" and "The people

escalate to mirror the "Arab Spring" demonstrations that have swept the Middle East and North Africa, toppling some regimes. "Just as they supported the Arab revolutions through Facebook and Twitter, and elsewhere, we want to export these revolutions to them," this site says. "Enter their pages . . . and spread photos of their revolution and incite them to continue. Make video clips of their protests and heroic acts."

This site posts a picture of three masked youths, the centre one holding the Union Jack, as smoke surrounds London's Big Ben. "Welcome to London and Europe: Spring.

Revolutions World," the picture is titled. "Those who are demonstrating are mostly young people, and it is easy to make use of their enthusiasm," the site adds cynically. In the absence of opening the way to a terror attack, efforts to encourage more violence may

# Taking no chances

#### By Chief Superintendent Brian Kelly

Source:http://www.publicservice.co.uk/article.asp?publication=Home%20Affairs&id=515&content\_name =Security%20and%20Counterterrorism&article=16897

On Wednesday 6th July 2005, Jacques Rogge uttered the words: "The Games of the 30th Olympiad in 2012 are awarded to the city of...London."

These words triggered celebrations across the UK, but were also the green light for people in many areas of Olympic and Paralympic Games planning to begin programmes of work to put into place the infrastructure, technology and other activity required to host a safe and





#### LONDON 2012 OLYMPIC SAFETY AND SECURITY STRATEGIC RISK ASSESSMENT (OSSSRA) AND RISK MITIGATION PROCESS

SUMMARY VERSION 2 (JANUARY 2011)

#### memorable Games.

The London Host City Contract includes commitments from the Prime Minister, Home Secretary and Chancellor of the Exchequer to take the measures necessary to guarantee the safety, security and peaceful celebration of the Games. More than 14,000 athletes from 205 achieve other jihadist aims, according to a supporter of the jihadist entries. "One of the goals of this workshop is to exhaust the economy of the British government," the supporter says, according to SITE.

nations are expected to attend London 2012, and over nine million tickets will be sold to spectators. It is easy to appreciate the degree of planning now required. The Games are a global event, and the eyes of the world will be on the UK.

Delivering the overlay required to meet the government's guarantee of a safe and secure Games is a massive undertaking and will involve one of the largest peacetime police and security operations ever mounted in the UK. The UK is hugely experienced in hosting and policing major events, and this no doubt contributed to the decision to award the Games to London. Nevertheless, significant challenges lie ahead, and none of us will forget the tragic events of the day after we won the right to host the Games, when London was victim to a series of terrorist bombings.

Ministers overseeing the preparations for the Games have agreed a risk-based and intelligence-led 2012 Olympic and Paralympic Safety and Security Strategy, with the overarching aim to deliver a safe and secure Games in keeping with the Olympic culture and spirit. This is a single vision shared by the aovernment, the emergency services, the London Organising Committee of the Olympic and Paralympic Games (LOCOG) and the Olympic Delivery Authority (ODA). In the context of this strategy, 'safe' means the protection of people and property from hazards caused by non-malicious incidents. 'Secure' means the protection of people and property from threats caused by incidents and attacks of a malicious nature. The latest version of the strategy was published in March.

Supporting the Strategy is the Olympic Safety and Security Strategic Risk Assessment (OSSSRA), which informs strategic-level decision-making and prioritisation of resources



through the identification and understanding of specific risks to the Games.

A number of planning principles and assumptions underpin all of this work:

• There must be a clear focus on ensuring the Games will go ahead in almost any circumstances;

 All delivery partners will make reasonable adjustments to business as usual to accommodate the requirements of the strategy;

Provision of security is based on existing roles, functions and processes;

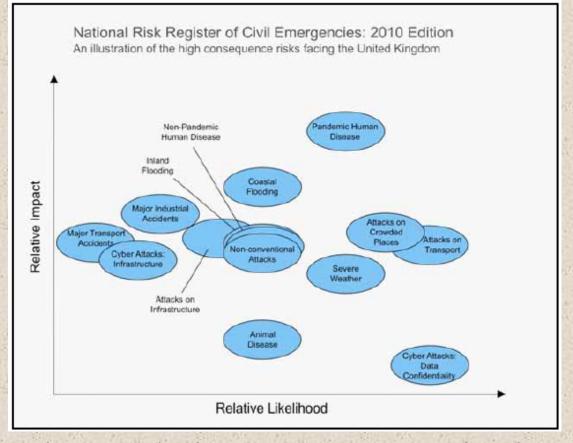
• Emergency services will maintain core service provision and the ability to respond to non-Olympic threats and hazards.

In relation to this, other than for specific activities such as the Torch Relay, the scope extends to Games time, running from July to September 2012. The OSSSRA focuses solely on those risks that fall within this timeframe, or whose impacts may not become apparent until Games time, and which are directly related to

Home Office and the Cabinet Office, which incorporates expertise from a wide range of departments and agencies. It assesses the relative severity of a wide range of potential risks, natural events and accidents – collectively known as 'hazards' – as well as malicious attacks, including terrorism, serious and organised crime, domestic extremism, public disorder and crowd management, known as 'threats'. Clearly the full range of risks and mitigation measured cannot be disclosed, but an unclassified version of the document has now been published.

The OSSSRA uses a well-established methodology adapted from the National Risk Assessment (NRA) - the document compiled by the Civil Contingencies Secretariat on behalf of the government, which considers the greatest threats and hazards facing the UK in order to inform resilience planning.

Potential threats and hazards are identified in consultation with a wide range of stakeholders



the safety and security of the Games. For example, a national pandemic would impact far beyond the Games and this would be dealt with and mitigated elsewhere.

The OSSSRA is a classified cross-government document, completed jointly between the

and through a bespoke Olympic Strategic Threat Assessment produced by the newly created Olympic Intelligence Centre. A 'reasonable worst case scenario' is agreed for each threat or hazard, which is then assessed by subject matter experts for impact\_and

likelihood. For natural events, the likelihood of something happening is based on historical and scientific evidence and forecasting. For malicious attacks, the likelihood of a threat occurring is considered by assessing the intent and capability of those who may carry out such an act, and the vulnerability of the person, place or thing that may be the intended target. Impact is assessed against a Games-specific

set of impact These criteria. include the likely number of fatalities and casualties. other 'harm' indicators including the reputational damage that may be caused to the Games or the UK following an incident occurring, and a number of 'disruption' criteria that may affect the



Games. Once assessed, risks are then mapped on to a risk matrix.

Once the risks facing the Games have been identified, the next stage is to establish Strategic Design Requirements (SDRs) for the activity that is required to mitigate that particular risk, either by reducing the potential for it to occur or reducing the impacts should it happen. This is a similar process to the development of planning assumptions derived from the NRA, but addresses the protective security work required that is over and above the resilience aspect of the NRA planning assumptions. The SDRs provide the high-level framework within which all risk-mitigating operational requirements will be set.

Of course, identifying risks and then putting measures in place to mitigate them is only part of the story. The Home Office's Olympic and Paralympic Security Directorate (OSD) has developed a Risk Reduction Assessment process (RRAt) that allows an indicative assessment of the level of mitigation achieved against each risk. Supported by a robust assurance process that ensures the delivery of all the mitigating activity planned, the RRAt considers the combined effect that 26 projects being managed within the OSD and by the police, and work being undertaken by LOCOG and partners in other safety and security agencies, will have on reducing risk. Or, to put it another way, it will identify the level of residual risk after mitigation

> has been put in place. Considerations can then be made by ministers and those charged with operational command of the safety and security overlay as to whether the level of risk remaining is acceptable and manageable. In times of austerity, the RRAt process also shows where our money is being spent and

whether we are getting best value for it, as well as providing a means of demonstrating, if funding was to change (up or down) how that might affect risk reduction.

The OSSSRA is refreshed every six months and this will become more frequent as we approach the Games. Existing threats will be assessed to ensure they are still relevant and emerging threats will be assessed and considered in exactly the same way as those already included.

The Games are first and foremost a celebration of sport. The Home Office and its partners are absolutely clear that our job is to provide a safe and secure platform upon which the Games can take place. A risk-based and intelligence led approach will ensure this is not seen as a security event with a sporting overlay. There is a huge amount of pride among those working on Olympic security at being part of this task, as well as anticipation at the opportunity to rise to the challenge.

Chief Superintendent Brian Kelly is member of the Olympic and Paralympic Security Design Team.

**NOTE:** You can download the OSSSRA Summary (Version 2) for the "CBRNE-CT Papers" section of the Newsletter's website.





and the second second

# Robots help evacuate buildings, search for trapped people

Source: https://research.cc.gatech.edu/rim/content/crisis-robots-show-people-emergency-exits

Two Georgia Tech engineers designed an emergency robot to help people evacuate buildings in an emergency; they say that emergency robots pacing the hallways and instructing people how to get to the emergency exits is a better solution than static emergency instructions placed on the wall; the robots will also search for injured or trapped people who failed to evacuate the building. may not be a good idea under the circumstances. Also, the hall may fill up with smoke, s people need to move out of them.

A Georgia Institute of Technology release reports that the Howard and Robinnette argue that emergency robots pacing the hallways and instructing people how to get to the emergency exits is a better solution. They say that the robots should be at least as tall as a human, so that they can be seen in a crowd, and styled



Robot stays with victim during testing // Source: wired.com

Smokes fills the halls, ear-piercing alarm sounds, people leave their offices in a panic not knowing what to do. Two Georgia Institute of Technology researchers — Ayanna Howard and Paul Robinette, electrical engineers at the Georgia Institute of Technology in Atlanta – say: follow the robot.

The two engineers say that robots would be a better solution in a crisis than emergency instructions on static signs attached to walls. In an emergency, we want people to move as fast as they can toward emergency exits, and standing in the hallways to read instructions after familiar exit signs with lights and arrows to guide the way. The researchers have created two possible designs.

They propose that teams of these robots would be stored in large buildings and receive instructions from a human operator during an emergency. A robot would start in "rescuer mode," searching for people in need of help, and then change to "leader mode" when it finds people it can guide to safety. If a robot comes across an injured person, it will make their location known to emergency personnel and with them stay to act as а communication device.



# Hybrid Warfare and Transnational Threats, 2011

#### Source:

http://www.censa.net/index.php?option=com\_c ontent&view=article&id=308:hybrid-warfareand-transnational-

threats&catid=38:compendiums&Itemid=145

Deconstructs the debate surrounding the employment of "hybrid warfare" as a useful term, the implementation of hybrid techniques in foreign theaters of war, and the evolution of hybrid tactics over time.

Hybrid Warfare and Transnational Threats tackles the complexity of modern warfare, delivering a breadth of insights aimed at bolstering our nation's security. The volume explores key aspects of the emerging international security environment to inform debates about the future of U.S. defense strategy and the changing nature of warfare.

In addition to traditional defense and foreign policy issues, the volume addresses stability and security operations, conceptual shifts in how we analyze and respond to national security challenges, and the theological dynamics underlying the continuing conflict with a loose network of violent Islamists.

The volume's twenty chapters provide an interdisciplinary perspective on U.S. national security affairs, focusing on key dimensions of

#### Advance Praise for Hybrid Warfare and Transnational Threats

"Is there such a thing as 'conventional warfare' anymore? As the authors of this paradigm shifting volume amply demonstrate, the collision of rudimentary modes of guerilla conflict with technologically enhanced operations is the new norm of global conflict. They not only provide a deep analysis of historical and ongoing approaches to warfare in Iraq, Afghanistan, Lebanon, Somalia and other places, but are also far ahead of others in taking seriously the permanent and systemic character of non-state actors and groups ranging from Diaspora fighters to global sympathizers. Hybrid Warfare and Transnational Threats represents a new paradigm in conflict studies, bringing theory into line with practice."

– Parag Khanna, Director of the Global Governance Initiative at the New American Foundation, author of How to Run the World and The Second World, former advisor to US Special Operations Forces in Iraq and Afghanistan

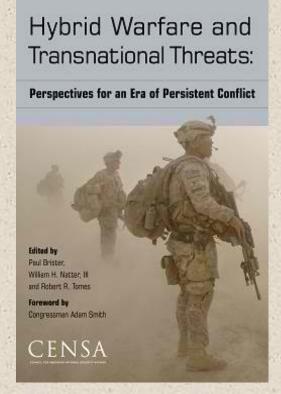
"Deserves a prominent place in any credible and current glossary of war."

- William H. Natter, III, Deputy Undersecretary of the Navy

#### Dedication

It is with profound respect that CENSA dedicates this book to the **memory of Colonel (ret) John J.** "Jack" McCuen. A renowned scholar and practitioner of Irregular and Hybrid Warfare, Colonel McCuen's life was as vast as it was adventurous. Alongside his book The Art of Counter-Revolutionary War—a brilliant piece that remained on the Department of the Army's required reading list for over a

what have been described as hybrid threats that increasingly involve transnational actors. Contributors familiar to readers include Steven Biddle, Martin van Creveld, Sebastian Gorka, Frank Hoffman, and Congressman Adam Smith.



decade—Jack commanded an Armored Cavalry Squadron, served as the Director of Internal Defense and Development Studies at the US Army War College, and later worked as the Chief of the Military Assistance Group-Indonesia. Following 28 years of distinguished service, Colonel McCuen retired, yet continued to serve as a lecturer and consultant on the complexities of modern warfare. Although saddened by the loss of this great warrior, we celebrate his legacy and acknowledge the significant contributions he has made to the study of modern warfare.

# **Riots thwarted by Blackberry and Twitter chat - police**

Source: http://www.bbc.co.uk/news/uk-politics-14542588

Police say they prevented attacks by rioters on the Olympic site and London's Oxford Street after picking up intelligence on social networks. Assistant Met Police Commissioner Lynne Owens told a committee of MPs officers learned of possible trouble via Twitter and Blackberry messenger. secure - users are invited to join each other's contacts list using a unique PIN, although once they have done so, messages can be distributed to large groups.

Switch off request

Ms Owens said officers had been attempting to sift through an "overwhelming" amount of



The London 2012 Olympic Park is in east London

But Acting Commissioner Tim Godwin said he had considered asking authorities to switch off social networks.

He said they provided intelligence but could also be misleading.

A number of politicians, media commentators and members of the police force have suggested that Twitter and Blackberry Messenger (BBM) had a role to play in the riots.

The BBM system is popular among many young people because it is both private and

"chitter chatter" on social networks during last week's riots in London, but some had proved vital.

"Through Twitter and BBM there was intelligence that the Olympic site, that both Westfields [shopping centres] and Oxford Street were indeed going to be targeted," she told the home affairs select committee.

"We were able to secure all those places and indeed there was no damage at any of them."

Mr Godwin said that on Monday, when disorder spread to 22 of London's 32 boroughs, police were receiving a new piece of intelligence every second.



And while much of the information coming via social media "was obviously wrong and rather silly", he said police did considered trying to

### Viewpoint

# Ben Wood, mobile technology expert

Not only are Rim (Research in Motion, Blackberry's owner) the most secure messaging operator, they're also the most fastidious - they log everything. If you were a looter using a Blackberry, you're going to get found out.

The police have the power to serve Rim with an order to reveal information. Under the same law, Rim are barred from disclosing whether they've done so or not.

But although Rim can't say it themselves, I can say with confidence that they'll be doing everything they can to help. It's a reputation issue - these people are a tiny minority of their users and they want the remainder to see them doing all they can to track them down.

Rim don't need to reveal the actual contents of messages in order do that. They can tell police who sent a message to whom and when. The police can then ask the network operators where that was done - and the sum total will probably be enough to be used as evidence.

If you know a Blackberry belonging to a suspect sent a message to 45 other Blackberries and then those 45 owners all turn up in Ealing or Tottenham an hour later, it's clear what's going on.

shut the networks down in order to prevent them being used to organise further violence. "We did contemplate, I contemplated, asking the authorities to switch it off. The legality of that is very questionable and additionally, it is also a very useful intelligence asset," he said. "So, as a result of that, we did not request that that was turned off, but it is something that we are pursuing as part of our investigative strategy."

Blackberry has offered to co-operate with police investigating the riots - prompting attacks by hackers angry that the company could be prepared to hand over user data to authorities.

Asked what Blackberry's co-operation would involve, Mr Godwin asked to "plead the fifth", adding: "I would rather not answer that question as it is an investigative strategy."

'Seamless working'

Sir Hugh Orde, president of the Association of Chief Police Officers, which played a key role in coordinating the Met's response, said the riots were "fundamentally different" from the sort of disorder he and the rest of the police force had ever dealt with before.

He told the committee the violence was "multisite" and "far more spontaneous", and there was almost "non-existent pre-intelligence" which could have helped police manage things differently.

Sir Hugh also defended the way police resources were managed, insisting there was "a pretty seamless working of the system" which was able to meet all the requests made for additional resources.

The senior officers were asked about an apparent spat which broke out between the police and senior ministers over who was responsible for bringing about the surge in officer numbers which returned calm to London.

Mr Godwin insisted that the prime minister and home secretary had been "very supportive" and any differences between them were "overplayed". "Sometimes the perception of us at loggerheads is not helpful," he added.

# The Global Challenge of Chemical, Biological, Radiological, and Nuclear (CBRN) Terrorism

Office of the Coordinator for Counterterrorism Country Reports on Terrorism 2010 August 18, 2011

Source: http://www.state.gov/s/ct/rls/crt/2010/170261.htm

### THE MATERIAL THREATS

Chemical. Preventing chemical terrorism is particularly challenging since terrorists can use toxic industrial chemicals and other commonly available chemical agents and materials as low-cost alternatives to traditional chemical weapons and delivery systems. Today's chemical terrorism threat ranges from the potential acquisition and dissemination of chemical warfare agents with military delivery.

systems to the production and use of toxic industrial chemicals or improvised dissemination systems for chemical agents. The growth and sophistication of the worldwide chemical industry, including the development of complex synthetic and dual-use materials, makes the task of preventing and protecting



against this threat more difficult.

Biological. Bioterrorism involves the deliberate dispersal of pathogens (viruses, fungi, and bacteria) through inhalation, ingestion, injection vectors to cause disease. Even though the necessary technical skills are not beyond the expertise of motivated scientists with university-level training, developing a masscasualty bioterrorism capability presents some scientific and operational challenges. International laboratories that store and work with dangerous pathogens are often not adequately secured. Moreover, many Select Agent pathogens, such as anthrax, are widely available in nature. Equipment suitable for cultivating and disseminating such materials is almost entirely dual-use and is widely employed for legitimate purposes.

Radiological. Radioactive materials are used widely in industrial, medical, and research applications. They may be employed in devices used for power supply in remote locations, cancer therapy, food and blood irradiation, and radiography. Their widespread use in nearly every country makes these materials much more accessible for deployment in a radiological dispersal device (RDD), often referred to as a "dirty bomb," than the fissile materials required for nuclear weapons.

Nuclear. The diffusion of scientific and technical information regarding the assembly of nuclear weapons – some of which is now available on the Internet – has increased the

risk that a terrorist organization in possession of sufficient fissile material could develop its own crude nuclear weapon. The complete production of a nuclear weapon strongly depends on the terrorist group's access to special nuclear materials as well as significant engineering and scientific expertise.

Dual Use Materials, Equipment, and Technologies. Dual-use materials, equipment, and technologies have legitimate commercial applications but may be used in the development of weapons of mass destruction (WMD) advanced and conventional capabilities. Terrorists have shown an interest acquiring in sophisticated dual-use technologies to advance their own weapons programs and are taking advantage of the availability of such material and expertise and diverting it to illicit end-uses. As a result, reducing the risk of terrorist access to and exploitation of dual-use science remains a critical challenge.

The United States regulates export, re-export, transit, transshipment, and brokering of dualuse goods based on its international commitments in the multilateral export control regimes. The United States also maintains unilateral controls on a wide range of dual-use items predominantly for antiterrorism reasons. Effective partnerships with private sector organizations, industry, academia, and governmental scientific communities, play an important role in mitigating the risk of dual-use capabilities falling into the wrong hands.

# STATE SPONSORSHIP OF TERRORISM: A KEY CONCERN

A state that directs CBRN resources to terrorists or does not secure dual-use resources poses a grave CBRN terrorism



threat. Although terrorist organizations

continue to seek a CBRN capability independent of state programs, the sophisticated CBRN knowledge and resources of a state could enable a terrorist capability. State sponsors of terrorism and all nations that fail to live up to their international counterterrorism nonproliferation and obligations deserve continued scrutiny as potential facilitators of CBRN terrorism.

# NON-STATE FACILITATORS: AN EMERGING THREAT

State sponsors of terrorism with CBRN programs represent just one facet of the overall risk of CBRN terrorism. The non-governmental entities (terrorist groups and smugglers) state sponsors use to facilitate their CBRN programs have emerged as a growing proliferation threat in recent years that could eventually provide terrorists with access to materials and expertise particularly hard to acquire.

# ADDRESSING THE INTERNATIONAL NUCLEAR THREAT

The first Nuclear Security Summit was held in Washington, April 12-13, 2010. Forty-six nations were invited to participate; all accepted, and the United Nations, the International Atomic Energy Agency, and the European Commission also participated. The United States was very pleased with the outcome of the 2010 Summit, which helped develop a common understanding of the threat posed by nuclear terrorism and achieved broad political agreement on effective measures to secure nuclear material and prevent nuclear smuggling and nuclear terrorism. The Summit's Joint Communiqué and detailed Work Plan articulate a common commitment among countries to evaluate the threat, improve security as conditions change, and continually exchange information, best practices, and practical security solutions.

# PARTNERSHIPS TO COMBAT CBRN TERRORISM

Since September 11, 2001, the international community has made significant strides in responding to the threat of CBRN terrorism. States are working together bilaterally and multilaterally to address these threats and protect their populations. Through a variety of multinational initiatives such as the Global Threat Reduction Initiative, the Proliferation Security Initiative (PSI), and the Global

Initiative to Combat Nuclear Terrorism (GICNT), the United States has taken a leadership role in reducing the threat of CBRN terrorism. Some of these efforts are focused on preventing threats from non-state actors and terrorists; others aim at preventing the proliferation of weapons of mass destruction to states as well as non-state actors.

UN Security Council Resolution 1540: In 2004, the UN Security Council unanimously adopted Resolution 1540, which requires states to take measures to prevent the spread of weapons of mass destruction, including adopting and enforcing laws to prohibit the transfer of WMD and related materials to non-state actors. While the Resolution is legally binding on all UN Member States, universal compliance with the resolution has not yet been achieved. Several states lack the capacity to comply with the resolution's requirements and need assistance to do so. The United States is one of the leading providers of such assistance. Several programs are in place to help countries develop their abilities to combat illicit trafficking in WMD and related materials. Other sources of assistance include other developed nations. international organizations such as the International Atomic Energy Agency (IAEA), and the Organization for the Prohibition of Chemical Weapons (OPCW), and a variety of non-government organizations (NGOs).

The Proliferation Security Initiative (PSI): Announced in 2003, the PSI has led to a number of important interdictions over the last eight years and is an important tool in the overall global effort to combat WMD proliferation to both state and non-state actors. In its eighth year, the PSI is a cooperative global effort that aims to stop the trafficking of WMD, their delivery systems, and related materials to and from states and non-state actors of proliferation concern. The PSI relies on voluntary actions by states, using existing national and international legal authorities to put an end to WMD-related trafficking. PSI partners take steps to strengthen those legal authorities as necessary, share information, and cooperate on interdiction activities. States that wish to participate in the PSI endorse its Statement of Interdiction Principles, by which states commit to undertake specific actions to halt the trafficking of WMD and related materials. As of December 31, 2010, 98 states have endorsed the Statement. Each year P

endorsers conduct a series of activities, including exercises, workshops, and expert's group meetings, to improve operational capabilities to conduct interdictions, share information, and develop new operational concepts.

The Global Initiative to Combat Nuclear Terrorism (GICNT): The GICNT, which is cochaired by the United States and Russia, is a cross-cutting strategic framework of 82 partners and four observers who are determined to strengthen individual and global capacity to prevent, detect, and respond to a nuclear terrorist event. These partners have endorsed a set of core nuclear security principles encompassing the full spectrum of deterrence. prevention, detection, and Partners response objectives. utilize multilateral activities and exercises to share best practices and lessons learned in order to strengthen individual and collective capacity to combat nuclear terrorism. To date, partners have conducted over 40 multilateral activities and six senior-level meetings in support of these nuclear security goals. Through these activities, partners have improved international understanding in emerging nuclear detection technologies, emergency response and preparedness practices, and anti-smuggling assistance programs. The Initiative is open to nations that share in its common goals and are committed to combating nuclear terrorism on a determined and systematic basis.

Nuclear Smuggling Outreach Initiative (NSOI): The NSOI seeks to enhance partnerships with key countries around the world to strengthen capabilities to prevent, detect, and respond to incidents of nuclear smuggling. It focuses on both bilateral partnerships to improve such capabilities and partnerships donor to support these improvements. In its bilateral partnerships, NSOI engages those countries seen to be most important to the global effort to combat smuggling of nuclear or highly radioactive materials. In its donor partnerships, NSOI engages those countries that have resources or expertise that can be provided to improve the capabilities of other countries. The NSOI team works with the governments of potential donor partners to identify their particular interests and assets for such assistance. NSOI has to date completed Joint Action Plans and

developed anti-nuclear smuggling cooperative projects with Ukraine, Kazakhstan, Georgia, the Kyrgyz Republic, Armenia, and the Democratic Republic of the Congo. It has engaged several additional bilateral partners with whom it plans to complete such documents soon, and it plans to engage several more over the coming years. NSOI has also developed donor partnerships with ten countries and three international organizations and hopes to create more such partnerships over the coming years.

Export Control and Related Border Security Program (EXBS): The EXBS program is the U.S. government's premier initiative to assist other countries in improving their strategic trade control systems. EXBS seeks to prevent the proliferation of weapons of mass destruction and their delivery systems, as well as destabilizing accumulations of advanced conventional weapons by helping to build effective national export control systems in countries that possess, produce, or supply strategic items as well as in countries through which such items are most likely to transit. EXBS is directed by the Office of Export Control Cooperation in the Bureau of International Security and Nonproliferation at the Department of State (ISN/ECC), which also leads the U.S. government interagency working group that seeks to coordinate U.S. government nonproliferation export and border control assistance and ensure EXBS is harmonized with and complements the Department of Homeland Security's Container Security Initiative, the Department of Energy's Second Line of Defense Program, the Megaports Initiative, and other international donor assistance programs. EXBS programs improve partner countries' capabilities to combat proliferation threats and fulfill their commitments as part of the Proliferation Security Initiative, the Global Initiative to Combat Nuclear Terrorism, and UNSCR 1540. EXBS currently has 23 Program Advisors stationed globally and is active in over 60 countries.

Second Line of Defense (SLD): Under its SLD Program, the Department of Energy's National Nuclear Security Administration (DOE/NNSA) cooperates with partner countries to provide radiation detection systems and associated training to enhance partner: nation.

capabilities to deter, detect, and interdict illicit trafficking of special nuclear and other radiological materials across international borders. The SLD Program includes two components: the Core Program and the Megaports Initiative. The Core Program focuses on providing equipment to land border crossings, feeder seaports, and international airports. This work originally began in Russia and has since expanded to include former Soviet states, the Caucasus, Eastern Europe, and other key regions. Mobile detection equipment is also provided to selected countries for use at land borders and internal checkpoints.

Global Threat Reduction (GTR): GTR programs work globally to prevent terrorists from acquiring CBRN expertise, materials, and technology. GTR is actively engaged in a variety of countries including the front line countries of Pakistan, Iraq, Yemen, and Afghanistan. GTR programs have expanded to meet emerging CBRN proliferation threats worldwide and focus on promoting biological, chemical, and nuclear security in those countries where there is a high risk of CBRN terrorism or proliferation. The programs also engage scientists with WMD and WMDapplicable skills. By engaging biological, chemical, and nuclear, scientists with dual-use expertise, and helping to secure dual-use material, GTR seeks to keep CBRN and dualuse materials, technology, and expertise away from terrorists who would use these materials against the US homeland.

The Global Threat Reduction Initiative (GTRI): The goal of GTRI, announced by the United States on May 26, 2004, in Vienna, Austria, is to secure, remove, or facilitate the conversion of final arrangements for disposal of materials as expeditiously as possible, including nuclear and radioactive materials in civilian applications around the world that have been identified as vulnerable or posing a potential threat to the international community. GTRI focuses on minimizing the use of highly enriched uranium in research reactors and isotope-production processes around the world

as well as protecting or removing unwanted or unused plutonium and high-activity radioactive sources. Approximately one hundred international partners cooperate with GTRI programs under this initiative.

Biological Weapons Convention Intersessional Work Program: In response to a proposal from the United States, the States Parties to the Biological Weapons Convention (BWC) in 2002 embarked on a series of expert exchanges aimed at raising awareness, sharing best practices, and facilitating assistance on topics related to implementation of the BWC and reducing the threat of BW use, with a new emphasis on the terrorist threat. Work has included exchanges on national legislative and regulatory frameworks; laboratory biosecurity; outreach to promote responsible conduct by members of the scientific community; and investigation of and response to suspect attacks.

National Strategy for Countering Biological Threats: In November 2009, President Obama approved a new national strategy to provide greater policy cohesion and coordination for U.S. efforts to prevent state or non-state actors from acquiring or using biological weapons. (Efforts to mitigate the consequences of use are dealt with through other policy/strategy Federal frameworks). agencies have developed detailed implementation plans and are actively coordinating efforts in support of the Strategy's seven key objectives, which are to:

- 1. Promote global health security
- 2. Reinforce norms of responsible/beneficent conduct
- 3. Obtain timely/accurate insight on current/emerging risks
- 4. Take reasonable steps to reduce potential for exploitation
- 5. Expand capability to disrupt, apprehend and attribute
- 6. Communicate effectively with all stakeholders
- 7. Transform international dialogue on biological threats

**NOTE:** You can download full report from the "CBRNE-CT Papers" section of the Newsletter.



Climate change ... You are responsible too!

### Researchers developing graffiti analysis app

Source:http://www.laboratoryequipment.com/news-App-Fights-Graffiti-Hazmat-081911.aspx?xmlme nuid=51

Law enforcement officials could soon have an app for their mobile phones that allows them to

snap a picture of gang graffiti and have its meaning translated. In а presentation to DHS officials and law enforcement agencies in Indianapolis, researchers from Purdue University showed off their new graffiti analysis app.

"The whole idea of these projects is that you literally take a picture of the gang graffiti or a hazardous materials placard with a mobile phone and then the system interprets the images," said Edward Delp, a professor of Electrical and Computer

Engineering at Purdue. The project has been dubbed "GARI," or Gang Graffiti Automatic Recognition and Interpretation, and is being funded by the DHS Security Science & Technology Directorate (S&T).

"Gang graffiti basically tells a story," explained Timothy F. Collins, the managing director of Purdue's Visual Analytics for Command, Control and Interoperability Environments Center of Excellence (VACCINE), which is leading the research.

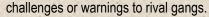


Ubiquitous graffiti may be conveying intergang messages // Source: metropotam.ro



a way of communicating messages like

According to Collins, gangs often use graffiti as



"Investigators want to not only catch who put it there but also to understand its meaning. Sometimes they indicate when someone is about to get killed or whether a rival gang has moved in that could lead to an increase in crime. An officer might take a picture of graffiti and ask the system to show all the similar graffiti that has occurred within 2 miles of the location."

He added that it is also "an excellent way to track gang affiliation and growth, or even sometimes to obtain membership information."

With the new app, an officer can take a picture of the graffiti and the system uses image analysis algorithms to analyze the graffiti and also marks the location with GPS coordinates.

"You take a picture with an Android mobile phone, and it not only records the image, it also records the GPS coordinates, the date and time," said David S. Ebert, Purdue's Silicon Valley Professor of Electrical and Computer Engineering and VACCINE director. "It can provide some analysis right on the phone and also can access a more extensive database of graffiti on a server."

Researchers are still testing the software as analyzing graffiti is a complex process. "Interpreting these images is not a trivial task," said Delp. To analyze the image, the software

examines several elements of the graffiti including colors, shapes, and characters. The information from the photo is then sent to a server and cross-referenced against a graffiti database. Matching results are then returned to the mobile phone, where users can review them and provide further details for more analysis.

"Once the graffiti is completely decoded and interpreted, it is labeled and added to the database," said Collins, who is also a former Indiana state trooper. "Gangs are a serious threat to public safety throughout the United States. Gang members are continuously migrating from urban to suburban areas and even rural areas. They are responsible for an increasing percentage of crime and violence in many communities."

# Micro Unmanned Ground Vehicle helps soldiers, first responders

Source:http://www.homelandsecuritynewswire.com/micro-unmanned-ground-vehicle-helps-soldiers-first-responders

Weighing just over ten pounds, Dragon Runner 10 (DR10) is small enough to carry in an assault pack and rugged enough to throw into



10 (DR10) is small enough to carry in an assault pack and rugged enough to throw into buildings and hostile environments. The DR10

has multiple sensor and payload options, and thus is suitable for reconnaissance and surveillance missions to support small military units, patrols, and first responder teams.

Soldiers use a wearable controller to send DR10 in first, to assess the situation in advance. Whether it is being driven or thrown into a potentially hostile area, DR10 can gain situational awareness and report information back to the operator. Equally capable in daytime or night missions, the DR10 can serve as the team's

buildings and hostile environments; the DR10 has multiple sensor and payload options, and thus is suitable for reconnaissance and surveillance missions to support small military units, patrols, and first responder teams.

#### QinetiQ's Dragon Runner 10, muti-option, MUGV // Source: defense-update.com

QinetiQ North America announced the availability of a

new Micro Unmanned Ground Vehicle (MUGV) for military and first responder robotic missions. Weighing just over ten pounds, Dragon Runner



forward eyes and ears, while also carrying out missions such as explosive ordnance disposal, setting counter-IED charges, delivering remote sensors, gathering intelligence,

conducting surveillance. "Military robotic missions save lives, and if possible, it's better to send the robot in first," said QinetiQ North America Technology Solutions Group president J. D. Crouch. "Dragon Runner 10 is a practical solution that makes it easier to carry and operate sophisticated robots in theater." DR10 is 15" long, 13.5" wide, and 5.8" tall. When thrown, DR10 has the ability automatically to flip video images, antennae, and controls upon landing. Multiple payloads are available, including a variety of sensors, radios, cameras, and robotic arms. DR10 can be equipped with either tracked or wheeled mobility options to negotiate different types of terrain.

# Antenna-equipped garments here

Source: http://www.homelandsecuritynewswire.com/antenna-equipped-garments-here

To make communications devices more reliable, researchers are working on incorporating radio antennas directly into clothing, using plastic film and metallic thread; the new antenna design has a range four times larger than that of a conventional antenna worn on the body -- one that is used by American antennas directly into clothing, using plastic film and metallic thread.

In the current issue of the journal IEEE Antennas and Wireless Propagation Letters, they report a new antenna design with a range four times larger than that of a conventional antenna worn on the body — one that is used

soldiers today. The next generation of communications systems could be built with a sewing machine. To make communications devices more reliable, Ohio State University researchers are working on incorporating radio

by American soldiers today. "Our primary goal is to improve communications reliability and the mobility of the soldiers," said Chi-Chih Chen, a research associate professor of electrical and computer



engineering at Ohio State. "But the same technology could work for police officers, fire fighters, astronauts – anybody who needs to keep their hands free for important work."

An Ohio State University release reports that for typical foot soldiers, mobility and communications are often at odds. An antenna can be a large and unwieldy addition to an already heavy load.

The idea of embedding communications devices in clothing to address this problem is not new, Chen explained. The Ohio State system takes elements from previous research and combines them in a new way, with the addition of a unique computer control device that lets multiple antennas work together in a single piece of clothing.

The result is a communications system that can send and receive signals in all directions, even through walls and inside a building, without a need for the wearer to carry an external antenna.

John Volakis, the Roy & Lois Chope Chair Professor and Director of the ElectroScience Laboratory at Ohio State, found a common analogy for the new design.

"In a way, we're doing what's already been done on a cell phone. You don't see cell phones with external antennas anymore, because the antenna is part of the body of the phone," Volakis said.

When antennas make contact with the human skin, however, the body tends to absorb radio signals and form a short circuit — a fact driven home by the recent difficulties with the antenna placement on the iPhone 4. Also, if an antenna is improperly placed, a person's body can block it when he or she moves against a wall or other obstacles.

The Ohio State system overcomes these problems by surrounding the body with several antennas that work together to transmit or receive a signal, no matter which way a person is facing. An integrated computer control device senses body movement and switches between the antennas to activate the one with the best performance given the body's position. The engineers created a prototype antenna by etching thin layers of brass on a commercially available plastic film, called FR-4. The film is light and flexible, and can be sewn onto fabric. They attached it into a vest at four locations chest, back, and both shoulders. The computer controller - a metal box a little smaller than a credit card and an inch thick - was worn on a belt. In laboratory tests, the experimental antenna system provided significantly greater signal strength compared to a conventional military "whip" antenna, enabling a range of communications four times larger. Perhaps most importantly, the new antenna system worked in all directions, even as researchers tested it inside the hallways of the ElectroScience Lab, where doors and windows would normally interfere with the signal. Key to technology the engineers' the was development of network communications coding to coordinate the signals among the antennas. Doctoral student Gil-Young Lee developed a computer module to make the antenna control automatic. Lee, Chen, and Volakis co-authored the IEEE paper with Dimitrios Psychoudakis, senior research associate at the ElectroScience Lab.

The release notes that they are partnering with an antenna design company, Applied EM of Hampton, Virginia, to commercialize the research, which was funded by a Small Business Innovation Research grant.

Chen currently estimates that the antenna systems, as demonstrated in the prototype, would cost \$200 per person to implement, but mass production would bring that cost significantly down.

In the meantime, the engineers are working on printing antennas directly onto clothing, and embroidering antennas into clothing with metallic threads. A typical home sewing machine is now part of their laboratory equipment, and early tests have shown that the swirly designs they've embroidered into fabrics such as cotton — and even taffeta — can work as functional antennas.

That's why Volakis envisions the technology to be adaptable for the general public. The elderly or disabled could wear clothing that would let them communicate in case of emergency, without the stigma they might feel in wearing a more visible assistive device.

"Imagine a vest or shirt, or even a fancy ball gown made with this technology," he said, scrunching a sample of embroidered taffeta in his hand. "The antennas would be inconspicuous, and even attractive. People would want to wear them."



# Balancing the Risks, Benefits, and Costs of Homeland Security

By Mueller, John and Mark G. Stewart

*Homeland Security Affairs* 7, Article 16 (August 2011) Source: http://www.hsaj.org/?article=7.1.16

#### Introduction

In seeking to evaluate the effectiveness of the massive increases in homeland security expenditures

since the terrorist attacks on the United States of September 11, 2001, the common and urgent query has been "are we safer?" This, however, is the wrong question. Of course we are "safer"— the posting of a single security guard at one building's entrance enhances safety, however microscopically. The correct question is "are the gains in security worth the funds expended?" Or as this absolutely central question was posed shortly after 9/11 by risk analyst Howard Kunreuther, "How much should we be willing to pay for a small reduction in probabilities that are already extremely low?"1

# Tallying the Costs — One Trillion Dollars and Counting

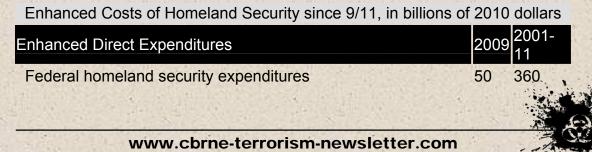
We have, in fact, paid — or been willing to pay - a lot. In the years immediately following the terrorist attacks of September 11, 2001 on New York, it was Washington and understandable that there was a tendency to fashion policy and to expend funds in haste and confusion, and maybe even hysteria, on homeland security. After all, intelligence was estimating at the time that there were as many as 5,000 al Qaeda operatives at large in the country,<sup>2</sup> and as New York Mayor Rudy Giuliani reflected later, "Anybody, any one of these security experts, including myself, would have told you on September 11, 2001, we're looking at dozens and dozens and multi-years of attacks like this."3

The intelligence claims and the anxieties of Giuliani and other "security experts" have clearly proved, putting it mildly, to be

unjustified. In the frantic interim, however, the United States government increased its expenditures for dealing with terrorism massively. As we approach the tenth anniversary of 9/11, federal expenditures on domestic homeland security have increased by some \$360 billion over those in place in 2001. Moreover, federal national intelligence expenditures aimed at defeating terrorists at home and abroad have gone up by \$110 billion, while state, local, and private sector expenditures have increased by two hundred billion more. And the vast majority of this increase, of course, has been driven by much heightened fears of terrorism, not by growing concerns about other hazards - as Veronique de Rugy has noted, by 2008 federal spending on counterterrorism had increased enormously while protection for such comparable risks as fraud and violent crime had not, to the point where homeland security expenditures had outpaced spending on all crime by \$15 billion.4

Tallying all these expenditures and adding in opportunity costs - but leaving out the costs of the terrorism-related (or terrorism-determined) wars in Iraq and Afghanistan and quite a few other items that might be included - the increase in expenditures on domestic homeland security over the decade exceeds one trillion dollars. The details are in Table 1. This has not been enough to move the country into bankruptcy, Osama bin Laden's stated goal after 9/11, but it clearly adds up to real money, even by Washington standards.<sup>5</sup> Other countries like Britain, Canada, and Australia have also dramatically increased their expenditures.

# Table 1. The Trillion Dollar Table



<b>CBRNE-Terrorism</b>	Newsletter	* Autumn-2011

Federal intelligence expenditures	15	110
Local and state expenditures	10	110
Private-sector spending	10	110
Total	85	690
Opportunity Costs		
Terrorism risk insurance premiums	4	40
Passenger delays caused by airport screening	10	100
Increase in short-haul traffic fatalities for people avoiding airport delays	3	32
Deadweight losses and losses in consumer welfare	30	245
Total	47	417

Relevant spending elements not included in the table

- Terror-related wars in Iraq and Afghanistan
- Costs of crime facilitated by focus of police and FBI on, or preoccupation with, terrorism
- Costs resulting from hurricane Katrina that might have been mitigated if DHS had not been so preoccupied by terrorism
- Additional Post Office expenditures to deal with the effects of 9/11 and the anthrax letters
- Effects on tourism, property and stock market values, business location decisions, etc. though dead weight losses might capture some of these
- In addition to the short-haul fatality effect included in the table, the increase in traffic fatalities in the U.S. of 2,300 lives to the end of 2003 due to the fear of flying and the inconvenience of extra passenger screening
- Extra fuel cost to airlines because of the weight of hardened (heavier) cockpit doors
- Free airline seats to Federal Air Marshals
- Passenger delays and inconvenience cause by false positive identification on TSA's no fly list.
- Cutbacks to Medicare, Medicaid, education, social security, and other government services in an effort to reign in budget deficits caused by wars in Iraq and Afghanistan and mushrooming homeland security budgets
- Note: For sources and full explanation for these numbers, see John Mueller and Mark G. Stewart, Terror, Security and Money: Balancing the Risks, Benefits, and Costs of Homeland Security (New York and Oxford, UK: Oxford University Press, forthcoming September 2011).

### **Evaluating the Expenditures**

In this article we seek to apply conventional cost-benefit and risk analytic approaches to this massive increase in expenditure in an effort to provide an answer to Kureuther's exceedingly apt question. These approaches have been recommended for many years by the United States Office of Management and Budget, and they are routinely used by such agencies as the Nuclear Regulatory Commission, the Environmental Protection and the Federal Aviation Agency, Administration, and in 2004 the 9/11 Commission specifically called on the government to apply them to assess the risks

and cost-effectiveness of security measures put in place to deal with terrorism.<sup>6</sup> However, it appears that this simply has not been done.

Upon taking office in 2005, Department of Homeland Security Secretary Michael Chertoff did strongly advocate a risk-based approach, insisting that the department "must base its work on priorities driven by risk."<sup>7</sup> Yet, a year later, when DHS expenditures had increased by some \$135 billion beyond those already in place in 2001 and when the department had become the government's largest non-military bureaucracy, one of its senior economists wistfully noted, "We really don't know a whole lot about the overall costs and benefits of homeland security."<sup>8</sup>

By 2007, RAND President James Thomson was contending that DHS leaders "manage by inbox" with the "dominant mode of DHS behavior being crisis management." Most programs are implemented, he continued, "with little or no evaluation" of their performance or effectiveness, and the agency "receives little analytical advice on issues of policy, program, and budget."<sup>9</sup> And, after an exhaustive assessment, the Congressional Research Service concluded at the same time that DHS simply could not answer the "central question" about the "rate of return, as defined by quantifiable and empirical risk reductions" on its expenditure.<sup>10</sup>

The boilerplate emphasis on risk-informed decision making continued with the change of administrations after the 2008 elections, as Secretary Janet Napolitano insisted that

Development and implementation of a process and methodology to assess national risk is a fundamental and critical element of an overall risk management process, with the ultimate goal of improving the ability of decision makers to make rational judgments about tradeoffs between courses of action to manage homeland security risk.<sup>11</sup>

Such declarations notwithstanding, however, we have been able to find only one published reference to a numerical estimate of risk reduction after an extensive search of the agency's reports and documents.<sup>12</sup> Moreover, we have been able to find no reference whatever to the likelihood of a terrorist attack beyond rather vague references such as "high," "imminent," "dynamic," "persistent," and "emerging."

Indeed, at times DHS has ignored specific calls by other government agencies to conduct risk assessments. In 2010, the Department began deploying full-body scanners at airports, a technology that will cost \$1.2 billion per year. Accountability Office Government The specifically declared that conducting a costbenefit analysis of this new technology to be "important."13 As far as we can see, no such study was conducted. Or there was GAO's request that DHS conduct a full cost/benefit analysis of the extremely costly process of percent of U.S.-bound scanning 100

containers. To do so would require the dedicated work of a few skilled analysts for a few months or possibly a year. Yet, DHS replied that, although it agreed that such a study would help to "frame the discussion and better inform Congress," to actually carry it out "would place significant burdens on agency resources."<sup>14</sup>

Clearly, DHS focuses all or almost all of its analyses on the contemplation of the consequences of a terrorist attack while substantially ignoring the equally important likelihood component of risk assessment as well as the key issue of risk reduction. In general, risk assessment seems to be simply a process of identifying a potential source of harm and then trying to do something about it without evaluating whether the new measures reduce risk sufficiently to justify their costs.

This conclusion was strongly supported by a 2010 report of the National Research Council of the National Academies of Sciences, Engineering, and Medicine. Requested by Congress to assess the activities of the Department of Homeland Security, а committee worked for nearly two years on the project and came up with some striking conclusions. Except for the analysis of natural disasters, the committee "did not find any DHS risk analysis capabilities and methods that are yet adequate for supporting DHS decision making," and therefore "only low confidence should be placed in most of the risk analyses conducted by DHS." Indeed, "little effective attention was paid to the features of the risk problem that are fundamental." It also found an "absence of documentation of methods and processes" with the result that the committee sometimes had to infer details about DHS risk modeling. Indeed, "in a number of cases examined by the committee, it is not clear what problem is being addressed." It also found "a pattern" of "trusting numbers that are highly uncertain." And, concluded the committee rather glumly, "it is not yet clear that DHS is on a trajectory for development of methods and capability that is sufficient to ensure reliable risk analyses": although it found that "there are people at DHS who are aware of these current limitations," it "did not hear of efforts to remedy them."15



Overall, it seems, security concerns that happen to rise to the top of the agenda are serviced without much in the way of full evaluation — security trumps economics, as one insider puts it — and such key issues as acceptable risk are rarely discussed while extravagant worst case scenario thinking dominates, and frequently savagely distorts, the discussion.

It is clearly time to examine massive homeland security expenditures in a careful and systematic way, applying the kind of analytic risk management approaches emphasizing cost-benefit analysis and determinations of acceptable and unacceptable risks that are routinely required of other governmental agencies and that have been standard coin for policy decision-making for decades throughout the world when determining regulations even in such highly charged and politicized decisions as those regarding where to situate nuclear power plants, how to dispose of toxic waste, and how to control pollution-decisions that engage the interests and passions of multiple groups.

#### **Probability Neglect**

A recent book by Gregory Treverton, a risk analyst at the RAND Corporation whose work we have found highly valuable at various points in this study, contains a curious reflection:

When I spoke about the terrorist threat, especially in the first years after 2001, I was often asked what people could do to protect their family and home. I usually responded by giving the analyst's answer, what I labeled "the RAND answer." Anyone's probability of being killed by a terrorist today was essentially zero and would be tomorrow, barring a major discontinuity. So, they should do nothing. It is not surprising that the answer was hardly satisfying, and I did not regard it at such.<sup>16</sup>

From this experience, he concluded, "People want information, but the challenge for government is to warn without terrifying."<sup>17</sup>

It is not clear why anyone should find his observation unsatisfying since it simply puts the terrorist threat in general and in personal context, suggesting that excessive alarm about the issue is scarcely called for. It is, one might suspect, exactly the kind of accurate, reassuring, adult, and non-terrifying information people have been yearning for. And it deals frontally with a key issue in risk assessment: evaluating the likelihood of a terrorist attack.

Treverton's "RAND answer," calmly (and accurately) detailing the likelihood of the terrorist hazard and putting it in reasonable context, has scarcely ever been duplicated by politicians and officials in charge of providing public safety. Instead the awkward problem of dealing with exceedingly low probabilities has been finessed and questionable \_ expenditures accordingly justified - by five stratagems that in various ways embrace a form of risk aversion that can be called "probability neglect."

#### Focusing on Worst Case Scenarios

Cass Sunstein, who seems to have invented the phrase, "probability neglect," assesses the version of the phenomena that comes into being when "emotions are intensely engaged." Under that circumstance, he argues, "people's attention is focused on the bad outcome itself, and they are inattentive to the fact that it is unlikely to occur." Moreover, they are inclined to "demand a substantial governmental response — even if the magnitude of the risk does not warrant the response."<sup>18</sup> It may be this phenomenon that Treverton experienced.

Playing to this demand, government officials are inclined to focus on worst case scenarios, presumably in the knowledge, following Sunstein's insight, that this can emotionally justify just about any expenditure no matter how unlikely the prospect the dire event will actually take place. Accordingly, there is a preoccupation with "low probability/high consequence" events such as the detonation of a sizeable nuclear device in midtown Manhattan even though the vast bulk of homeland security expenditures are focused on comparatively low consequence events like explosions set off by individual amateurs.

It is sometimes argued that conventional risk analysis breaks down under extreme conditions because the risk is now a very large number (losses) multiplied by a very small.

number (attack probability). However, it is not the risk analysis methodology that is at fault here, but our ability to use the information obtained from the analysis for decision-making. Analyst Bruce Schneier has written penetratingly of worst-case thinking. He points out that

[It] involves imagining the worst possible outcome and then acting as if it were a certainty. It substitutes imagination for thinking, speculation for risk analysis, and fear for reason. It fosters powerlessness and vulnerability and magnifies social paralysis. And it makes us more vulnerable to the effects of terrorism.<sup>19</sup>

#### It leads to bad decision making because

It's only half of the cost-benefit equation. Every decision has costs and benefits, risks and rewards. By speculating about what can possibly go wrong, and then acting as if that is likely to happen, worst-case thinking focuses only on the extreme but improbable risks and does a poor job at assessing outcomes.<sup>20</sup>

It also assumes "that a proponent of an action must prove that the nightmare scenario is impossible," and it "can be used to support any position or its opposite. If we build a nuclear power plant, it could melt down. If we don't build it, we will run short of power and society will collapse into anarchy." And worst, it "validates ignorance" because, "instead of focusing on what we know, it focuses on what we don't know — and what we can imagine." In the process "risk assessment is devalued" and "probabilistic thinking is repudiated in favor of "possibilistic thinking."<sup>21</sup>

What is necessary is due consideration to the spectrum of threats, not simply the worst one imaginable, in order to properly understand, and to coherently deal with, the risks to people, institutions, and the economy. The relevant decision-makers are professionals, and it is not unreasonable to suggest that they should do so seriously. Notwithstanding political pressures, the fact that the public has difficulties with probabilities when emotions are involved does not relieve those in charge of the requirement, even the duty, to make decisions about the

expenditures of vast quantities of public monies in a responsible manner.

# Adding, Rather than Multiplying, the Probabilities

A second stratagem for neglecting probability that is sometimes applied at DHS is to devise a rating scale where probabilities of attack are added to the losses. Thus, as a Congressional Research Service analysis points out, to determine whether a potential target should be protected, DHS has frequently assessed the target's vulnerability and the consequences of an attack on it on an 80 point scale and the likelihood it will be attacked on a 20 point ranked scale. It then adds these together.22 Thus, a vulnerable target whose destruction would be highly consequential would be protected even if the likelihood it will be attacked is zero, and a less consequential target could go unprotected even if the likelihood it will be attacked is 100 percent.

This procedure violates the principles espoused in all risk assessment techniques such as those codified in international risk management standards supported by twentysix countries including the United States.23 In these risk is invariably taken to be a product in which the attack probability is multiplied by the losses, not added to them. Essentially, what often seems to be happening is that DHS has a pot of money to dole out, and it has worked out a method for determining which projects are most worthy while avoiding determining whether any of them are actually worth any money at all.

# Assessing Relative, Rather than Absolute, Risk

A third technique, related to the second, is, as the CRS study points out, simply to rank relative risk while neglecting to determine the actual magnitude of the risk.<sup>24</sup> The 2010 National Research Council study finds this approach to be wanting:

Risk management decisions seek to reduce risks in accordance with specified, absolute risk criteria for human health protection. Many of the risk analyses thus far conducted by DHS involve risk ranking, based on scales of presumed relative risks, and do not include attempts to provide absolute measures of risk.<sup>25</sup>

It may be true that New York is more likely to be struck by a terrorist than, say, Columbus, Ohio. But it is also more likely to be struck by a tsunami, and not only in Hollywood disaster thrillers. Before spending a lot of money protecting New York from a tsunami, we need to get some sort of sense about what the likelihood of that event actually is, not simply how the risk compares to that borne by other cities. And the same goes for terrorism.

# Inflating the Importance of Potential Terrorist Targets

A fourth stratagem is to inflate the importance of potential terrorist targets. Thus, nearly half of American federal homeland security expenditure is devoted to protecting what the Department of Homeland Security and various presidential and Congressional reports and directives rather extravagantly call "critical infrastructure" and "key resources."

Applying common sense English about what "critical infrastructure" could be taken to mean, it should be an empty category. If any element in the infrastructure is truly "critical" to the operation of the country, steps should be taken immediately to provide redundancies or backup systems so that it is no longer so. An official definition designates "critical infrastructure" to include "the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof."26 Yet vast sums of money are spent under the program to protect elements of the infrastructure whose incapacitation would scarcely be "debilitating" and would at most impose minor inconvenience and guite limited costs.

And the same essentially holds for what DHS designates as "key resources," or formerly as "key assets." These are defined to be those that are "essential to the minimal operations of the economy or government."<sup>21</sup> It is difficult to imagine what a terrorist group armed with

anything less than a massive thermonuclear arsenal could do to hamper such "minimal operations." The terrorist attacks of 9/11 were by far the most damaging in history, yet, even though several major commercial buildings were demolished, both the economy and government continued to function at considerably above the "minimal" level.

The very phrase, "homeland security," contains aspects of a similar inflation in its suggestion that that essential security of the entire country is at stake. In Canada, the comparable department is labeled with more accuracy and less drama simply as "public safety." Given the actually magnitude of the terrorist hazard, the homeland is, as it happens, really quite secure, though there may be justifiable concerns about the public's safety under some conditions.

### Inflating Terrorist Capacities

A final stratagem is to fail to assess, or massively to inflate, the capacities of the terrorists, and therefore by inference both the likelihood they will attack and the consequences of that attack. This is something that should be of absolutely key importance yet, in its big national infrastructure protection report of 2009, the DHS devotes only two paragraphs to describing the nature of the "terrorist adversary" — a designation that implies far more coordination among terrorists than experience suggests is valid.<sup>28</sup> Moreover. none of this fleeting discussion shows any depth, and the report prefers instead to spew out adjectives like "relentless," "patient," and "flexible," terms that scarcely characterize the vast majority of potential terrorists.

The report goes on to argue without qualification that the "terrorist adversary" not only "shows an understanding of the potential consequence of carefully planned attacks on economic, transportation, and symbolic targets," but that it "seriously threatens national security, and could inflict mass casualties, weaken the economy, and damage public morale and confidence." This too is a rather extravagant exaggeration of the threat most terrorists present.

The ultimate in such thinking — common during the administration of George W. Bush.

and continued more sporadically in the administration of his successor, Barack Obama — is to characterize the terrorist threat as "existential." In 2008, Homeland Security Secretary Michael Chertoff even proclaimed the "struggle" against terrorism to be a "significant existential" one — carefully differentiating it, apparently, from all those insignificant existential struggles Americans have waged in the past.<sup>29</sup> Rather amazingly, such extreme expressions, which if accepted as valid, can close off all judicious evaluation of the problem, have only rarely been called into question.

In stark contrast, Glenn Carle, a twenty-threeyear veteran of the Central Intelligence Agency, where he was deputy national intelligence officer for transnational threats, has warned "We must not take fright at the specter our leaders have exaggerated. In fact, we must see jihadists for the small, lethal, disjointed and miserable opponents that they are." Al-Qaeda "has only a handful of individuals capable of planning, organizing and leading a terrorist organization," and although they have threatened attacks, "its capabilities are far inferior to its desires."<sup>30</sup>

In evaluating al-Qaeda's present capacity to inflict damage and its likelihood of doing so, a good place to start is with analyses provided by Marc Sageman.<sup>31</sup> A former intelligence officer with experience in Afghanistan, Sageman has carefully and systematically combed through both open and classified data on jihadists and would-be jihadists around the world.

Al-Qaeda central, he concludes, consists of a cluster less than 150 actual people. Other estimates of the size of al-Qaeda central generally come in with numbers in the same order of magnitude as those suggested by Sageman.<sup>32</sup> Sageman may be going too far when he argues "there is not much left of al-Qaeda except in the minds of those inside the beltway."<sup>33</sup> But that possibility should be included in the discussion at least as much as ones that confer on al-Qaeda capacities that are at once monumental and mounting.

Beyond the tiny band that constitutes al-Qaeda central, there are, continues Sageman, thousands of sympathizers and wouldbe jihadists spread around the globe who mainly connect in Internet chat rooms, engage in radicalizing conversations, and variously dare each other to actually do something.<sup>34</sup> All of these rather hapless — perhaps even pathetic — people should of course be considered to be potentially dangerous. From time to time they may be able to coalesce enough to carry out acts of terrorist violence, and policing efforts to stop them before they can do so are certainly justified. But the notion that they present an existential threat to just about anybody seems at least as fanciful as some of their schemes.

By 2005, after years of well-funded sleuthing, the FBI and other investigative agencies noted in a report that they had been unable to uncover a single true al-Qaeda sleeper cell anywhere in the United States, a finding (or non-finding) publicly acknowledged two years later in a press conference and when the officer who drafted that year's National Intelligence Estimate testified that "we do not see" al-Qaeda operatives functioning inside the United States.<sup>35</sup> Indeed, they have been scarcely able to unearth anyone who might even be deemed to have a "connection" to the diabolical group.

It follows that any terrorism problem in the United States and the West principally derives from rather small numbers of homegrown people, often isolated from each other, who fantasize about performing dire deeds and sometimes receive a bit of training and inspiration overseas. Indeed, in testimony on January 11, 2007, Mueller stressed that his chief concern within the United States had become homegrown groups, a sentiment later endorsed by Obama's Homeland Security Secretary Janet Napolitano in 2009.<sup>36</sup>

Assessing the threat from homegrown Islamist terrorists, Brian Jenkins stresses that their number is "tiny," representing one out of every 30,000 Muslims in the United States. This "very low level" of recruitment finds very little support in the Muslim community at large: "they are not Mao's guerrillas swimming in a friendly sea." Given this situation, concludes Jenkins, what is to be anticipated is "tiny conspiracies, lone gunmen, one-off attacks rather than sustained terrorist campaigns."<sup>37</sup> In the meantime, note other researchers, Muslim extremists have



been responsible for one fiftieth of one percent of the homicides committed in the United States since 9/11.38

Because terrorism of a considerably destructive nature can be perpetrated by a very small number of people, or even by a single individual, the fact that terrorists are few in number does not mean there is no problem, and from time to time some of these people may actually manage to do some harm, though in most cases their capacities and schemes or alleged schemes — seem to be far less dangerous than initial press reports suggest.

The situation seems scarcely different in Europe and other Western locations. Political scientist Michael Kenney has interviewed dozens of officials and intelligence agents and analyzed court documents. He finds that, in sharp contrast with the boilerplate characterizations favored by the DHS, Islamic operationally militants there are unsophisticated, short on knowhow, prone to make mistakes, poor at planning, and limited in their capacity to learn.<sup>39</sup> Another study documents the difficulties of network coordination that continually threaten operational unity, trust, cohesion, and the ability to act collectively.40

For several decades, the United States State Department collected data on international or transnational terrorism, defining the act as premeditated, politically motivated violence perpetrated by subnational groups or clandestine agents against noncombatant targets (civilians and military personnel who at the time of the incident are unarmed or not on duty) that involve citizens or the territory of more than one country.41 The number of people worldwide who died during the period as a result of all forms of transnational terrorism (Islamist or other) by this definition is 482 a year. Another study using comparable data for the longer period from 1968 to 2006 arrives at an average of 420 per year.42

Another approach is to focus on the kind of terrorism that really concerns people in the developed world by restricting the consideration to violence committed by Muslim extremists outside of war zones, whether that violence be perpetrated by domestic Islamist terrorists or by ones with international connections. Included in the count would be terrorism of the much publicized sort that occurred in Bali in 2002 and 2005, in Saudi Arabia, Morocco, and Turkey in 2003, in the Philippines, Madrid, and Egypt in 2004, and in London and Jordan in 2005. Three publications from think tanks have independently provided lists or tallies of such violence committed in the several years after the 9/11 attacks.<sup>43</sup> The lists include not only attacks by al-Qaeda but also those by its imitators, enthusiasts, lookalikes, and wannabes, as well as ones by groups with no apparent connection to it whatever. Although these tallies make for grim reading, the total number of people killed in the years after 9/11 by Muslim extremists outside of war zones comes to some 200 to 300 per year. That, of course, is 200 to 300 too many, but it hardly suggests that the destructive capacities of the terrorists are monumental. For comparison, during the same period more people — 320 per year — drowned in bathtubs in the United States alone.44 Or there is another, rather unpleasant comparison, Increased delays and added costs at U.S. airports due to new security procedures provide incentive for many short-haul passengers to drive to their destination rather than flying, and, since driving is far riskier than air travel, the extra automobile traffic generated has been estimated in one study to result in 500 or more extra road fatalities per year.45

# Evaluating Increases in Homeland Security Spending in the United States

In the end, one might darkly suspect, various versions of probability neglect are grasped because, if realistic probabilities that a given target would be struck by terrorists were multiplied into the risk calculation and if the costs of protection from unlikely threats were sensibly calculated following standard procedures, it would be found that vast amounts of money have been misspent.

Although measuring risk can be difficult, it is done as a matter of course in other areas including such highly charged ones as nuclear power plant accidents (where malevolent threats are explicitly considered), aviation safety, and environmental protection. Moreover, there is plenty of data on how much

damage terrorists have been able to do over the decades and about how frequently they attack. Seen in reasonable context, both of these numbers are exceedingly small, at least outside of war zones.

The insurance industry has a distinct financial imperative to understand terrorism risks. In the immediate aftermath of the 9/11 attacks in which insured losses reached \$35 billion, most insurance firms placed terrorism exclusions on their policies.<sup>46</sup> Since then, however, the United States government implemented the Terrorism Risk Insurance Act to provide "a temporary window of reinsurance relief to help insurers manage the ongoing risk of terrorism."47 With that, insurance firms re-entered the terrorism insurance market, and by 2009 the median terrorism insurance premium for a \$303 million property had more than halved to only \$9,541 per year.48 This represents a conservative measure of expected loss or risk, and a simple back-calculation in the risk equation suggests that the insurer estimates the likelihood of a

terrorist attack on a property to be very low: less than one in thirty thousand per year.<sup>49</sup> If the private sector can estimate terrorism risks and is willing to risk its own money on the validity of the estimate, why can't the DHS?

It is certainly true that improbable disastrous events — like the 9/11 attacks — do sometimes transpire. That is, in fact, why we call them improbable as opposed to impossible. But because improbable events sometimes do take place does not mean that all improbable events therefore become probable. To avoid or to ignore this elemental consideration is to engage in faulty, even irrational, planning and decision-making.

A conventional approach to cost-effectiveness compares the costs of security measures with the benefits as tallied in lives saved and damages averted. A security measure is costeffective when the benefit of the measure outweighs the costs of providing the security measures.

#### Benefit

The benefit of a security measure is a function of three elements:

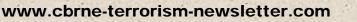
# Benefit = (probability of a successful attack) × (losses sustained in the successful attack) × (reduction in risk)

In the matter at hand, where we are concerned with the cost-effectiveness of enhanced (post-9/11) security expenditures, the probability of a successful attack is the likelihood a successful terrorist attack will take place if no new security measures were put into place. As discussed earlier, terrorism, at least outside war zones, is very infrequent: it is a low-probability event.

The losses sustained in the successful attack include the fatalities and other damage — both direct and indirect — caused by the terrorist attack, taking into account the value and vulnerability of people and infrastructure as well as any psychological and political effects. A successful terrorist attack can inflict costs in the tens of millions of dollars. Exceptional attacks, like the one on 9/11, can cost \$200 billion, and losses could conceivably reach five trillion dollars for the nightmare scenario of the detonation of a sizeable nuclear device in a densely populated area of a city.<sup>50</sup>

The third and final consideration in calculating the benefit of the security expenditures is the reduction in risk, which in this case concerns the effectiveness of the security measures to foil, deter, disrupt, or protect against a terrorist attack.<sup>51</sup> That is, it is the degree to which new security measures reduce the likelihood of a successful terrorist attack and/or the losses sustained in such an attack.

In assessing risk reduction, it is important first to look at the effectiveness of homeland security measures that were in place before 9/11 in reducing risk. The 9/11 Commission's report points to a number of failures, but it acknowledges as well that terrorism was already a high priority of the United States government before 9/11.<sup>52</sup> More pointed is an observation of Michael Sheehan, former New York City Deputy Commissioner for Counterterrorism:



The most important work in protecting our country since 9/11 has been accomplished with the capacity that was in place when the event happened, not with any of the new capability bought since 9/11. I firmly believe that those huge budget increases have not significantly contributed to our post-9/11 security.... The big wins had little to do with the new programs.<sup>53</sup>

As this suggests, police and domestic intelligence agencies have long had in place procedures, techniques, trained personnel, and action plans to deal with bombs and shootings and those who plot them. Indeed, according to 9/11's chief planner, Khalid Sheikh Mohammed, the greatest difficulty the plotters faced was getting their band of terrorists into the United States. It may be even more difficult now, but the strictures before already presented a considerable hurdle.<sup>54</sup>

There is another consideration. The tragic events of 9/11 massively heightened the awareness of the public to the threat of terrorism, resulting in extra vigilance that has often resulted in the arrest of terrorists or the foiling of terrorist attempts. Most dramatically, because airplane passengers have become much more attuned to suspicious or dodgy behavior of their fellow passengers, two terrorist attempts to blow up airliners have been foiled: the shoe bombing effort of 2001 and the underwear effort of 2009. Both were detected and restrained by crews and passengers, not by the many costly enhanced security measures put into place by the TSA. The same holds for the peddler in New York who reported the smoking vehicle bomb in Times Square in 2010. Indeed, tip-offs have been key to prosecutions in many of the terrorism cases in the United States since 9/11. Importantly, the inspiration of extra vigilance comes at no cost to the taxpayer.

In our analysis we will assume that risk reduction caused by the security measures in place before 9/11 and by the extra vigilance of the public after that event reduced risk by 50 percent. This is an exceedingly conservative estimate not only because of Sheehan's observation, but because security measures that are at once effective and relatively inexpensive are generally the first to be implemented — for example, one erects

warning signs on a potentially dangerous curve in the road before rebuilding the highway. Furthermore, most terrorists (or would-be terrorists) do not show much intelligence, cleverness, resourcefulness, or initiative, and therefore measures to deal with them are relatively inexpensive and are likely to be instituted first. Dealing with the smarter and more capable terrorists is more difficult and expensive, but these people represent, it certainly appears, a decided minority among terrorists.

In addition, we will assume that the increase in US expenditures on homeland security since 2001 has been dramatically effective, reducing the remaining risk by an additional 45 percent. Total risk reduction, then is generously assumed to be 95 percent with the pre-existing measures and the extra public vigilance responsible for 50 percent of the risk reduction and the enhanced expenditures responsible for the remaining 45 percent.

#### Cost

As indicated, benefits are a multiplicative composite of three considerations: the probability of a successful attack, the losses sustained in a successful attack, and the reduction in risk furnished by security measures. This product, the benefit, is then compared to the cost of the security measures instituted to attain the benefit.

For the purposes of this analysis, we assess only the costs of increased government expenditures on homeland security after the 9/11 attacks. That is, we assume homeland security measures in place before the attacks continue, and we evaluate the additional funds that have been allocated to homeland security, almost all of it designed, of course, to deal with terrorism, the only hazard that notably inspired increased alarm after the attacks.

United States federal government spending on homeland security increased from \$20.1 billion in 2001,<sup>55</sup> to \$75 billion in 2009.<sup>56</sup> In all, federal government spending on homeland security for 2009 was \$75 billion or \$50 billion higher in 2010 dollars than in 2001, adjusting for inflation.<sup>57</sup>



To limit our focus to increases in expenditures by the federal government reported by the OMB would be a considerable restriction because this ignores the recently declassified national intelligence costs as well as state and local government outlays on homeland security. As shown in Table 1, we conservatively estimate enhanced intelligence expenditures since 9/11 devoted to domestic homeland security to be \$15 billion in 2009. As the Table also indicates, enhanced outlays for state and local homeland security spending are approximately \$10 billion per year.

The increase in annual federal government outlays, then, is \$50 billion per year, and the addition of national intelligence and state and local homeland security outlays of \$25 billion gives a total of \$75 billion. We will use this figure, although it is a very conservative measure of the degree to which homeland security expenditures have risen since 9/11 because we do not include several other items totaling (far) more than \$200 billion per year as tallied in Table 1. These include (1) private sector expenditures on homeland security related measures costing \$10 billion per year; (2) terrorism risk insurance premiums of nearly \$4 billion per year; (3) hidden and indirect costs or "dead weight losses" of implementing security-related regulations that amounted to at least \$30 billion in lost output per year; (4) various opportunity costs including those attendant on the increase of 500 traffic fatalities per year due to increased delays and added costs at airports diverting many short-haul passengers to their cars instead valued at \$3.2

billion, as well as other opportunity costs; and (5) the costs of the terror-related wars in Iraq and Afghanistan which reached \$150 billion in 2009.

#### Results

To summarize, our analysis for the United States applies these estimates and assumptions:

- We assume those security measures in place before 9/11 continue and that these, combined with the extra public vigilance induced by 9/11, reduce the likelihood of a successful terrorist attack or reduce the losses sustained in such an attack by 50 percent;
- We assume the enhanced security expenditures since 9/11 have successfully reduced the likelihood of a successful terrorist attack or have reduced the losses sustained in such an attack by a further 45 percent, leading to an overall risk reduction of 95 percent; and
- We include in our cost measure only enhanced local, state, and federal security expenditures and enhanced intelligence costs since 9/11 (totaling \$75 billion per year), leaving out many other expenditures including those incurred by the private sector, opportunity costs, and the costs of the terror-related wars in Iraq and Afghanistan.

Table 2 puts this all together. It displays the benefit generated by enhanced security measures if they have been able to prevent or protect against an otherwise successful attack for a range of losses from a successful attack and for a range of annual attack probabilities.

Table 2. Net benefit in billions of dollars for US enhanced homeland security expenditures of

\$75 billion per year assuming these have reduced risks by 45 percent

	Losses from a successful terrorist attack						
Annual Probability of a successful attack	\$100 million	\$1 billion	\$5 billion	\$100 billion	\$200 billion	\$1 trillion	\$5 trillion
in the absence of security expenditures	1.1.1		London Bombing	1984	9/11	Nuclear Port	Nuclear Grand Central
0.1%	-75	-75	-75	-75	-75	-75	-73
dale and considered days.		· Jan - Your	1. 147. C.	Elle (1)		147. 2. 42	

a state of the sta	and the second second second			Contraction of the local division of the loc			
1.0%	-75	-75	-75	-75	-74	-71	-53
5.0%	-75	-75	-75	-73	-71	-53	38
10.0%	-75	-75	-75	-71	-66	-30	150
25.0%	-75	-75	-74	-64	-53	38	488
50.0%	-75	-75	-74	-53	-30	150	1050
100.0% <sup>1</sup>	-75	-75	-73	-30	15	375	2175

Note: Each entry above represents the benefit-minus-cost result for each loss and for each attack probability. Entries that are positive would be considered to be cost-effective. A value of -75 denotes no benefit.

	Break-Even Analysis								
The number of otherwise successful attacks averted by security expenditures required for the enhanced expenditures to be cost- effective at several levels of loss—that is, for the security benefit of the expenditures to equal their costs									
	1667	167	33	2	1	1	1		
a :	per year	per	per	per	per	in 6	in 30		
	per year	vear	vear	vear	vear	vears	vears		

#### <sup>1</sup>One per year.

In the years since 2001 (or, for that matter, in those previous to it), al-Qaeda-like terrorists operating outside of war zones have generally inflicted less than \$1 million in property damage and a limited number of fatalities in each successful attack. A monetary value of the destruction wreaked in attacks like that would be tens of millions of dollars.58 Something like that would probably have been the losses inflicted if the Times Square bomber of 2010 had carried out what seems to have been his mission, though possibly the damage

could have been higher. Of late, a number of analysts and policy makers have suggested that these are the kind of attacks that are far the most likely. If a loss of \$100 million - a high estimate for small successful attacks — is taken to be the approximate norm, Table 2 indicates in the first column that, even if the likelihood of such an attack were 100 percent per year without the security measures, the money spent to prevent or protect against them would not be worth it: the costs of security would outweigh the benefit of the security.

years

years

There is another way to look at this. If

# Benefit = (probability of a successful attack) × (losses sustained in the successful attack) × (reduction in risk)

the same equation can be used in a break-even analysis to calculate how many attacks would have to take place to justify the expenditure. That is, thinking of the "benefit" as the cost of the security measure:

# (probability of a successful attack) = security cost/[(losses sustained in the successful attack) × (reduction in risk)]

Thus for a successful terrorist attack in which the security cost in \$75 billion, losses sustained are \$100 million, and the reduction in risk is .45, the probability of a successful attack would need to be at least

# (probability of a successful attack) > \$75 billion/[\$100 million × .45] = 1667 attacks per year



That is, in order for enhanced United States expenditures on homeland security to be deemed cost-effective under our approach which substantially biases the consideration toward the opposite conclusion — they would have to deter, prevent, foil, or protect each year against 1,667 otherwise successful attacks something like the one attempted on Times Square in 2010, or more than four per day. The array of numbers at the bottom on Table 2 gives this quantity for a variety of loss levels. Even for attacks inflicting \$1 billion in damage, the frequency would have to be about one every other day.

The losses from attacks like those of July 2005 in London would not exceed five billion dollars. For enhanced security measures to be costeffective for attacks of that magnitude, their rate of occurrence without those enhanced measures would have had to exceed thirty per year.<sup>59</sup> If we posit that such an attack is thwarted once per year (a conservative threat likelihood by any measure) the ratio of benefit to cost is a meager 0.03 meaning that spending \$1 buys only three cents of benefits.<sup>60</sup>

For a terrorist attack, or set of attacks, that, like those of September 11, 2001, caused \$200 billion dollars of destruction (something that has only occurred once in all of history), enhanced expenditures would be cost-effective only if that sort of attack would have occurred more than once a year without them. Moreover, it is not clear that other 9/11-like attacks would trigger the extreme economic reaction engendered by the original intensely shocking event — that is, the full costs of another 9/11 might not reach those sustained in the original event.

An extreme upper bound would be the detonation of a 10-kiloton nuclear device at New York's Grand Central Terminal on a busy day, a nightmare scenario that might exact losses of up to \$5 trillion. Enhanced homeland security expenditures would be cost-effective in this case only if, without them, such an extreme attack would have successfully been executed once every thirty years.<sup>61</sup> The same, roughly, would hold for another extreme scenario, one in which the terrorist attack triggers an expensive war like the one in Iraq.<sup>62</sup>

There are extreme scenarios that can be taken to suggest that enhanced U.S. security expenditures could be cost-effective — the nightmare nuclear vision as well as the costly overreaction scenario. However, for those who find such outcomes dangerously likely, the policy response would logically be to spend on reducing the risk of nuclear terrorism in the one case and to develop strictures to overreaction in the other. The logical policy response would not be, for example, to spend tens of billions of dollars each year on protection measures.

In virtually all contexts, then, overall enhanced expenditures on homeland security in the United States fail to be cost-effective spectacularly so in most instances — even in an analysis that very substantially biases the calculations in favor of the opposite conclusion. In consequence, a great deal of money appears to have been misspent and would have been far more productive — saved far more lives — if it had been expended in other ways.

We are not arguing that much of homeland security spending is wasteful because we believe there will be no more terrorist attacks. Like crime and vandalism, terrorism will always be a feature of life, and a condition of zero vulnerability is impossible to achieve. However, future attacks might not be as devastating as 9/11, as evidenced by the attacks on Western targets in the ten years since 9/11 that, although tragic, have claimed victims numbering in the tens to a few hundred — and none, certainly, have posed an existential threat. The frequency and severity of terrorist attacks are low, very low in fact, which makes the benefits of enhanced counterterrorism expenditures of a trillion dollars since 9/11 challenging, to say the least, to justify by any rational and accepted standard of cost-benefit analysis.

Our findings dealing with the total enhanced homeland security expenditures should not be taken to suggest that all security measures necessarily fail to be cost-effective: there may be specific measures that are cost-effective.<sup>63</sup> But each should be subjected to the kind of risk analysis we have applied to the overall increases in expenditure.

# Gauging the Impact of Counter-terrorism Measures on the Hazard

We have assessed the hazard terrorism poses under present conditions — which include, of course, the existence of counter-terrorism measures specifically designed to reduce that hazard. The analysis suggests that additional efforts to reduce its likelihood are scarcely justified.

It is possible, of course, that any relaxation in these measures will increase the terrorism hazard, that it is the counter-terrorism effort is the reason for the low hazard terrorism currently presents. However, in order for the terrorism risk to border on becoming "unacceptable" by established risk conventions — that is, to reach an annual fatality rate of one in 100,000 — the number of fatalities from all forms of terrorism in the U.S. would have to increase thirty-five-fold.<sup>64</sup>

Thus, to justify current counterterrorism efforts in this manner, one would need to establish, in the case of the United States, that the measures have successfully deterred, derailed, disrupted, or protected against attacks that would otherwise have resulted in the deaths of more than 3,000 people in the country every year, equivalent to experiencing attacks as devastating as those on 9/11 at least once a year or eighteen Oklahoma City bombings every year. Even if all the (mostly embryonic and in many cases moronic) terrorist plots exposed since 9/11 in the United States had been successfully carried out, their likely consequences would have been much lower. Indeed, as the earlier discussion indicates, the number of people killed by terrorists throughout the world outside (and sometimes within) war zones both before and after 2001 generally registers at far below that number.

### A Future Increase in Terrorist Destruction?

We have been using "historical" data here, and these suggest the chances an American will perish at the hands of a terrorist is about one in 3.5 million per year.<sup>65</sup> However, although there is no guarantee that the terrorism frequencies of the past will necessarily persist into the future, there seems to be little evidence terrorists are becoming any more destructive, particularly in the West. In fact, if anything, there seems to be a diminishing, not expanding, level of terrorist activity and destruction at least outside of war zones. As Andrew Mack concludes, there is "no evidence of any substantial increase in the fatality toll since data on both domestic and international terrorism began to be collected in 1998." Indeed, the two datasets he examines that have statistics going back to that year both "reveal a decline in deaths from terrorism."<sup>66</sup>

Moreover, as discussed earlier, according both to official and prominent academic accounts, the levels of violence likely to be committed by Islamic extremists within Western countries seems, if anything to be in decline. Fears about large, sophisticated attacks have been replaced by fears concerning tiny conspiracies, lone wolves, and one-off attackers.

Those who wish to discount such arguments and projections need to demonstrate why they think terrorists will suddenly get their act together and inflict massively increased violence, visiting savage discontinuities on the historical data series.<sup>67</sup> Moreover, they should also restrain themselves from using historical data themselves to explain, for example, why attacks on New York are more likely than ones on Xenia, Ohio, or Perth, Australia.

Actually, a most common misjudgment has been to embrace extreme events as harbingers presaging a dire departure from historical patterns. In the months and then years after 9/11, as noted at the outset, it was almost universally assumed that the terrorist event was a harbinger rather than an aberration.68 There were similar reactions to Timothy McVeigh's 1995 truck bomb attack in Oklahoma City as concerns about a repetition soared. And in 1996, shortly after the terrorist group Aum Shinrikyo set off deadly gas in a Tokyo subway station, one of terrorism studies' top gurus, Walter Laqueur, assured the world that some terrorist groups "almost certainly" will use weapons of mass destruction "in the foreseeable future."69 Presumably any future foreseeable in 1996 is now history, and Laqueur's near "certainty" has yet to occur.



### The Tradeoffs, Opportunity Costs

Risk reduction measures that produce little or no net benefit to society or produce it at a very high cost cannot be justified on rational lifesafety and economic grounds - they are not only irresponsible, but, essentially, immoral. When we spend resources on regulations that save lives at a high cost, we forgo the opportunity to spend those same resources on regulations and processes that can save more lives at the same cost, or even at a lower one. Homeland security expenditure invested in a wide range of more cost-effective risk reduction programs like flood protection, vaccination and screening, vehicle and road safety, health care, and occupational health and safety would likely result in far more significant benefits to society.

For example, diverting a few percent of the nearly \$10 billion per year spent on airline security could save many lives at a fraction of the cost if it were instead spent on such proven life savers as seat belts, bicycle helmets, spectrometry screening tandem mass programs, airbags, smoke alarms, and tornado shelters. A government obliged to allocate funds in a manner that best benefits society must explain why it is spending billions of dollars on security measures with very little proven benefit and why that policy is something other than a reckless waste of resources.

It may be useful in this light to put counterterrorism expenditures in broadest comparative context. A group of international experts assembled by Bjorn Lomborg applied cost-benefit thinking to a wide range of issues and found many in which the benefit is ten times greater than the cost and in which the number of lives saved is spectacular. According to these analysts, an investment of merely \$2 billion could save over 1.5 million lives: one million child deaths could be averted by expanded immunization coverage while community-based nutrition programs could save another half a million. If a miserly \$2 billion were redirected from the homeland security budget. the likelihood and consequences of such attacks would hardly change, but anywhere from 300 to 60,000 times more lives - albeit not necessarily American or Western ones - would be saved if the funds were instead spent on the risk

reducing measures suggested by Lomberg and his associates.<sup>70</sup>

# **Political Realities**

Politicians and bureaucrats do, of course, face considerable political pressure on the terrorism issue. In particular, they are fully wary of the fact that Jeffrey Rosen is on to something when he suggests that "we have come to believe that life is risk free and that, if something bad happens, there must be a government official to blame."<sup>71</sup>

The dilemma is nicely parsed by James Fallows. He points out that "the political incentives here work only one way." A politician supports more extravagant who counterterrorism measures "can never be proven wrong" because an absence of attacks shows that the "measures have lsquo;worked'," while a new attack shows that we "must go farther still." Conversely, a politician seeking to limit expenditure "can never be proven Isquo;right'" while "any future attack will always and forever be that politician's lsquo;fault'." Or in the words of Michael Sheehan, "No terrorism expert or government leader wants to appear soft on terrorism. It's always safer to predict the worst; if nothing happens, the exaggerators are rarely held accountable for their nightmare scenarios."72

In Friedman's view, the problem is quite general not only in government and political agencies, but in associated think tanks: "the path of least resistance is to write about how to control a danger instead of evaluating its magnitude." And, although such analysts "rarely take orders," at the same time "few offer analyses that harms their benefactors." It is a rare bureaucrat or expert, he contends, who "will voice opinions harmful to his organization or prospects for appointment, but even fewer will offer those opinions without being asked, and few policy-makers will ask."<sup>73</sup>

# **Explaining Risk versus Stoking Fear**

However, nothing in all this relieves politicians and bureaucrats of the fundamental responsibility of informing the public honestly and accurately of the risk that terrorism presents. Daniel Gardner notes that the failure of Bush administration "to put the risk in perspective was total."<sup>74</sup> That continues to be the case with the new one.

the emphasis has Instead. been on exacerbating fears. As Friedman aptly notes, "For questionable gains in preparedness, we spread paranoia" and facilitate the bureaucratically and politically appealing notion that "if the threat is everywhere, you must spend everywhere," while developing and perpetrating the myth, or at least the impression, that the terrorists are omnipotent and omnipresent.<sup>75</sup>

Thus it was in 2003 that Homeland Security Secretary Tom Ridge divined that "extremists abroad are anticipating near term attacks that they believe will either rival, or exceed" those of 2001. And in 2004, Attorney General John Ashcroft, with FBI Director Robert Mueller at his side, announced that "credible intelligence from multiple sources indicates that al-Qaeda plans to attempt an attack on the United States in the next few months," that its "specific intention" was to hit us "hard," and that the "arrangements" for that attack were already 90 percent complete. (Oddly enough, Ashcroft fails to mention this memorable headlinegrabbing episode in Never Again, his 2006 memoir of the period.) In 2003 Director Mueller reported that, although his agency had yet actually to identify an al-Qaeda cell in the U.S., such unidentified (or imagined) entities nonetheless presented "the greatest threat," had "developed a support infrastructure" in the country, and had achieved both the "ability" and the "intent" to inflict "significant casualties in the U.S. with little warning." In 2005, at a time when the FBI admitted it still had been unable to unearth a single true al-Qaeda cell. Mueller continued his dire I-think-thereforethey-are projections: "I remain very concerned about what we are not seeing," he ominously ruminated.<sup>76</sup> Needless to say, the media remained fully in step. Thus, on the fifth anniversary of 9/11, ABC's Charles Gibson dutifully intoned, "Putting your child on a school bus or driving across a bridge or just going to the mall - each of these things is a small act of courage — and peril is a part of everyday life."77

Terrorism induced fears can be debilitating. For one thing they can cause people routinely to adopt skittish, overly risk averse behavior, at least for a while, and this can much magnify the impact of the terrorist attack, particularly economically. That is, the problem is not that people are trampling each other in a rush to vacate New York or Washington, but rather that they may widely adopt other forms of defensive behavior, the cumulative costs of which can be considerable. As Cass Sunstein notes. "in the context of terrorism, fear is likely to make people reluctant to engage in certain activities, such as flying on airplanes and appearing in public places," and "the resulting costs can be extremely high."78

Yet, despite the importance to responsible policy of seeking to communicate risk and despite the costs of irresponsible fearmongering, just about the only official who has ever openly put the threat presented by terrorism in some sort of context is New York's Mayor Michael Bloomberg who, in 2007, pointed out that people should "get a life" and that they have a greater chance of being hit by lightning than of being struck by terrorism.<sup>79</sup>

Things are not much better in the media. There seemed to be a brief glimmer on the December 28, 2009, PBS NewsHour when Gwen Ifill, in introducing a segment on the then-recent underwear bomber's attempt to down an airliner, actually happened to note that the number of terrorist incidents on American airliners over the previous decade was one for every 16.5 million flights.<sup>80</sup> This interesting bit of information, however, was never brought up again either by Ifill or by the three terrorism experts she was interviewing. Nor, of course, did anyone think of suggesting that, at that rate, maybe the airlines are already safe enough.

In 2007, now-former CIA Director Tenet revealed on CBS' 60 Minutes that his "operational intuition" was telling him that al-Qaeda had "infiltrated a second wave or a third wave into the United States at the time of 9/11," though he added, "Can I prove it to you? No." (One might think that aging members of that "wave" would have since had a great incentive to actually do something since the longer they linger, the greater the likelihood

they will be exposed and caught.) And DHS Secretary Michael Chertoff informed us a few months later that his gut was telling him there'd be an attack during that summer. It would seem that when officials responsible for public safety issue fear-inducing proclamations based by their own admission on nothing, they should be held to account. Then in 2010, Napolitano joined in announcing that, although the likelihood of a large-scale organized attack was reduced, the continued danger of a small-scale disorganized attack meant that the terrorist threat was somehow now higher than at any time since 9/11. As Ian Lustick puts it, the government "can never make enough progress toward 'protecting America' to reassure Americans against the fears it is helping to stoke."81

Political realities supply an understandable excuse for expending money, but not a valid one, and they do not relieve officials of the responsibility of seeking to expend public funds wisely. It is particularly important to do so with homeland security expenditures. They deal not with bridges to nowhere or with crop subsidies, but with public safety - or domestic tranquility - the central, fundamental reason for the existence of government in the first place. It is imperative that decisions be made sensibly and responsibly in this area. To be irrational with your own money may be to be foolhardy, to give in to guilty pleasure, or to wallow in caprice. But to be irrational with other people's money, particularly where public safety is the issue, is to be irresponsible, to betray an essential trust. In the end, it becomes a dereliction of duty that cannot be justified by political pressure, bureaucratic constraints, or emotional drives.

# Are Political Concerns Overwrought?

However, although political pressures may force actions and expenditures that are unwise, they usually do not precisely dictate the level of expenditure. Thus, although there are public demands to "do something" about terrorism, nothing in that demand specifically requires removing shoes in airport security lines, requiring passports to enter Canada, spreading bollards like dandelions, or making a huge number of buildings into forbidding fortresses. The United Kingdom, which seems to face an internal threat from terrorism that is considerably greater than that for the United States, appears nonetheless to spend proportionately much less than half as much on homeland security, and the same holds for Canada and Australia. Yet politicians and bureaucrats there do not seem to suffer threats to their positions or other political problems because of it.<sup>82</sup>

As this might suggest, it is possible politicians and bureaucrats are overly fearful about the political consequences. It is often argued that there is a political imperative for public officials to "do something" (which usually means overreact) when a dramatic terrorist event takes place — "You can't just not do anything." However, history clearly demonstrates that overreaction is not necessarily required. Sometimes, in fact, leaders have been able to restrain their instinct to overreact. Even more important, restrained reaction - or even capitulation to terrorist acts - has often proved to be entirely acceptable politically. This is a particularly important issue because it certainly appears that avoiding overreaction is by far the most cost-effective counterterrorism measure.

Consider, for example, the two instances of terrorism that killed the most Americans before September 2001. Ronald Reagan's response to the first of these, the suicide bombing in Lebanon in 1983 that resulted in the deaths of 241 American Marines, was to make a few speeches and eventually to pull the troops out. The venture seems to have had no negative impact on his reelection a few months later. The other was the December 1988 bombing of a Pan Am airliner over Lockerbie, Scotland, in which 187 Americans perished. Perhaps in part because this dramatic and tragic event took place after the elections of that year, the official response. beyond seeking to obtain compensation for the victims, was simply to apply meticulous police work in an effort to tag the culprits, a process that bore fruit only three years later and then only because of an unlikely bit of luck.83 But that cautious, even laid back, response proved to be entirely acceptable politically.

Similarly, after an unacceptable loss of American lives in Somalia in 1993, Bill Clinton



responded by withdrawing the troops without noticeable negative impact on his 1996 reelection bid. Although Clinton reacted with counterproductive) (apparently military retaliations after the two U.S. embassies were bombed in Africa in 1998, his administration did not have a notable response to terrorist attacks on American targets in Saudi Arabia (Khobar Towers) in 1996 or to the bombing of the U.S.S. Cole in 2000, and these non-responses never caused it political pain. George W. Bush's response to the anthrax attacks of 2001 did include a costly and wasteful stocking up of anthrax vaccine and enormous extra spending by the U.S. Post Office. However, beyond that, it was the same as Clinton's had been to the terrorist attacks against the World Trade Center in 1993 and in Oklahoma City in 1995 and the same as the one applied in Spain when terrorist bombed trains there in 2004 or in Britain after attacks in 2005: the dedicated application of police work to try to apprehend the perpetrators. This approach proved to be entirely acceptable politically. Similarly, the Indian government was able to neglect popular demands for retaliatory attacks on Pakistan for the damage inflicted on Mumbai in 2008 by terrorists based there.84

Thus, despite short-term demands that some sort of action must be taken, experience suggests politicians can often successfully ride out this demand after the obligatory and essentially cost-free expressions of outrage are prominently issued.

It is true that few voters spend a great amount of time following the ins and outs of policy issues and even fewer are certifiable policy wonks. But they are grown-ups, and it is just possible they would respond reasonably to an adult conversation about terrorism. After all, Mayor Bloomberg's "get a life" outburst in 2007 did not have negative consequences for him. He is still in office and, although he had some difficulties in his reelection two years later, his blunt comments about terrorism were not the cause.

There is also a tendency to assume that the outsized reaction to 9/11 will necessarily be repeated if there is another attack in the United States. However, London experienced a double hit in 2005: attacks on the underground

two weeks apart (of which only the first was successful). But the politicians in charge survived. Also potentially relevant here is the fact that terrorist attacks on resort areas in Bali in 2002 had a far larger negative impact on tourism than did subsequent ones in 2005.

Interesting in this regard is the remarkably muted reaction of the American public (and media) to the 2009 shootings by a Muslim psychiatrist at Fort Hood, Texas, that killed thirteen and injured thirty more. Although this could be considered to an act of a deranged man, it is generally taken to be a case of Islamic terrorism, and it is by far the worst since 9/11 in the United States. Although obviously far less costly than the earlier terrorist event, it could have been taken to be the next step in a terrorist onslaught something that Americans have long been ominously waiting for. However, it failed to generate much outrage or demand for an outsized response. Indeed, a year later it was scarcely remembered, as when the prominent journalist, James Fallows, mused about raising "the certainty that some day another terrorist attack will succeed" without noting that one had already taken place.85

Then in 2010, President Barack Obama rather candidly observed to Washington Post reporter Bob Woodward, "We can absorb a terrorist attack. We'll do everything we can to prevent it, but even a 9/11, even the biggest attack ever ... we absorbed it and we are stronger."<sup>26</sup> This may have been the first time any official acknowledged the issue in public, and Obama even used the unpleasant word "absorb" rather than the more politically correct "resilient." Obama's highly unconventional statement drew great attention in the press, but it hardly seems to have hurt the President's effectiveness or approval ratings.

Terrorism can inspire self-destructive overreaction like no other hazard, and this can be massively costly — the two wars impelled or facilitated by 9/11 are only the most vivid examples. Indeed, the costs of overreaction can be far higher than those inflicted by the terrorists themselves — as they were even for 9/11, by far the most destructive terrorist act in history.<sup>97</sup> Osama bin Laden has gloated over this phenomenon, claiming his goal is to bleed

America into bankruptcy, something only the United States could do to itself.<sup>88</sup>

The notion that this is a problem seems to be dawning on people considering terrorism. In 2004, Stephen Flynn began an article by dramatically proclaiming that the United States is "living on borrowed time - and squandering it" and ending it with a warning about the "long, deadly struggle against terrorism." He also admitted that he often labored under a sense of despair and dread and suggested that officials must assume that terrorists will "soon" launch attacks far more deadly and disruptive than those of 9/11.89 And late in the same year he contributed to an op-ed article vividly entitled "Our Hair Is on Fire'," declaring that al-Qaeda had both the ability and the intent to detonate a weapon of mass destruction in the United States and envisioning graves by the hundreds of thousands, the collapse of the economy, and "perhaps a fatal blow to our way of life."90 However, by 2010, he was arguing that the greatest threat from terrorism "comes from what we would do to ourselves when we are spooked" and that is it this "that makes it an appealing tool for our adversaries."91

And in early 2005, Richard Clarke, counterterrorism coordinator from the Clinton administration, issued a scenario that appeared in the Atlantic as a cover story in which he

darkly envisioned shootings at casinos, campgrounds, theme parks, and malls in 2005, bombings in subways and railroads in 2006, missile attacks on airliners in 2007, and devastating cyber attacks in 2008.92 By 2010, however, he was advocating that "we should not adopt procedures that inconvenience the public more than they do the terrorists and amount to little more than security theater," that "those who seek political gain from the murder of Americans" should be "regarded as despicable," and that, should terrorists successfully attack again, we should "refine our tactics and procedures," but "not overreact." To do this, however, notes Clarke, would require "a good dose" of that oxymoronic commodity, "political courage."93

The 2004 article in which Flynn proclaimed the United States to be "living on borrowed time — and squandering it" and warned about the "long, deadly struggle against terrorism" also includes something of a midcourse correction. In seeking to supply a standard for "how much security is enough," he suggested that that happy moment would come about when "the American people can conclude that a future attack on U.S. soil will be an exceptional event that does not require wholesale changes in how they go about their lives."<sup>94</sup> It seems reasonable to suggest that they can do so right now — and, for that matter, could have done so in 2004.

John Mueller is professor of political science at Ohio State University. He is the author of over a dozen books, several of which have won prizes. Among the most recent: The Remnants of War (2004), Overblown (2006), and Atomic Obsession: Nuclear Alarmism from Hiroshima to Al-Qaeda (2010). He is also editor of Terrorism Since 9/11: The American Cases published as a web book in 2011 by the Mershon Center at OSU, http://polisci.osu.edu/faculty/jmueller/since.html. He has published extensively in scholarly journals and general magazines and newspapers, is a member of the American Academy of Arts and Sciences, and has been a John Simon Guggenheim Fellow. In 2009, Mueller received the International Studies Association's Susan Strange Award as one "whose singular intellect, assertiveness, and insight most challenge conventional wisdom and intellectual and organizational complacency in the international studies community." For more information or to contact John Mueller, please go to www.polisci.osu.edu/faculty/jmueller.

Mark G. Stewart is professor of civil engineering and director of the Centre for Infrastructure Performance and Reliability at the University of Newcastle in Australia. He is the lead author of Probabilistic Risk Assessment of Engineering Systems (Chapman & Hall, 1997), as well as more than 300 technical papers and reports. He has more than twenty-five years of experience in probabilistic risk assessment of infrastructure systems that are subject to man-made and natural hazards. Since 2004, Stewart has received extensive Australian Research Council support to develop probabilistic terrorism risk-modeling techniques for buildings subject to explosive blasts and cost-benefit assessments of counterterrorism protective measures for critical infrastructure. In 2011, he received a five-year Australian Professorial Fellowship from the ARC to continue and to extend that work. For more information or to contact Mark Stewart, please go to www.newcastle.edu.au/researchcentre/cipar/staff/mark-stewart.html.



107

#### Notes:

- Howard Kunreuther, "Risk Analysis and Risk Management in an Uncertain World," Risk Analysis 22, no. 4 (August 2002): 662-63. See also John Mueller, "Some Reflections on What, if Anything, Isquo;Are We Safer?' Might Mean," cato-unbound.com, 11 September 2006, www.cato-unbound.org/2006/09/11/john-mueller/arewe-safer/.
- 2. Bill Gertz, "5,000 in U.S. Suspected of Ties to al Qaeda; Groups Nationwide Under Surveillance," Washington Times, July 11, 2002; Richard Sale, "US al Qaida Cells Attacked," UPI, October 31, 2002.
- 3. Rudy Giuliani, interviewed on CNN, July 22, 2005.
- Veronique de Rugy, "The Economics of Homeland Security," in Terrorizing Ourselves: Why U.S. Counterterrorism Policy Is Failing and How To Fix It, eds. Benjamin H. Friedman, Jim Harper, and Christopher A. Preble (Washington, DC: Cato Institute, 2010), 123.
- 5. As he put it mockingly in a videotaped message in 2004, it is "easy for us to provoke and bait... All that we have to do is to send two mujahidin... to raise a piece of cloth on which is written al-Qaeda in order to make the generals race there to cause America to suffer human, economic, and political losses." He proclaimed his policy is one of "bleeding America to the point of bankruptcy," triumphally pointing to the fact that the 9/11 terrorist attacks cost al-Qaeda \$500,000 while the attack and its aftermath inflicted, he claims, "a cost of more than \$500 billion on the United States" (Full transcript of bin Laden's speech, aljazeera.net, October 30, 2004). However this was not his original idea. Initially, he apparently expected that the United States would essentially under react to the 9/11 attacks. Impressed, in particular, with the American reaction to rather small losses in Lebanon in 1983 and in Somalia in 1993, he appears to have believed that the country would respond to an attack on itself by withdrawing from the Middle East (Lawrence Wright, The Looming Tower: Al-Qaeda and the Road to 9/11 (New York: Knopf, 2006), 174, 200). Bin Ladin reformulated his theory after it was blown to shreds when the United States and its allies not only forced al-Qaeda out of its base in Afghanistan and captured or killed many of its main people, but also toppled the accommodating Taliban regime there.
- 6. Thomas H. Kean, Chair, The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States (Washington, DC: U.S. Government Printing Office, 2004), 391, 396
- 7. Matt A. Mayer, Homeland Security and Federalism: Protecting America from Outside the Beltway (Santa Barbara, CA: ABCCLIO, 2009), 62.
- Troy Anderson, "Terror May Be at Bay at Port; Shipping Hubs Too Vulnerable," The Daily News of Los Angeles, May 18,2006.
- 9. James A. Thomson, "DHS AWOL? Tough Questions About Homeland Security Have Gone Missing," RAND Review, (Spring 2007).
- Todd Masse, Siobhan O'Neil, and John Rollins, The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress (Washington, DC: Congressional Research Service, 2 February 2, 2007), 14.
- 11. National Research Council of the National Academies, Review of the Department of Homeland Security's Approach to Risk Analysis (Washington, DC: National Academies Press, 2010), 108.
- 12. Transportation Security Administration, "DHS Announces Security Standards for Freight and Passenger Rail Systems," Press Release, November 13, 2008.
- 13. Steve Lord, Aviation Security: TSA is Increasing Procurement and Deployment of the Advanced Imaging Technology, but Challenges to This Effort and Areas of Aviation Security Remain (United States Government Accountability Office, GAO10484T, March 17, 2010), 5. For our risk assessment of the scanners, concluding that they are unlikely to be cost-effective, see John Mueller and Mark G. Stewart, Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Homeland Security (New York: Oxford University Press, forthcoming 2011), chap. 7; and Mark G. Stewart and John Mueller, "Risk and CostBenefit Analysis of Advanced Imaging Technology Full Body Scanners for Airline Passenger Security Screening," Journal of Homeland Security and Emergency Management 8, no. 1, Article 30 (2011).
- 14. United States Government Accountability Office, Report to Congressional Requesters: Supply Chain Security: Feasibility and Cost-Benefit Analysis Would Assist DHS and Congress in Assessing and Implementing the Requirement to Scan 100 Percent of U.S.-Bound Containers, GAO-10-12 (Washington, DC: Government Printing Office, October 2009). See, however, Susan E. Martonosi, David S. Ortiz, and Henry H. Willis, Evaluating the Viability of 100 Percent Container Inspection at America's Ports (Santa Monica, CA: RAND Corporation, 2004).
- 15. National Research Council, Review of DHS Approach to Risk Analysis.
- Gregory F. Treverton, Intelligence for an Age of Terror (New York: Cambridge University Press, 2009), 24-25.
   Ibid, 188.
- 18. Cass R. Sunstein, "Terrorism and Probability Neglect," Journal of Risk and Uncertainty 26, no. 2/3 (MarchMay, 2003): 122.
- 19. Bruce Schneier, "Worst-Case Thinking," www.schneier.com, May 13, 2010.



20. Ibid.

- 21. Ibid.
- 22. Masse et al., DHS Risk Assessment Methodology, 6.
- 23. Such as the International Organization for Standardization standard, ISO 31000-2009, Risk Management -Principles and Guidelines (ISO 31000-2009, AS4360-2004 Geneva, Switzerland, 2009).
- 24. Masse et al., DHS Risk Assessment Methodology, 15.
- 25. National Research Council, Review of DHS Approach to Risk Analysis, 137, emphasis in the original.
- 26. Office of Management and Budget, Analytical Perspectives, Budget of the United States Government, Fiscal Year 2011 (Washington, DC: 2011), 381.
- 27. Department of Homeland Security, National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency (Washington, DC: Department of Homeland Security, 2009), 15n.
- 28. Ibid., 11.
- Shane Harris and Stuart Taylor Jr., "Homeland Security Chief Looks Back, and Forward," GovernmentExecutive.com, March 17, 2008.
- Glenn L. Carle, "Overstating Our Fears," Washington Post, July 13, 2008; see also Marc Sageman, Leaderless Jihad (Philadelphia: University of Pennsylvania Press, 2008) and Fawaz Gerges, "Word on the Street," Democracyjournal.org (Summer 2008): 69-76.
- 31. This discussion stems from Sageman, Leaderless Jihad, from conversations with Sageman, and from a talk on the book he gave in Washington as televised on CSPAN in early 2008 (ably summarized in David Ignatius, "The Fading Jihadists," Washington Post, February 28, 2008).
- 32. Lawrence Wright, "The Rebellion Within," New Yorker, June 2, 2008. See also Fareed Zakaria, "Post 9/11, We're Safer Than We Think," Washington Post, September 13, 2010.
- 33. Kevin Johnson, "Weakened al-Qaeda is Still a Threat," USA Today, September 8, 2009.
- 34. On this point, see also Bruce Hoffman, Inside Terrorism, rev. ed. (New York: Columbia University Press, 2006), 271-72.
- 35. 2005 report: Brian Ross, "Secret FBI Report Questions Al Qaeda Capabilities: No 'True' Al Qaeda Sleeper Agents Have Been Found in U.S.," ABC News, March 9, 2005. Press conference: Michael Isikoff and Mark Hosenball, "The Flip Side of the NIE," Newsweek.com, August 15, 2007. Officer: Bill Gertz, "Al Qaeda Seen In Search of Nukes: Defense Official Warns U.S. Still Group's Target," Washington Times, July 26, 2007.
- Testimony by Mueller can be found through www.fbi.gov/congress/congress.htm. Napolitano: Spencer S. Hsu, "Homeland Security chief warns of threat from al-Qaeda sympathizers in U.S.," Washington Post, December 3, 2009.
- 37. Brian Jenkins, Would Be Warriors: Incidents of Jihadist Terrorist Radicalization in the United States Since September 11, 2001 (Santa Monica, CA: RAND Corporation, 2010), 4 (tiny), 5 (Mao), 13 (one-off).
- David Schanzer, Charles Kurzman, and Ebrahim Mooza, Anti-Terror Lessons of Muslim-Americans (North Carolina: Triangle Center on Terrorism and Homeland Security, January 6, 2010).
- 39. Michael Kenney, "Isquo;Dumb' Yet Deadly: Local Knowledge and Poor Tradecraft Among Islamist Militants in Britain and Spain," Studies in Conflict & Terrorism 33, no. 10 (2010): 122. To demonstrate how we face "a thinking enemy that is constantly adapting to defeat our countermeasures" former deputy secretary of homeland security James Loy argues that when cockpit doors were hardened to prevent hijackings, the terrorists moved to shoe bombs to "penetrate our defenses" ("Al-Qaeda's undimmed threat," Washington Post, November 7, 2010). However, the hardened doors (which anyway were not much in place in late 2001 when the shoe bomber made his move) were in no sense a defense against bombings, only, as Loy admits, against hijacking. Similarly, Loy's contention that terrorists group was under constant police surveillance and could be closed down at any time, and it was nowhere near having sufficient materials, personnel, effective bombs, or, for many of the conspirators, passports that would have allowed them to board the planes. John Mueller, ed., Terrorism since 9/11: The American Cases (Columbus: Mershon Center, Ohio State University, 2011).
- 40. Mette Eilstrup-Sangiovanni and Calvert Jones, "Assessing the Dangers of Illicit Networks," International Security, (Fall 2009).
- 41. After 2003, the State Department changed its definitions so that much domestic terrorism including much of what is happening in the war in Iraq is now included in its terrorism count (see National Counterterrorism Center, Report on Incidents of Terrorism 2005, April 11, 2006, ii-iii). Current numbers, therefore, are not comparable to earlier ones. However, when terrorism becomes really extensive in an area we generally no longer call it terrorism, but rather war or insurgency. Thus, the Irish Republican Army was generally taken to be a terrorist enterprise, while fighters in Algeria or Sri Lanka in the 1990s were considered to be combatants who were employing guerrilla techniques in a civil war situation even though some of them came from, or were substantially aided by, people from outside the country. Insurgents and guerrilla combatants usually rely on the hit-and-run tactics employed by the terrorist, and the difference between.



terrorism and such wars is not in the method, but in the frequency with which it is employed. Without this distinction, much civil warfare (certainly including the decade-long conflict in Algeria in the 1990s in which perhaps 100,000 people perished) would have to be included in the "terrorist" category. That is, with the revised definition, a huge number of violent endeavors that have normally been called "wars" would have to be recategorized. Indeed, the concept of civil war might have to be retired almost entirely. For more on the distinction, see John Mueller, The Remnants of War (Ithaca, NY: Cornell University Press, 2004), 18-20.

- 42. Todd Sandler, Daniel G. Arce, and Walter Enders, "Transnational Terrorism," in Global Crises, Global Solutions, ed. Bjorn Lomborg (Cambridge, U.K.: Cambridge University Press, 2009), 524.
- 43. Anthony H. Cordesman, The Challenge of Biological Weapons (Washington, DC: Center for Strategic and International Studies, 2005), 29-31, tallies "major attacks by Islamists" outside of Iraq: 830 fatalities for the period April 2002 through July 2005; we have corrected the total for the 2005 London bombings, given as 100 in this source, to 52. Brian Michael Jenkins, Unconquerable Nation: Knowing Our Enemy and Strengthening Ourselves (Santa Monica, CA: RAND Corporation, 2006), 17984, tallies "major terrorist attacks worldwide" by "jihadist extremists" outside Afghanistan, Iraq, Israel, Palestine, Algeria, Russia, and Kashmir: 1129 fatalities for the period October 2001 through April 2006. "Jihadi Attack Kill Statistics," IntelCenter, August 17, 2007 (www.intelcenter.com), 11, tallies "most significant attacks executed by core al-Qaeda, regional arms and affiliate groups excluding operations in insurgency theaters": 1,632 fatalities for the period January 2002 through July 2007.
- 44. John Stossel, Give Me a Break (New York: HarperCollins, 2004), 77.
- 45. Garrick Blalock, Vrinda Kadiyali, and Daniel H. Simon, "The Impact of Post9/11 Airport Security Measures on the Demand for Air Travel," Journal of Law and Economics 50, no. 4 (November 2007): 731-55.
- 46. Webel Baird, Terrorism Risk Insurance: An Overview, CRS Report for Congress (Washington, DC: Congressional Research Service, April 11, 2005), 1.
- "MarketWatch: Terrorism Insurance" (London: Marsh Inc., 2005). Governments in the United Kingdom, continental Europe, Australia, South Africa, India, and elsewhere enacted similar terrorism reinsurance schemes. "Terrorism Insurance Update" (London: Marsh Inc., June 2004).
- 48. Based on a survey of 1,382 firms in the United States. See The Marsh Report: Terrorism Risk Insurance 2010 (London: Marsh Inc., 2010), 16.
- 49. \$9,541 divided by \$303 million, or 0.003%.
- 50. For details, see Mueller and Stewart, Terror, Security, and Money, chap. 3.
- 51. System modeling and reliability techniques exist to calculate risk reductions for any system (see Mark G. Stewart and Robert E. Melchers, Probabilistic Risk Assessment of Engineering Systems (London: Chapman & Hall, 1997) and Mark G. Stewart, "Risk-Informed Decision Support for Assessing the Costs and Benefits of Counter-Terrorism Protective Measures for Infrastructure," International Journal of Critical Infrastructure Protection 3. No. 1 (2010): 29-40.) While there are many advantages to probabilistic and reliability analyses for calculating risk reductions, they are not always appropriate, particularly for the Isquo;new hazard' of terrorism. Hence, as is the case with any risk analysis of a complex system, information about risk reductions may be inferred from expert opinions, scenario analysis, statistical analysis of prior performance data, on system modeling as well as from probabilistic and reliability analysis. The discussion to follow draws on all these aspects to arrive at quantifiable risk reductions.
- Kean, 9/11 Commission Report, 108. On this issue, see also Benjamin H. Friedman, "Perception and power in counterterrorism: Assessing the American response to Al Qaeda before September 11," in American Foreign Policy and the Politics of Fear: Threat Inflation since 9/11, Trevor Thrall and Jane K. Cramer, eds. (London and New York: Routledge, 2009), 210-229.
- 53. Michael A. Sheehan, Crush the Cell: How to Defeat Terrorism Without Terrorizing Ourselves (New York: Crown, 2008), 263.
- 54. Terry McDermott, "The Mastermind: Khalid Sheikh Mohammed and the making of 9/11," New Yorker, September 13, 2010.
- 55. Bart Hobijn and Erick Sager, "What Has Homeland Security Cost? An Assessment: 2001-2005," Current Issues in Economics and Finance 13, no. 2 (Federal Reserve Bank of New York, 2007): 17.
- 56. Office of Management and Budget, Analytical Perspectives 2010, http://www.whitehouse.gov/omb/budget/Analytical\_Perspectives, 379. FY2009 is the most recent year where actual expenditures, as opposed to budget requests, are known. The federal budget includes expenditure from aviation security fees and other fee-funded homeland security programs.
- 57. Actual expenditures for FY2010 and FY2011 not known at this time.
- 58. For a full analysis of such calculations, see Mueller and Stewart, Terror, Security, and Money, chap. 2-3.
- 59. 75 billion dollars divided by risk reduction (45 percent) divided by 5 billion dollars.
- 60. The ratio of benefit to cost is equal to (attack probability) x (losses) x (risk reduction) / (security cost)
- 61. Interesting in this respect is Vice President Dick Cheney's "one-percent doctrine." When a top CIA analyst told him in 2001 that al-Qaeda probably didn't have a nuclear weapon, but that he couldn't "assure you that."

they don't," Cheney replied, "If there's a one percent chance that they do, you have to pursue it as if it were true." (George Tenet and Bill Harlow, At the Center of the Storm: My Years at the CIA (New York: HarperCollins, 2007), 264.) Table 2 suggests in the last column, however, that there would have to be at least a 3.3 percent yearly chance that al-Qaeda not only had a nuclear weapon but that, in addition, it possessed the capacity to set one off in a key place in a crowded American city. Under that circumstance enhanced homeland security expenditures would be deemed cost-effective.

- 62. On the costs of the Iraq War, see Joseph E. Stiglitz and Linda J. Bilmes, The Three Trillion Dollar War: The True Cost of the Iraq Conflict (New York: Norton, 2008).
- 63. For efforts to do so for various protective measures, see Mueller and Stewart, Terror, Security, and Money, chap. 5-7. It appears that the protection of a standard office-type building would be cost-effective only if the likelihood of a sizable terrorist attack on the building is a thousand times greater than it is at present. Something similar holds for the protection of bridges: Stewart, "Risk-Informed Decision Support." On the other hand, hardening cockpit doors may be cost-effective, though the provision for air marshals on the planes decidedly is not: Mark G. Stewart and John Mueller, "A Risk and Cost-Benefit and Assessment of U.S. Aviation Security Measures," Journal of Transportation Security 1, no. 3 (2008): 143-159. The cost-effectiveness of full-body scanners is questionable at best: Mueller and Stewart, Terror, Security, and Money, chap. 7; Stewart and Mueller, "Risk and Cost-Benefit Analysis."
- 64. For a fuller discussion of this point, see John Mueller and Mark G. Stewart, "Hardly Existential: Thinking Rationally About Terrorism," foreignaffars.com, April 2, 2010; Mueller and Stewart, Terror, Security, and Money, chap. 2.
- 65. "Global Terrorism Database 1970-2007," Mueller and Stewart, Terror, Security and Money, chap. 2.
- Andrew Mack, "Dying to Lose: Explaining the Decline in Global Terrorism," in Human Security Brief 2007 (Vancouver, BC: Human Security Report Project, School for International Studies, Simon Fraser University, 2008), 821.
- On the unlikelihood of atomic terrorism, see John Mueller, Atomic Obsession: Nuclear Alarmism from Hiroshima to Al-Qaeda (New York: Oxford University Press, 2010), chap. 12-15. See also Brian Michael Jenkins, Will Terrorists Go Nuclear? (Amherst, NY: Prometheus, 2008).
- For rare, perhaps unique, exceptions, see John Mueller, "Harbinger or Aberration? A 9/11 Provocation," National Interest (Fall 2002): 45-50, and Russell Seitz, "Weaker Than We Think," American Conservative 6 (December 2004).
- Walter Laqueur, "Postmodern Terrorism: New Rules for an Old Game," Foreign Affairs (September/October, 1996). For a lively discussion of expert prediction, see Dan Gardner, Future Babble (New York: Dutton, 2011).
- Bjorn Lomborg, Global Crises, Global Solutions (Cambridge, U.K.: Cambridge University Press, 2009). See also Mueller and Stewart, Terror, Security and Money, chap. 9; Tammy O. Tengs and John D. Graham, "The Opportunity Costs of Haphazard Social Investments", in Life-Saving, Risks, Costs, and Lives Saved: Getting Better Results from Regulation, R. W. Hahn, ed. (Washington, DC: American Enterprise Institute, 1996), 167-182.
- 71. Jeffrey Rosen, "ManMade Disaster," New Republic, December 24, 2008.
- 72. James Fallows, "If the TSA Were Running New York," www.theatlantic.com, May 2010; Sheehan, Crush the Cell, 7.
- 73. Benjamin H. Friedman, "The Terrible Isquo; Ifs." Regulation (Winter 2008): 39.
- 74. Daniel Gardner, The Science of Fear: Why We Fear the Things We Shouldn't and Put Ourselves in Greater Danger (New York: Dutton, 2008), 262.
- 75. Benjamin Friedman, "Leap Before You Look: The Failure of Homeland Security," Breakthroughs (Spring 2004): 33.
- 76. Mueller and Stewart, Terror, Money, and Security, chap. 9.
- On the media, see John Mueller, Overblown: How Politicians and the Terrorism Industry Inflate National Security Threats, and Why We Believe Them (New York: Free Press, 2006), 39-41; Gardner, The Science of Fear, chap. 8.
- 78. Sunstein, "Terrorism and Probability Neglect," 132.
- 79. Sewell Chan, "Buzz Over Mayor's Isquo;Get a Life' Remark," nytimes.com, June 6, 2007.
- 80. We calculate that, for the world at large, one airplane flight in 20 million was hijacked or attacked by terrorists in the period from 1999 to 2008.
- 81. Tenet: 60 Minutes, CBS, April 29, 2007. Tenet's assertion is strongly contradicted by the testimony of the chief 9/11 planner: "Substitution for the Testimony of Khalid Sheikh Mohammed," www.law.umkc.edu/faculty/projects/ftrials/moussaoui/sheikhstmt.pdf. Chertoff: E. A. Torriero, "U.S. security chief warns of rising risk: Chertoff cites worry over summer attack," Chicago Tribune, July 11, 2007. Napolitano: Richard A. Serrano, "U.S. Faces 'Heightened' Threat Level," Los Angeles Times, February 10,





2011. Ian Lustick, Trapped in the War on Terror (Philadelphia, PA: University of Pennsylvania Press, 2006), 97.

- 82. Mueller and Stewart, Terror, Security, and Money, chap. 4.
- Jeffrey D. Simon, The Terrorist Trap: America's Experience with Terrorism, 2nd ed. (Bloomington, IN: Indiana University Press, 2001), 227-34.
- 84. On Canada's notably measured reaction to the 1985 bombing of the Air India airliner that flew out of Toronto, mostly killing Canadian citizens, see Gwynne Dyer, "The International Terrorist Conspiracy," www.gwynnedyer.com, June 3, 2006
- 85. James Fallows, "The Evolution of the TSA," www.theatlantic.com, December 8, 2010. Emphasis in the original.
- 86. Steve Luxenberg, "Bob Woodward book details Obama battles with advisers over exit plan for Afghan war," Washington Post, September 22, 2010.
- 87. Mueller, Overblown, chap. 2.
- 88. See note 5.
- 89. Stephen Flynn, "The Neglected Home Front," Foreign Affairs (September/October 2004): 20, 33.
- 90. Warren Rudman, Gary Hart, Leslie H. Gelb, and Stephen Flynn, "Isquo;Our Hair Is on Fire'," Wall Street Journal, December 16, 2004.
- 91. Stephen Flynn, "5 Myths About Keeping America Safe from Terrorism," Washington Post, January 3, 2010.
- 92. Richard A. Clarke, "Ten Years Later," Atlantic (January/February 2005), 61-77.
- 93. Richard A. Clarke, "The Times Square bomb failed. What will we do when the next bomb works?" Washington Post, May 9, 2010. On security theater, see especially Bruce Schneier, Beyond Fear: Thinking Sensibly About Security in an Uncertain World (New York: Copernicus, 2003).
- 94. Flynn, "The Neglected Home Front," 27.

#### FDA Describes Obstacles in Preparing Anti-WMD Medical Tech

Source: http://www.globalsecuritynewswire.org/gsn/nw\_20110818\_9196.php

The absence of critical scientific data, procedures for evaluating protections and effectiveness and other resources has hindered the preparation of new medical treatments for responding to WMD threats, the U.S. Food and Drug Administration said in a report announced on Wednesday (Aug. 24).

The new "Strategic Plan for Regulatory Science" addresses the shortfalls in four primary objectives for promoting such such advancements, the Center for Infectious Disease Research and Policy reported (Center for Infectious Disease Research and Policy release, Aug. 17).

"FDA will ... focus its scientific agenda on four overarching areas: develop, characterize and

qualify animal models for MCM [medical countermeasure] development; modernize tools to evaluate MCM product safety, efficacy and quality; develop and qualify biomarkers of diseases or conditions; and enhance emergency communication," the report states. "In addition, FDA will conduct product needs assessment in collaboration with the clinical community, academia. industry, and Biomedical Advanced Research and Development Authority (BARDA) to identify products that can be delivered efficiently and applied easily without requiring advanced skill or expertise, and furthermore have potential for broadest impact," the document adds (U.S. Food and Drug Administration report, Aug. 17).

NOTE: You can download the FDA's report from the CBRNE-CT Section of the Newsletter's website.

#### Europeans overwhelmingly against immigration: Poll

Source:http://www.euractiv.com/en/socialeurope/europeans-overwhelmingly-immigration-poll-news-507074

An international survey of 23 countries by Ipsos has found opposition to immigration in numerous countries across the world, with majorities often considering its effects to be negative and its scale excessive. European nations were typical of this trend. Majorities in countries as diverse as Germany, South Africa, Russia, Turkey and the United States were found to consider immigration to have a "very or fairly negative impact". Anti-immigration sentiment was particularly strong in Europe, with over 65% of Spaniards,



Italians and British polled strongly or partly agreeing that "there are too many immigrants in our country".

Sweden and Poland were the only European countries surveyed that did not have majorities who considered immigration to have a negative impact. In no country did a majority consider immigration to have been beneficial.

Majorities in most EU countries surveyed agreed that immigration had made it more difficult for citizens to find employment and "placed too much pressure on public services," such as health care and education.

Anti-immigrant sentiment has put significant strain on freedom of movement within the EU. On 11 August, the European Commission approved Spain's measures to exclude Romanian workers from its labour market. The Spanish unemployment rate is by far the highest in the EU at 21%. Bulgaria and Romania recently saw their accession to the Schengen border-free area postponed.

The Dutch and Danish governments, whose parliamentary majorities are dependent on the support of far-right anti-immigrant parties, have pushed particularly hard to limit immigration. In the case of Denmark, the unilateral imposition of new border controls was harshly criticised by the European Commission and Germany.

### Immigration in Europe: Declining and uneven

The number of migrants in the world has increased dramatically over the past decade, according to the International Organisation for Migration, soaring from 150 million in 2000 to 214 million today. Immigration to the European Union, however, has dropped somewhat in recent years due to the economic recession.

A major study published last month by the Organisation for Economic Cooperation and Development (OECD) found that immigration to most European nations declined in 2009, including in France (7%), Germany (13%), Spain (18%) and Italy (25%). Immigration rates to Ireland and the Czech Republic virtually halved over the course of that year.

Similarly the EU's own statistical service, Eurostat, found that immigration to EU member states dropped by 6% in 2008, while emigration increased by 13%. But Eurostat also indicates that the number of foreign residents in various EU countries has nonetheless been on the rise, increasing from approximately 28,913,000 in 2007 to 32,493,000 today (including EU citizens residing in another member state).

While anti-immigration sentiment, according to the poll, is broadly shared across Europe, there are significant national differences. The number of foreigners in some countries, particularly Belgium, France and Germany, has grown relatively slowly over the past decade or has even declined.

Other countries, often traditionally lands of emigration, have seen spectacular increases in foreign residents. According to Eurostat, between 1999 and 2010 their numbers increased from 1.2 million to 4.2 million in Italy, from less than 120,000 to 420,000 in Ireland, and from 650,000 to 5.7 million in Spain.

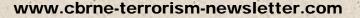
**NOTE:** Download poll's presentation from the CBRNE-CT Papers section of the Newsletter's website.

#### Answering the "What Ifs" With Real-Life Training

#### By Richard Schoeberl

Source: DomesticPreparedness.com

As emergency management professionals in London train and prepare for the upcoming 2012 Olympic Games, police are presently falling short in mitigation efforts to combat large-scale rioting throughout the United Kingdom. At the same time, Norway is dealing with mass casualties from a so-called "lone wolf" terrorist attack, spurring that nation to evaluate the reaction and be better prepared for a similar situation in the future. The quintessential message is: The world is filled with good guys and with bad guys. The time has passed for the world to understand the unpredictable state of day-to-day threats. It is now time for the world to be prepared to mitigate the crisis when and where it actually happens. The looming threat of a terrorist attack on U.S. soil (or against U.S. forces overseas) highlights the importance of effective planning efforts in responding to crisis situations. Whether the anomaly of the recent act of terrorism in Norway or staying ever vigilant against the threat posed by al Qaeda, preparation is paramount and complacency



has no place in emergency management. Emergencies and crisis situations similar to those of the past are inevitable, and for that reason public and private organizations must plan and jointly train to be successful when combating these evolving threats. Many if not all organizations are, in fact, continuing to prepare for that untimely day an attack will occur - but relatively few of them incorporate enough "real-life" exercises that integrate all responding agencies and other affected resources. Emergency exercises are designed as a practical response to the growing threat of a terrorist attack, a natural disaster, or other large-scale emergency. They are, therefore, or should be, a core component of the preparedness component of emergency management, and an effective exercise program impacts each phase of the emergency management cycle. Agencies conducting diverse emergency exercises increase their own prevention, preparedness, response, and recovery capabilities. These caveats can be fine-tuned through workshops and seminars, tabletop exercises, and functional exercises but most effectively through full-scale exercises.

#### TTEs & FSEs: The "Real-Life" Differences

In the wake of several attacks and attempted attacks, it becomes necessary at some point to test an agency's capability. The most common methods of testing are through the use of various mitigation and preparation exercise programs, including both tabletop exercises (TTEs) and full-scale exercises (FSEs). Most TTEs and FSEs are crafted to address policy as well as strategic issues. Both types of exercises test prevention and response systems and also: (a) require participants to make difficult decisions and carry out essential functions; and (b) challenge their capabilities to maintain a common operating picture during a significant incident. TTEs are usually more sanitized, typically performed in a classroomtype setting or simulated command post, and assist in facilitating a scenario. Unfortunately, they all too often lack the full integration that more accurately simulates the presence of a real-life situation. Unfortunately, because a typical TTE is a facilitated group analysis of an emergency situation, in an informal and stressfree environment, participants may feel that they are sometimes "just going through the motions." The TTE is particularly well designed

for an examination of operational plans, problem identification, and in-depth problem solving, but without the actual deployment of resources. In addition, it provides an opportunity for key agencies to become familiar one another, along with with their interconnected roles and unique duties and responsibilities. In contrast, an FSE is performed in the field, under simulated conditions but as close to "real life" as is physically possible, forcing participants to take the exercise more seriously. The FSE is designed to create a high level of stress, with the desired multi-agency approach, and involving an "actual" deployment of resources in order to fully evaluate the situation - as if it is actually happening in a real-life incident. In an FSE, incorporating both operational and tactical considerations into the exercise is imperative in order to include and evaluate tactics, technical aspects, and procedures that would be deployed to cope with a real-life threat.

### Vulnerabilities, Prevention-Mitigation and a Three-Phase Task Sequence

Having a well-balanced program, and coupling TTE with FSE, can create a valuable tool for emergency anagement executives - and should not be overly difficult. TTE and FSE go hand-in-hand by nature and the differing aspects of their training should be routinely conducted in an effort to develop a more cohesive and proactive approach to an actual crisis event. Such exercises are particularly valuable in pointing out vulnerabilities that management will have to address in the prevention-mitigation phase of response operations. In addition, such training allows participating agencies to practice a response that can help ensure a desired, measured, and efficient outcome to an actual crisis. Moreover, the FSE demonstrates exactly what resources may be required during the recovery phase of those same operations. Through the use and implementation of FSEs, agencies can also better assess, organize, and diminish lapses in emergency management plans by addressing any shortcomings detected in the exercise. Agencies that develop a highly structured FSE also will be better equipped to evaluate operational plans and response systems already in place, while examining interjurisdictional relationships in greater detail. Whether agencies follow the guidelines

established in the U.S. National Incident Management System (NIMS) or a modified version, several factors must be considered in the onset when developing and building an emergency exercise program involving both FSEs and TTEs - the cost of the program, for example, and how it fits into the annual budget. Among the other important factors to be considered are: (a) defining the capabilities of the agencies participating; and (b) the setting of realistic goals for the entire organization. Not all scenarios or "blanket scenarios" will work in every setting, of course. In the development of the program, therefore, both a short-term plan and a long-term plan should be established. After the agencies participating have crafted an acceptable plan, therefore, and that plan is approved, the process of staging the exercise for the organization should include a sequence of tasks that will transpire in three phases: (a) before the exercise; (b) during the exercise; and (c) after the exercise.

#### A Joint Approach

#### Fosters Improved Relationships

Although TTEs and FSEs are important to first responders, they can also be used as a means to prepare communities, agencies, and facilities for both natural and manmade disasters. Integrating the federal, state, and local levels of government allows all parties of interest to gain a better understanding

of overall response capabilities and the incident's possible effect on the community. A key aspect of an emergency exercise program is the fact that it fosters relationships within the critical-incident response phase that might otherwise not be present. As in a real-world response, agencies and organizations position resources into the field and face realistic incident-specific challenges, including the allocation of limited response resources and the exercise actions needed to effectively manage unforeseen conditions and circumstances as and when they develop. Planning and preparation for the exercise also help strengthen working relationships between the departments and agencies critical to successful prevention and response in real emergencies. Exercises are designed not only to create an understanding of deficiencies and response capabilities, but also - perhaps even more so - as a way to foster better working relationships between emergency management agencies' response components and governing

authorities. This in turn will create a greater opportunity for agencies to understand the risks involved in their specific facilities, to identify planning deficiencies, and to test emergency management personnel systems not only for known strengths but also for areas that need improvement.

Authorities should for that reason create a realistic scenario that challenges the partner agencies to respond to a crisis incident in order to test their objectives and to determine agency capabilities and reactions should such an incident actually occur. Crisis management exercises should also, when feasible, include both international and domestic scenarios and therefore provide for the inclusion of foreign governments. For example, an emergency exercise involving a terrorist incident should be broken down to meet several specific components. including: (a) the actual prevention and deterrence of the terrorist threat; (b) the deployment of resources that actually would respond to the terrorist incident; and (c) management of the probable and foreseeable consequences following the incident. The crisis management aspect also should include a major effort to provide: medical treatment and emergency services; decontamination services, if and when needed; the evacuation of victims and/or innocent onlookers from the scene of the incident; and the restoration of any services disrupted during the attack. Therefore, when an incident such as a terrorist attack does occur, often without warning, both crisis management and consequence management would immediately become fluid activities.

### No-Notice Exercises, Murphy's Law, and the "What If" Complications

There is considerable debate, understandably, among government agency executives regarding "no-notice exercises." Although it is important to see how quickly federal, state, and local agencies can respond, such exercises tend to be much broader in scope than preplanned exercises and can be disruptive to the normal day-to-day operations and responsibilities of the agencies directly involved. Emergency exercises should be led by a single agency - which would be responsible for planning the exercise, setting the objectives, scripting the scenario, coordinating the logistics, and evaluating the results. Logically, therefore, the lead agenci

almost always provides the bulk of the resources and personnel needed to coordinate the exercise. After-action reviews capture key lessons learned from all of the emergency responders involved. and make recommendations for improvements. The most important components of after-action reviews include the following: (a) An overview of the exercise and the emergency activities carried out; (b) An assessment of exercise goals and objectives; (c) An analysis of the outcomes and capacities needed to perform critical tasks; (d) The development of recommendations for improvement - including the specific improvements for each partner agency involved; and (e) The creation of an accountability plan for follow-up evaluations. As in other real-life events, "Murphy's Law" will likely play a role in training exercises as well. When planning exercises, each component should be spelled out in the contingency plans. It is not uncommon for communication systems to be disrupted and information technology (IT) components to fail. Building in contingency plans to engage the "what ifs" will assist with response efforts when those what ifs occur in reallife situations. There are clear benefits for conducting such exercises on a routine basis. Agencies will develop a greater consistency of response, a more proficient use of resources, and an increased confidence in staff - while building a stronger relationship with key partners in emergency management. A valuable exercise program will include both TTEs and FSEs and should be prepared to incorporate progressively multifaceted exercises, with each exercise building on the previous one, until they are as similar to reallife scenarios as is humanly possible. Furthermore, the exercise, whether FSE or TTE, should cast a wide net to encompass various organizations such as fire and police departments, emergency management, local public health, public safety, the Red Cross, and others as needed. Finally, all exercises should be both cautiously and comprehensively planned, with a clear end goal in mind.

Richard Schoeberl has over 15 years of counterintelligence, terrorism, and security management experience, most of it developed during his career with the Federal Bureau of Investigation (FBI), where his duties ranged from service as a field agent to leadership responsibilities in executive positions both at FBI Headquarters and at the National Counterterrorism Center. During most of his FBI career he served in the Bureau's Counterterrorism Division, providing oversight to the FBI's international counterterrorism effort. Schoeberl also was assigned a number of collateral duties – serving, for example, as an FBI Certified Instructor and as a member of the FBI SWAT program. He also has extensive lecture experience worldwide and is currently a terrorism and law-enforcement media contributor to Fox News, Sky News, al-Jazeera Television, and al-Arabiya.

#### **REMEMBER THIS:**

#### Mayor Bloomberg Predicts Riots in the Streets Without Job Creation

Source: http://www.klpw.com/content/mayor-bloomberg-predicts-riots-streets-without-job-creation



Mayor Bloomberg warned Friday that there would be riots in the streets if Washington doesn't find a way to start generating more jobs.

He pointed to demonstrations in both Cairo and Madrid as examples of dissatisfied citizens taking to the streets to show their unhappiness.

In Cairo, angry Egyptians demonstrated their frustrations by toppling leader Hosni Mubarak and, more recently, attacking the Israeli Embassy. In Madrid, recent protests were sparked by the

government's decision to spend millions on Pope Benedict's visit rather than dealing with their widespread unemployment problems.

Bloomberg's prediction comes as President Obama has been pressuring Republicans to pass his proposed job creation plan.



1.12

116

#### IED used in the Agra hospital blast

Source:

http://www.dnaindia.com/india/report\_breakingnews-explosion-in-agra-s-jai-hospital\_1588321

A low intensity blast in which a crude Improvised Explosive Device (IED) was used ripped through a reception area of a private hospital in the city this evening leaving six people injured.



It was not immediately clear whether the explosion at the 70-bedded Jai hospital, located three km from Taj Mahal, was a terror attack or some criminal gang was behind it.

Security around the 17th century monument of love in this tourist town in Uttar Pradesh has been beefed up as it has been on the radar of terrorists for an attack.

The explosion which occurred at 5:45pm broke the windowpanes in the reception area where 10 to 15 people were seated in steel chairs. Shards of glass lay strewn on the ground floor



of the 12-year-old hospital located on the Agra-Kanpur highway. Preliminary reports said the

crude bomb may have been kept below a chair in the reception area.

Inspector General of Police (Agra Range) PK Tiwari said six people suffered minor injuries and that it was too early to say whether the incident was a terror strike.

Tiwari ruled out the possibility of tiffin boxes



being used in the explosion which set off panic among the patients and medical personnel at the hospital.

He said the injuries sustained were not of a serious nature and all were being treated in the



#### hospital itself.

Official sources in Delhi said that according to preliminary reports the explosion was triggered by a loosely assembled IED.

A team of national Security Guards(NSG) were also rushed to the spot.

Forensic teams have been rused to the spot to collect clues from the blast site.

Patients were evacuated from the hospital and police cordoned off the entire area and conducted an intensive combing operation.



#### Technology, Revolution and the Wisdom of Crowds

Source:http://techinsider.nextgov.com/2011/09/technology\_revolution\_and\_the\_wisdom\_of\_crowds.php ?oref=latest\_posts



While the crossroads between foreign policy and information technology has been preoccupied with the still largely unresolved question of whether social media can spark revolutions, a few committed technologists are examining traditional media's ability to predict when revolutions will occur. In a Friday post on the Foreign Policy blog, Joshua Keating profiled Kalev Leetaru, a

University of Illinois professor, who argues that a sophisticated "tonal analysis" of news coverage can suggest when revolutions and other upheavals are in the works.

The tone of Egypt news coverage -- ranging from international outlets to local newspapers and blogs -- reached its most negative point in years in January, just before the nation erupted in protests that ended Hosni Mubarak's decades-long rule, Leetaru's analysis showed. Director of National Intelligence James Clapper's office gave some sanction to the idea of tonal news analyses in August when its Intelligence Advanced Research Projects Activity division launched a study to mine news outlets, blogs and social media for clues to upcoming revolutions, famines and disease outbreaks.

The Fund for Peace has, for several years, used a similar analysis to rank which nations are most likely to become failed states.

a hot topic recently. Those analyses show promise, scholars at a U.S. Institute of Peace conference on Friday said. They warned, though, that most analyses so far have tended to favor some social media outlets over others, likely skewing the results.

Social media's predictive power has also been

In a lecture at The George Washington University on Sept. 15, University of Washington **Professor Phil Howard** offered a model for predicting which regimes are most likely to face social media-fueled uprisings

using the nation's level of Internet penetration and the regime's history of fixing elections as two critical axes.

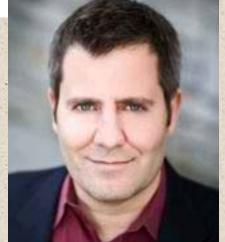
He predicted Iran's 2012 legislative elections may lead to even more turmoil than the 2009 presidential elections, which sparked the Green Revolution that nearly toppled Iranian President Mahmoud Ahmadinejad.

The model is included in Howard's new book The

Digital Origins of Dictatorship and Democracy: Information Technology and Political Islam.

Using the wisdom of crowds is nothing new to the foreign policy and intelligence world. Between 2001 and 2003, the Defense Advanced Research Project Agency invested \$500,000 in a virtual betting pool to gauge the likelihood certain cities would be attacked by terrorists or that certain people would be assassinated, including then-Palestinian Authority Leader Yassar Arafat.

The pool was shut down after Sens. Byron Dorgan, D-N.D., and Ron Wyden, D-Ore., exposed the program and called it "ill conceived," "repugnant" and "unbelievably stupid." Others have have argued the program should have been allowed to go forward.



#### **Reality Check - Iran's Missile Capability**

Source: http://www.uncommonthought.com/mtblog/archives/cat\_rowan\_wolf\_-\_utj\_editor.php





# Original Papers

#### **Swiss CBRN Protection Goes National**

By Dr. Marc Kenzelmann

**Abstract.** In 2003 the *National NBC Protection* project was launched in Switzerland, the aim of which was better coordination of all NBC partners and ultimately more effective CBRN protection in Switzerland in the long term. It led to a flurry of activity in the field of CBRN protection, which continues today. The present article outlines some of the activities that have helped to identify and define how Switzerland can sharpen its response to a CBRN incident. The years to come will show whether Swiss policy makers are really willing to implement these recommendations and accept the consequences they entail. Only then can we say that we have learnt lessons from major emergencies like Fukushima.

**Keywords.** National NBC Protection Project, NBC Protection Strategy for Switzerland, NBC reference scenarios, Federal NBCN crisis management board, subsidiary federal support, medical CBRN protection

#### Introduction

Swiss security policy in relation to potential CBRN<sup>1</sup> risks has profoundly changed since the end of the cold war. The fear of military deployment of weapons of mass destruction (WMD) has given way to new threats such as growing terrorist activity, violent extremism, WMD proliferation as well as transport and technical accidents involving hazardous materials. Safety-related CBRN events such as the sarin attack in Tokyo (1995), the US anthrax attacks (2001) and the SARS epidemic (2002/2003), led to serious debate about the risks of potential CBRN incidents in Switzerland and its response to them. This new situation called for consistent professional expertise to ensure that the Swiss population enjoyed all-inclusive civil-based and militarysupported CBRN protection. It also required a review of all the organisations and structures currently involved in CBRN defence (1). The swine flu epidemic (2009) and the nuclear disaster at Fukushima Daiichi following a major earthquake and catastrophic tsunami that struck Japan in March 2011 have brought into sharp focus efforts to devise plans that would

<sup>1</sup> Although the term *CBRN* is internationally accepted, the official term in Switzerland is still *NBC*.

ensure an optimal response to CBRN events. This is due in no small part to the media hype surrounding these incidents, which brought enormous political pressure to bear.

One of the direct results of these events is a root-and-branch reform of CBRN protection in Switzerland. A huge number of projects have already been launched, many of them running in parallel or in partial overlap, or even in direct "competition" with one another. So as not to spread our resources too thinly, we must ensure the optimal coordination and implementation of these research activities.

#### **Federal Politics in Switzerland**

To understand at least some of the issues associated with the establishment of a national CBRN protection system in Switzerland, it is worth first reflecting on the country's unique political model. Switzerland is a nation established by the will of the people and composed of several ethnic groups with a variety of languages and religions. It has been a federal state since 1848 and is one of 23 worldwide, with the United States of America being the oldest.

Switzerland has three political levels: the municipalities, the cantons and the

Confederation. It also has a somewhat unique democratic tradition and has 27 political systems, one federal and 26 at the cantonal level (2,3). It is a Confederation of 26 cantons of which 20 are considered full cantons and the remaining 6 half-cantons because they originated from internal divisions in three cantons. However, they are different in size (both area and population), and their structures vary widely. Yet, all cantonal institutions have equal competences and rights of autonomy. and their internal organisation does not depend on whether they are full or half cantons. The distinction between full and half cantons comes into play only in relation to voting arithmetic: full cantons may send two members to the lower house of Switzerland's federal parliament, half cantons only one.

Swiss political philosophy can be described as a form of federalism that grants the cantons and the municipalities a maximum of political self-determination and restricts the competences of the federation to the minimum needed to run a modern state. Governments, administrations, parliaments and courts are organized at federal, cantonal and municipal levels. The political system is a direct democracy with frequent referendums at all three political levels. Additionally, Switzerland has four official languages: German, French, Italian and Rumantsch (2,3).

#### The Swiss Joint Civil Protection System

On 1<sup>st</sup> January 2004, the Federal Council enacted the new "Federal Law on Civil Protection and Protection and Support" (BZG). It was passed by the federal parliament (only one dissenting vote) on 4<sup>th</sup> October 2002. A referendum was subsequently held on 18<sup>th</sup> May 2003 in response to a citizens' initiative; 80.6% of the Swiss population voted in favour of the new law.

The new Joint Civil Protection System is the ideal response to current security challenges. It enables the comprehensive protection of the population, its vital resources and cultural property. Bringing together the combined forces of five partner organisations, it constitutes an integrated management, protection, rescue and relief system. Each of the partner organisations - police, fire services, health services, technical services and P&S (Protection and Support, formerly Civil Defence) - has its own particular mission but provide the other partners in the system with support. Joint management ensures coordinated planning, preparation and operational command.

Given that incidents must be brought under control at the scene and take account of the affected community, operational responsibility for civil protection lies first and foremost with the cantons and municipalities. The Confederation sees to the coordination of civil protection services and defines its fundamental aspects. For events on a national scale, the Confederation coordinates the deployment of the relevant partners and assumes responsibility for the operational command.

The Federal Office for Civil Protection (FOCP) supports the cantons and municipalities as well as the partner organisations with their civil protection activities. The creation of the FOCP in 2003 grouped together all areas of the Federal Department of Defence, Civil Protection and Sports (DDPS) specialising in Civil Protection issues, a move that reflects the growing importance of civil protection (1,4).

As a direct consequence of the *Swiss Security Policy Report 2010* (5), the Federal Council requested the formulation of a *Strategy of the Joint Civil Protection System and the Protection & Support Service 2015+.* Work began at the end of 2010 and was completed in June 2011. The strategy defines future trends as well as the development of the Joint Civil Protection System in Switzerland, thereby also setting out the prospective organisational framework for natural disaster and CBRN incident intervention. The report is set to be approved by the Swiss government in autumn 2011 and will be submitted to parliament for its approval in 2012.

The fire service in Switzerland is organised on a cantonal basis, although local fire services are subject to municipal regulations. There are some 2,300 fire services in Switzerland, of which the vast majority (local, company and

operational services) are made up of volunteers (99%) and are equipped according to the size and location of the service. Regional services provide each other with back-up, where necessary. Only 15 fire services are staffed by full-time professionals (6).

In the event of a CBRN incident the fire service is the primary first responder. But since only about 1% of all fire services in Switzerland are professionalised (in major cities such as Zurich. Winterthur, Geneva, Bern and Basel) and in the absence of a common and binding mandate to deal with CBRN incidents, the level of CBRN training varies across fire services. In order to harmonise and to define competences, tasks and intervention times with greater precision, the Conference of the Cantonal Councillors ("ministers") responsible for military and civil protection affairs (RK MZF) approved in 2009 the 2015 action plan for the Swiss fire services, which for the first time officially designates CBRN as a core competence of all fire services. In reality, though, CBRN responsibilities will be assumed for the most part only by the professional and regional fire services.

In 2010 a task force of fire service specialists undertook a review of the tactical and technical documentation on the fire services' CBRN action plans. This work, which is scheduled for completion in 2012, will set down the fundamentals of CBRN intervention nationwide, thereby unifying response tactics and imposing interoperable intervention material.

#### Federal-civil CBRN support

Since the successful management of many, if not most, CBRN incidents may exceed the capacities of the cantons, the federal government must be prepared to step in. It currently provides support, among others, through its C-terror Task Force (EEVBS), which is currently being restructured to become a fully-fledged CBRN Task Force, as well as through the Emergency Organisation Radioactivity (EOR), the SPIEZ LABORATORY (the Swiss centre of expertise for protection against CBRN threats and hazards), and through arming the CBRN defence within the Swiss Armed Forces. The EOR comprises, *inter alia*, the National Emergency Operations Centre (NEOC) and its military staff; additional departments and bodies of the federal authority, state organisations (Swisscom, Swiss railway corporation SBB), as well as several sampling and monitoring organisations. The press centre of the Federal Chancellery supports the EOR with the provision of public information.

Should risks arise from accidents either in one of Switzerland's five nuclear power plants or in a foreign nuclear facility, the EOR receives additional assistance from the Swiss Federal Nuclear Safety Inspectorate ENSI (1).

### Subsidiary Support of the Swiss Armed Forces

Switzerland has long enjoyed peace, security and freedom, whether the freedom of movement for all citizens, the freedom of expression or economic freedom. The longterm preservation of this situation is the mission of Swiss security policy. Here, the Swiss Armed Forces have a part to play. The Federal Constitution and the Military Act assign the following three missions to the Armed Forces:

- 1. Defence
- 2. Support of the civilian authorities
- 3. Promotion of peace within an international context

Defence against an armed attack, whether on the ground or in the air, is the central mission of the Armed Forces. As this is extremely unlikely today, they must not be in a constant state of readiness. However, the Armed Forces must be capable of protecting key installations and transport axes in the event of a threat. Finally, they must be able to adapt in good time to emerging threats. As a neutral state Switzerland does not belong to any defensive alliance, though our Armed Forces are able to cooperate with other states for training purposes.

Supporting the civilian authorities when their resources no longer suffice involves bringing emergencies under control and safeguarding

domestic security. The Armed Forces assist the police with providing security at international conferences and major events. Should disaster strike, the Armed Forces can be deployed within hours at the scene to assist the fire services, the medical services and the Protection & Support organisation.

As regards international peace support within an international context, the Swiss Armed Forces are committed to security and peace abroad. When mandated by international organisations they help to bring stability to other countries after wars and crises. A more peaceful world is beneficial for Switzerland too (7).

To relieve any excessive demands on the resources of civilian authorities, a three-step action plan is in place to provide support in the event of natural, technological or violence related disasters:

- Preventive support: in the normal situation, civilian partners are permanently given military disaster relief equipment for use (e.g. swap body containers of the disaster relief battalions) outside the normal troop courses;
- Spontaneous assistance: all troops located within the vicinity of an event provide rapid assistance which is limited in both time (approx. 48 hours at the most) and space;
- Military disaster relief: within the context of national security cooperation primarily, this amounts to rescue operations in situations where damage is severe and extensive or during major fires. In addition, the military can provide the following services:
  - assistance to cut-off areas or otherwise vulnerable communities;
  - containment of the disaster area as well as prevention of consequential damage;
  - assistance with the provisional restoration of critical infrastructures;
  - reinforcement or relief of civilian and/or military resources that have already been deployed.

The rescue corps and its specialised units are the main pillar of military disaster relief. These units include:

- the disaster relief standby company, which can intervene within hours, and
- the disaster relief battalions which can be called up and deployed within days to ensure sustainability, concentration of forces and reinforcement.

Where required, the specialised units of the rescue corps can be augmented with elements from other services to form operational units that are set up according to the requirements of the situation at hand. Candidates are primarily the resources and services of the Swiss Air Force, the engineer, logistic and medical forces, military security as well as the NBC defence forces (8).

The NBC-EOD Competence Centre of the Armed Forces ensures the operational readiness of the NBC resources of the Swiss Armed Forces. Apart from managing the Armed Forces NBC defence, it runs NBC training courses for civilian partners in Switzerland and abroad. After the successful integration of a new CBRN decontamination system, specialist aspects of CBRN reconnaissance and mobile CBRN detection (much of the technical detection equipment has been tested by experts at the SPIEZ LABORATORY) will also be brought in. Since the beginning of 2011 its CBRN expertise has been expanded to cover CBRNe thanks to its merger with the EOD competence centre of the Swiss Armed Forces.

The NBC-EOD Competence Centre in Spiez is mobilised in the event of a major CBRN incident that exceeds the capabilities of the local civilian operational forces. Thanks to its wide range of resources and services, the NBC-EOD Competence Centre can be rapidly deployed to provide both civilian and military organisations with subsidiary back-up.

Future trends of the Swiss Armed Forces Swiss government plans to cut the material, troop numbers and budget of the Swiss Armed Forces by about 20% (Federal Council Decree of 26<sup>th</sup> November 2008) contradicts the other

objectives set out in its 2010 Security Policy Report. Although defence budgets have long seen a consistent rise across Europe and the rest of the world, Swiss military spending has continued to shrink since the end of the Cold War in 1989. Today, Switzerland spends around CHF 4.2 billion on defence (including real estate maintenance), or a mere 0.8% of its gross domestic product, leaving it trailing far behind other comparable European countries (9).

The Swiss Armed Forces Report 2010 called for a reduction of the headcount to 80,000 troops (from about 190,000 in 2010) and capped the defence budget at about CHF 4.2 billion a year. According to the report, 35,000 troops would be assigned to the mission of supporting the civilian authorities, one of the central tasks of the Swiss Armed Forces. Since these numbers would not suffice if a natural disaster with lasting consequences or a CBRN incident were to occur, the Swiss parliamentary security policy commission asked the authors to revise the report and present alternative organisational models based on troop numbers of 60,000, 80,000, 100,000 and 120,000 respectively. The new report was submitted to parliament in March 2011. Its decision is awaited with much anticipation.

Whatever parliament decides, the decision will have a considerable impact on the capabilities of the Swiss Armed Forces to provide civilian authorities with disaster relief support in the future. (As a point of comparison: some 100,000 Japanese troops have helped and continue to help the Japanese civilian authorities manage the consequences of the natural and radiological disaster of March 2011.)

#### **Modern CBRN Threats**

Disasters, emergencies, and terrorist attacks are the main risks Switzerland faces today. Due to our modern and high-tech society, they can cause even greater damage than before. Their likelihood of occurrence is high and may appear without any or only brief prior warning. All these risks may involve a CBRN element (1), a point that was made explicitly in the Report of the Federal Council to the Federal Assembly on the Security Policy of Switzerland 2010 (5).

Assignment of Basic CBRN Tasks According to the Swiss Constitution. the Confederation and the cantons see to the security of the country and to the protection of the population within the limits of their respective competences. While the responsibility for nuclear and radiological (NR) events is at the federal level, the management of chemical and biological (CB) incidents is largely a municipal and/or cantonal responsibility (Joint Civil Protection System). For CB incidents, the Federal Law on Civil Protection states that the Confederation, in agreement with the cantons, can be asked to coordinate activities and, when necessary, take over responsibility for the management of intervention resources if a disaster impacts on several cantons, on the country as a whole, or on cross-border regions. However, the fact that the 26 cantons have devised their own incident responses and assigned responsibilities differently can cause duplications, misunderstandings, and lead to inefficient crisis prevention and management (1).

The National NBC Protection Project and the NBC Protection Strategy for Switzerland In 2003, the Swiss Armed Forces and the Association of Swiss Cantonal Chemical Officers signalled the need for a national NBC protection plan which would take account of not only all possible threats in this field but also the country's existing political structures. The Federal Council agreed, and tasked the Federal Commission for NBC Protection (ComNBC) and the Director of the Federal Office for Civil Protection (FOCP) with the "National NBC Protection" project. The aim was to identify what action needed to be taken, and to propose recommendations on how processes and organisations could be optimised. The project team identified several weaknesses in current protection that could seriously hamper the effective management of major incidents. These include a lack of coordination between federal and cantonal levels, the involvement of myriad agencies and individuals, noticeable overlaps, and the lack of a uniform approach to operational planning at

the cantonal level. The project outlined 16 measures to remedy the situation, such as optimised federal command structures, national coordination of strategic and operational tasks in the prevention of CBRN incidents, optimised availability of resources, a review of federal and cantonal responsibilities, and the standardisation of operation doctrines, training courses and material components (10,11).

On 5<sup>th</sup> July 2006, the Federal Council ordered the implementation of four priority measures, based on the project findings:

- Development of a national "NBC Protection Strategy for Switzerland";
- Creation of a "National NBC Protection and Coordination Centre";

- Expansion of the Radioactivity Steering Committee (LAR) to an NBC Steering Committee;
- Greater federal support for the cantons.

The ComNBC was tasked with developing a "NBC Protection Strategy for Switzerland" (12). It devised 14 reference scenarios which it believes cover the entire hazard spectrum (Table 1). Documented according to their duration, their potential impact and incident management, they provide a valuable tool for the identification of shortcomings in relation to prevention and intervention, and for the development of appropriate solutions to these problems. Several also include variations that factor in the threatened deployment of NBC resources (13).

#### Table 1. CBRN reference scenarios

RN	1.	Accident in a nuclear facility: release of radioactivity with prior warning
12.2	2.	Dirty bomb: spontaneous release of radioactivity causing contamination
10	3.	Deployment of a nuclear weapon: ground explosion close to the Swiss border
1	4.	Attack on a transport carrying highly radioactive waste
В	5.	Deliberate contamination of food with ricin
1	6.	Terrorist attack involving the pox viruses
127	-7.	Terrorist attack involving anthrax
8	8.	Pandemic (SARS, etc.)
1 80	9.	Accident in a Biosafety Level 3 laboratory with unintentional release of contaminants
С	10.	Transport attack or accident
	11.	Accident in a chemical storage facility
8.5	12.	Chemical terrorism: hydrocyanic acid attack in a shopping centre
100	13.	Chemical terrorism: sarin attack in an airport
1	14.	Long-range missile attack on Switzerland

Starting in autumn 2011 the technical aspects of these scenarios will be revised and updated in line with new scientific findings. A scenario on epizootic disease (foot-and-mouth disease) will also be added, as will three natural disaster scenarios (earthquake, flooding, and storms) due to the creation of a federal interdepartmental command structure (Federal NBCN crisis management board) on 1<sup>st</sup> January 2011 to administer federal government responsibilities in CBRN events (NBC) and in natural disasters (N). The new scenario catalogue will be completed by the inclusion of a "combined scenario" (earthquake as a primary event followed by a CBRN secondary event, based on the Fukushima disaster in 2011).

The "NBC Protection Strategy for Switzerland" (12), which was revised in 2011 based on an actual threat and risk assessment (by the Swiss Intelligence Service (NDB) amongst others), focuses solely on measures that must be implemented if the objectives of the Swiss NBC Protection Strategy are to be met. The report also contains a series of recommendations:

Review of the legal bases of NBC security.

The ComNBC is responsible for examining whether the existing legal

The report *Review of NBC Security Legislation* has meanwhile been completed and was



## **Swiss CBRN Protection**



## 2011 Drill



bases adequately prevent the abuse of dangerous NBC substances.

approved by the ComNBC at the end of 2010. It demonstrates how effective Swiss legal provisions have been at preventing the theft

and subsequent abuse of hazardous NBC substances. The authors found no evidence to suggest that legal reforms were needed, but concluded that work was needed on certain implementing provisions. They therefore put forward nine recommendations to rectify the situation. Following the interdepartmental consultation process in autumn 2011, the report will be submitted to the Swiss government who will make the final decision on the proposals.

Consequently, the cantons began to reevaluate their intervention capabilities in 2008 and 2009. So far, 19 cantons have completed their analysis, and work is still under way in the other six. Based on the canton-specific risk portfolio and in order to optimise CBRN crisis management these analyses identified measures that should be taken either on their own, or as part of regional cooperation efforts, or at the government level. This general deficiency analysis has generated the first nationwide overview of the status and weaknesses of current capabilities organisational, resource-based, educational and interoperability - of the various levels to deal with CBRN incidents.

• Further development of the National CBRN Protection and Coordination Office and the cantonal coordination platform.

The cantonal CBRN coordination platform (the cantonal "counterpart" of the National CBRN Protection and Coordination Office) was established officially in late 2007 and was immediately operational but lacked an official political mandate at the cantonal level. This was remedied in May 2010 by the Conference of the Cantonal Councillors ("ministers") responsible for military and civil protection affairs (RK MZF).

 Promotion of regional cooperation. The cantons are called on to promote cooperation on CBRN matters by forming intercantonal regions.

The thinking behind this recommendation is that in the event of any CBRN disaster, the regional networks can help reinforce the initial  Evaluation and management of CBRN risks based on 14 CBRN reference scenarios.

The cantons are called upon to reexamine their CBRN risk portfolio based on the 14 CBRN reference scenarios, to re-evaluate their intervention resources and, where necessary, to adapt them accordingly.

intervention measures taken by the cantonal and/or municipal organisations. This makes sense, especially given that it is unreasonable to expect every canton to have the resources needed to manage a CBRN incident singlehandedly. Mutual assistance may then also be regulated and put to the test during the preparatory phase. During cantonal risk evaluations, assisted by the cantonal CBRN coordination platform and the National CBRN Protection and Coordination Office, the cantons organised themselves into four intercantonal regions, which largely correspond to the regions already established by the Joint Civil Protection System (e.g. police, fire services coordination, biological laboratory network). As such, they do not constitute a new organisational and administrative level. After approval of these regions by the cantonal CBRN coordination platform in autumn 2011, official political approval is likely to be given by 2013.

Consensus on CBRN intervention resources

Together with the Confederation and the cantons, the ComNBC is responsible for reaching a written consensus on the CBRN intervention resources which should be procured and managed by the cantons, regions and Confederation.

 Decentralisation of federal CBRN intervention resources In line with the aforementioned written consensus, the Confederation is advised to decentralise its CBRN intervention resources. These resources must be included in all cantonal plans and training exercises.



The Federal Council tasked the ComNBC with the implementation of both these recommendations and the entire project. In turn, the ComNBC commissioned the National CBRN Protection and Coordination Office to carry out the project by the end of 2011. The aim of this "consensus report" is to define the responsibilities of all partners and to establish which CBRN resources should be procured and managed at cantonal, regional and federal level. The Confederation also must strategy. As its name suggests, the report is based on broad-based nationwide consensus. It is set to be approved by the ComNBC in December 2011. Swiss government approval is expected by the end of 2012.

## **Figure 1.** National CBRN protection as a cyclical process

of

а

Organisation

decentralise its subsidiary intervention resources to ensure that they can be rapidly mobilised. The report is based on the risk and deficiency analyses of the cantons and the government. It sets out about 12 recommendations to be fulfilled in the fields of: precise definition of responsibilities, medical CBRN protection, SIBCRA, standardisation (interoperability and uniformity) of CBRN material components, standardised technical CBRN education and development of a common wide-ranging decontamination The cantons called for the introduction at federal level of a single point of contact for all CBRN incidents, which led to a review of CBRN protection responsibilities of existing staffs and bodies (Staff of the Security Committee to the Federal Council, the Special Staff Unit for Hostage-Taking and Extortion-SOGE, Special Staff Unit for Pandemics, National Emergency and Operations Centre NEOC etc.). The Confederation was subsequently

www.cbrne-terrorism-newsletter.com

federal

interdepartmental command structure. Debriefing, conclusions, long-term Threat measures analysis Engagement List of scenarios Exercises NBC Protection General and Strategy for political situation, Switzerland incidences Scenario analysis Training Standards of Concept of engagement protection

advised to set up a federal interdepartmental command structure for CBRN incidents (14 reference scenarios). This body must also ensure efficient cooperation with the chiefs of staff of the cantonal command bodies, which will be put to the test during training exercises.

On 1<sup>st</sup> January 2011 the new *ordinance on the* organisation of deployment in the case of CBRN incidents and natural disasters came into force. It details the operational organisation at federal level and provides for the creation of a Federal NBCN crisis management board, comprising the directors of the Federal Offices concerned with NBCN matters as well as the relevant cantonal representatives. This new unit integrates many existing staffs and bodies (see above), thereby eliminating an excess of back office bureaucracy should an incident occur. The Federal NBCN crisis management board is already operational but it is still adding new members.

The ordinance also includes a (radiological) dose-dependent action plan detailing measures to protect the population in an event involving the release of radiological substances. The ordinance and especially the dose-dependent action plan is now being revised and adapted in line with the *lessons learnt* from the Fukushima Daiichi incident.

Together with the cantons, the Federal NBCN crisis management board is also responsible for NBCN preparedness in Switzerland. This should ensure broadly accepted, targetoriented preparedness planning, and should, in turn, keep administrative problems to a minimum.

The aim of all the listed measures that have been taken or are still to be taken is to convert CBRN protection in Switzerland into a cyclical process, thereby ensuring its continual optimisation.

#### **Medical CBRN protection**

Based on the concepts of the Swiss Coordinated Sanitary Service (KSD) regarding the CBRN decontamination of patients in a mass-casualty incident (2007), 13 Swiss hospitals have declared themselves as "decontamination hospitals", i.e. they are able to decontaminate more than 30 contaminated patients per hour. However, given that the Swiss population (about 8 mn inhabitants) is not evenly distributed over Swiss territory (1/3 of the Swiss territory is covered by mountains), the distribution of decontamination hospitals should consider criteria such as population density, the geographical location of economic centres and transport axes. This has not been the case so far. Additionally, the current absence of a political mandate for hospitals to become decontamination centres is suboptimal. However, plans are afoot to resolve this issue through the introduction of such a mandate by 2013. Furthermore, another project is under way to re-define the set of CBRN antidotes and their distribution in Switzerland in the event of CBRN mass-casualty incidents.

## Further activities in the field of CBRN preparedness

In response to events in Fukushima, the Swiss government created an interdepartmental working group - "Management of extreme emergencies" - on 5th May 2011. Its mission is to investigate whether Switzerland needs to introduce legal and organisational measures to improve its emergency response plans. The group will closely examine the ordinance on the organisation of deployment in the case of CBRN incidents and natural disasters, the ordinance on radiation protection and the emergency response ordinance. The federal NBCN crisis management board will assist the group for the duration of its work, which is scheduled to end in late 2011 with the submission of its report to the Swiss government. The findings and measures detailed therein should inform both the major earthquake exercise SEISMO 2012 and the 2013 nuclear emergency exercise (accident in a Swiss nuclear power plant involving the release of radioactivity).

National emergency response and crisis management efforts taken at all levels should be reviewed in a national security exercise in

2014, which is being planned at the request of the Swiss government.

Another major project in this regard is the development of a national resource management plan, including international cooperation. Work is in full swing and should be completed by the end of 2012.

#### Outlook

Coordinated CBRN protection in Switzerland is still in its infancy. Nevertheless, the introduction of measures is well on track and we shall soon see whether the stated aims of this new approach have been achieved.

Nevertheless, several issues have yet to be resolved. The coordination of all ongoing projects could be better still. For example, the ordinance on the organisation of deployment in the case of CBRN incidents and natural disasters, the Strategy of the Joint Civil Protection System and the Protection & Support Service 2015+ report as well as the consensus report explicitly reckon with the earmarking of the military resources concentrated within the DDPS for the provision of subsidiary support to the civilian authorities, especially in the event of an NBC incident. Furthermore, the deployment of these military resources (or more generally, military capabilities) in such instances are subject to binding regulations (Art. 3, para. 3, the CBRN ordinance). This, coupled with the measures set out in the consensus report, implies at least the consolidation, if not an increase, of army capabilities in disaster response situations, particularly NBC incidents.

However, following the 2010 Swiss Armed Forces Report and its call for cuts, the army have adopted a scattergun approach to finding ways to reduce its capabilities by up to 20%. This also applies to the NBC Defence Troops which are still under development (14).

Another important aspect is obvious: the above basic action plans that aim to improve how Switzerland responds to CBRN incidents will soon go onstream. However, the clearly defined measures proposed therein will come at a financial cost. Despite Fukushima and the recent terror attack in Norway in July 2011, most of us still find it hard to accept that events like these could happen in a prosperous hightech country such as Switzerland. Pragmatic security-related issues are only raised, if at all, by politicians seeking to win elections.

Nevertheless, lessons from Deepwater Horizon and Fukushima (15) clearly demonstrate that:

- even if day-to-day operations seem safe and secure, disasters still happen;
- we must ready ourselves for CBRN incidents even though we do not know that such an incident will ever occur;
- it really does help to think the unthinkable.

In the years to come we shall discover whether the political class has been willing to learn these lessons and to accept the consequences they entail. In addition to the Swiss Constitution proclaiming that the protection of the population is a core duty of the Swiss Confederation, history also shows us that safety and security has never, and never will, come cheap.

#### References

- M. Kenzelmann, D. Storch: Counteraction to CBRN Terrorism in Switzerland; in: Counteraction to Chemical and Biological Terrorism in East European Countries, NATO Science for Peace and Security Series – A: Chemistry and Biology, edited by C. Dishovsky and A. Pivovarov (2009), Springer, pp 15-23
- (2) The Swiss Confederation a brief guide 2011 http://www.bk.admin.ch/dokumentation/02070/index.html?lang=en
- (3) http://demokratie.geschichte-schweiz.ch/direkte-demokratie-schweiz.html
- (4) http://www.bevoelkerungsschutz.admin.ch/internet/bs/en/home.html
- (5) Swiss Security Policy Report 2010, Report of the Federal Council to the Federal Assembly on the Security Policy of Switzerland, 23<sup>rd</sup> June 2010
- (6) http://www.ch.ch/private/00108/00113/00324/00417/index.html?lang=en
- (7) http://www.vtg.admin.ch/internet/vtg/en/home/themen/auftraege.html
- (8) http://www.vtg.admin.ch/internet/vtg/en/home/themen/katahi.html
- (9) Weiterentwicklung der Armee: Kriterien/Forderungen, Positionspapier der Schweizerischen Offiziersgesellschaft June 2011

- (10) Schlussbericht Projekt "Nationaler ABC-Schutz"; Federal Commission for NBC Protection, ComNBC 2006-01-A, 30<sup>th</sup> January, 2006
- (11) A. Bucher, S. Maillard, M. Kenzelmann: Instrumente der Schweiz bei einer ABC-Bedrohung; *Terrorismus, Informationsschrift über den Koordinierten Sanitätsdienst (KSD) in der Schweiz* **2/08** (2008), pp 48-49
- (12) NBC Protection Strategy for Switzerland, Federal Commission for NBC Protection, ComNBC 2007-06-E, 26th June 2007
- (13) CBRN Reference Scenarios, in: Technical NBC Protection Strategy, SPIEZ LABORATORY, 2009
- (14) Ecke des Präsidenten, ABC Bulletin 03/2011; Swiss Association of CBRN specialists ABC SUISSE
- (15) In place of safety nets: Lessons from Deepwater Horizon and Fukushima; The Economist, 23rd April 2011

Marc Kenzelmann, Ph.D. is currently Head of the National CBRN Protection and Coordination Office, Federal Office for Civil Protection FOCP, Spiez Laboratory, Switzerland. Marc Kenzelmann earned his Master degree in Biology from the University of Fribourg, Switzerland in 1994 and then worked as research fellow at the University of Modena, Italy, in 1995 before he did his thesis work in Molecular Virology at the University of Berne, Switzerland, that he completed in 1999. From late 1999 until early 2007 he worked at the German Cancer Research Center (DKFZ) in Heidelberg, Germany, first as postdoc and then as research group leader in Functional Genomics. Since April 2007 he leads the National CBRN Protection and Coordination Office and in 2008 directed the coordination of the National CBRN Protection during the UEFA European Football Championship. He is a member of the Swiss Federal C-Terror task Force (C-EEVBS) and is currently the President of the Swiss Association of military and civilian CBRN specialists. Marc Kenzelmann is Lieutenant Colonel of the NBC Protection Troops of the Swiss Armed Forces and chief NBC officer of the Logistics Brigade 1.



## Climate change ... You are responsible too!



#### Top Ten Reasons That Hospitals are not Prepared to Evacuate in a Large Emergency

#### By Clif Carothers (Disaster & Emergency Management [DEM] Group at LinkedIn)

When natural emergencies disable a hospital, inhibiting its ability to provide care to its patients such as recently occurred when a

tornado devastated the St. Johns Regional Medical Center in Joplin, Missouri, the emergency

community rushes to its aid. Acting on years of training and planning, they quickly evacuate its patients and victims to safety. However, in large scale disasters affecting multiple hospitals within a region, the overwhelming emergency resources required to evacuate a single facility may not be available for days. During regional emergencies, hospitals are much more dependent on their own emergency and evacuation plans and resources to save lives. Having reviewed several hundred hospital evacuation plans, I can attest that while the hospital industry has made major strides in emergency preparation during the past decade, a majority of hospitals in America are unprepared to evacuate in a large scale emergency. As a brief summary, I have listed ten reasons:



**1. Insufficient transportation resources** – During a large emergency, local, state and federal resources place hospitals at a lower priority of evacuation. Most hospitals do not have alternate sources of transportation nor have they considered the number and type of resources that would be required to adequately respond to their emergency.

2. Undeveloped receiving facility resources – While most hospitals have mutual aid agreements and MOUs with other hospitals in their region, many have not developed detailed procedures for emergence.

acceptance and admittance. Most do not have agreements that go beyond their region in the event that their MOU receiving facilities are affected by the emergency.

**3. Limited tracking** – A large scale evacuation of several hundred patients in the span of 24 hours entails the potential use of dozens of ambulances, helicopters, and aircraft as well as the coordination of hundreds of personnel. In addition, internal and external tracking of patients, medicines, charts and personal belongings must be managed and tracked to mitigate the effect on patients and their families. Most hospitals do not have systems to accomplish this feat.

**4. Lack of Coordination with Emergency Community** – A majority of hospitals have reviewed their emergency and evacuation plans with their emergency management, EMS, police and fire departments. However, many have not relayed the weaknesses of their facility, nor have they clearly delineated the expectations they have of their local emergency providers. In the event that local providers are unable to assist, most hospitals have not detailed what is required to bring in outside providers. In addition, most have not detailed the communication plans that must be in place between the facility, their providers, and the emergency community.

**5. Unclear triggering strategy and methodology** – JCAHO standards outline minimum rationale for evacuating a hospital, yet realistic criteria are more complicated. Because of conflicting management issues, most decision criteria are not well delineated, creating confusion amongst the implementers of evacuation policies.

6. Undefined communication system – While most hospitals have acquired adequate communication hardware, including multiple backup methods, most have not defined the detailed communication processes that must be in place to implement a realistic evacuation. Rapid mass coordination of admission to receiving hospitals is one example.

**7. Limited triage plan** – Most hospitals have basic triage methodology to fit specific vulnerability analyses. However, many hospitals' triage procedures have not considered realistic timing limitations of known transport resources and receiving facilities as well as a realistic rate of patient and personnel evacuation.

8. Undeveloped patient preparation plan - While much work has been done by most hospitals to develop detailed vertical and horizontal evacuation plans that correspond to required fire safety protocols, many hospitals inadequately rely on this planning to fulfill emergency internal evacuation processes. As an example, in most cases, vertical evacuation should be coordinated with the arrival patterns of transportation vehicles.

**9.** Lack of cost tracking – To be reimbursed by the Federal Government after incurring emergency expenses during a federal emergency, the hospital must provide detailed time and cost records for all personnel, materials, and vehicles used in the emergency. Most hospitals do not have adequate procedures or capacity to account real time for costs, potentially forfeiting millions of recovery dollars as a result.

**10. Inadequate funding** – The United States has access to 70,000 ambulances, enough to overwhelm even most large disasters. However, many hospitals rely on the Stafford Act to fund their rescue, limiting access to available resources. Most have not planned for alternate funding mechanisms to draw upon during an ongoing emergency.

**Clif Carothers** is President at **EPI-Center, Inc.** and at **U.S. Air Ambulance.** EPI-Center, Inc. is uniquely positioned to prepare for and conduct rapid response, targeted, complete evacuations of health-care facilities involving thousands of patients for the benefit of private customers, local, state and federal governments during large-scale disasters. U.S. Air Ambulance provides **provides** 

transportation by air ambulance, airline critical care medical stretcher, airline escort, Amtrak train escort, and long distance ground ambulance. We also provide entire hospital evacuation services during a regional or national emergency. In addition, we provide large scale repatriation services to the federal government. **Disaster & Emergency Management [DEM] Group** at LinkedIn is a member only group of people specialized in DEM.



Climate change ... You are responsible too!

#### Lessons from High Reliability Organizations (HRO's) By Julian Talbot

Some of the best research in the area of risk management comes from studies into an area known as high reliability organizations (HRO's). HRO's include organizations such as nuclear power plants, aircraft carriers and air traffic control. This type of organization is notable, according to Rochlin [1] because "*these organizations have not just failed to fail; they have actively managed to avoid failures in an environment rich with the potential for error.*" That ability to actively and reliably manage to reduce the chances of mistakes occurring, rather than to avoid the hazards, has been the distinguishing hallmark of most HRO's and their experience offers many lessons for the application of risk management at the enterprise level.



Work by Karl Weick and Kathleen Sutcliffe [2] into this area suggests that five key elements contribute to what he describes as a state of 'mindfulness':

- 1. Preoccupation with failure
- 2. Reluctance to simplify interpretations
- 3. Sensitivity to operations
- 4. Commitment to resilience
- 5. Deference to expertise

At first many of these processes appear to be self-defeating on multiple levels. But, as Weick further explains why these processes are necessary if a high reliability organization is to be successful their validity becomes increasingly more apparent.



137

#### **Preoccupation with failure**

HRO's like most organizations celebrate their successes but Weick [3] also notes "*a chronic worry in HROs is that analytic error is embedded in ongoing activities and that unexpected failure modes and limitations of foresight may amplify those analytic errors.*"

#### **Reluctance to simplify interpretations**

Most organizations are happy to handle complex issues by simplifying them and categorizing them, thus ignoring certain aspects. HROs, however take nothing for granted and support cultures which attempt to suppress simplification because it limits their ability to envision all possible undesirable effects as well as the precautions necessary to avoid these effects. HROs pay attention to detail and actively seek to know what they don't know. They endeavor to uncover those things that might disconfirm their intuitions despite being unpleasant, uncertain or disputed. Skepticism is also deemed necessary to counteract the complacency that many typical organizational management systems foster.

#### Sensitivity to operations

Weick describes sensitivity to operations as pointing to "an ongoing concern with the unexpected. Unexpected events usually originate in 'latent failures' which are loopholes in the system's defenses, barriers and safeguards who's potential existed for some time prior to the onset of the accident sequence, though usually without any obvious bad effect." [4]

Management focus at all levels to managing normal operations offers opportunities to learn about deficiencies that which could signal the development of undesirable or unexpected events before they become an incident. HRO's recognize each potential near-miss or 'out of course' event as offering a 'window on the health of the system' – if the organization is sensitive to its own operations.

#### **Commitment to resilience**

HRO's develop capabilities to detect, contain, and bounce back from those inevitable errors that are a part of an indeterminate world. The hallmark of an HRO is not that it does not experience incidents but that those incidents don't disable it. Resilience involves a process of improvising workarounds that keep the system functioning and of keeping errors small in the first place.

#### **Deference to expertise**

HRO's put a premium on experts; personnel with deep experience, skills of recombination, and training. They cultivate diversity, not just because it helps them notice more in complex environments, but also because rigid hierarchies have their own special vulnerability to error. As highlighted by the work of James Reason and HFACs, errors at higher levels tend to pick up and combine with errors at lower levels, exposing an organization to further escalation.

HRO's consciously evoke the fundamental principle of risk management – that 'risk should be managed at the point at which it occurs'. This is where you will find the expertise and experience to make the required decisions quickly and correctly, regardless of rank or title.

Unfortunately most organizations do not work at this level, preferring to manage risk through the introduction of standard operating procedures, policy and work instructions. While these undoubtedly have their place, and can help people to make quick and consistent decisions, a significant body of research also indicates that the blanket application of these controls can reduce individuals 'mindfulness' and personal responsibility, thereby contribute indirectly to increasing operating risk.

#### Other lessons from HRO's

Other lessons from HROs include the strong support and reward for reporting of errors based on recognition that the value of remaining fully informed and aware far outweighs whatever satisfaction that might be gained from identifying and punishing an individual.

#### The Icarus Paradox



Many experiments have shown that people who succeed on tasks are less able to change their approaches even after circumstances change. (The hammer and the nail syndrome). Starbuck and Milliken in their analysis of the Challenger disaster said: "Success breeds confidence and fantasy. When an organization succeeds, its managers usually attribute success to themselves or at least to their organization, rather than to luck. The organization's members grow more confident of their own abilities, of their manager's skills, and of their organization's existing programs and procedures. They trust the procedures to keep them appraised of developing problems, in the belief that these procedures focus on the most important events and ignore the least significant ones." [5]

This level of complacency is a breeding ground for inadequate or ineffective organizational risk management and needs to be fully considered when reviewing the internal context and the risk management context.

#### Sources:

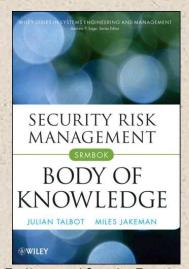
[1] Rochlin, Gene (1996) "Defining 'High Reliability' Organizations in Practice: A Taxonomic Prologue," p. 15 in Roberts, Karlene, 'New Challenges to Understanding Organizations', Macmillan Publishing Company, New York, USA

[2] [3] [4] Weick, Karl & Sutcliffe, Kathleen (2001), Managing the Unexpected: Assuring High Performance in an Age of Complexity, Jossey-Bass, New York, USA

[5] Starbuck, W. H. and Milliken, F. J. (1988) "Challenger: Fine-tuning the odds until something breaks", Journal of Management Studies, Vol. 25, 319-340, New York, USA

#### Security Risk Management Body of Knowledge

Wiley Series in Systems Engineering and Management Julian Talbot (Author), Miles Jakeman (Author)



A framework for formalizing risk management thinking in today's complex business environment. Security Risk Management Body of Knowledge details the security risk management process in a format that can easily be applied by executive managers and security risk management practitioners. Integrating knowledge, competencies, methodologies, and applications, it demonstrates how to document and incorporate best-practice concepts from a range of complementary disciplines. Developed to align with International Standards for Risk Management such as ISO 31000 it enables professionals to apply security risk management (SRM) principles to specific areas of practice. Guidelines are provided for: Access Management; Business Continuity and Resilience; Command, Control, and Communications; Consequence Management and Business Continuity Management; Counter-Terrorism; Crime Prevention through Environmental Design; Crisis Management;

Environmental Security; Events and Mass Gatherings; Executive Protection; Explosives and Bomb Threats; Home-Based Work; Human Rights and Security; Implementing Security Risk Management; Intellectual Property Protection; Intelligence Approach to SRM; Investigations and Root Cause Analysis; Maritime Security and Piracy; Mass Transport Security; Organizational Structure; Pandemics; Personal Protective Practices; Psych-ology of Security; Red Teaming and Scenario Modeling; Resilience and Critical Infrastructure Protection; Asset-, Function-, Project-, and Enterprise-Based Security Risk Assessment; Security Specifications and Postures; Security Training; Supply Chain Security; Transnational Security; and Travel Security. Security Risk Management Body of Knowledge is supported by a series of training courses, DVD seminars, tools, and templates. This is an indispensable resource for risk and security professional, students, executive management, and line managers with security responsibilities.

Julian Talbot has 25 years in risk management experience across government, corporate, resources and not-for-profit sectors in Australia, the US, Africa, Central America and South East Asia. During this time he conducted enterprise risk assessments for \$30 billion organizations, managed \$60 million risk plans, undertaken risk assessments for \$300 million IT projects, developed risk profiles for the legal profession, prepared health risk assessments and co-authored the <u>Security Risk Management</u> <u>Body of Knowledge</u> (SRMBOK). His background includes roles as Head of Security for the Australian government's most extensive international network (the Australian Trade Commission operating in over 60 countries); Security and Emergency Manager for Australia's largest natural resources project (Woodside's \$22 billion North West Shelf Venture); Senior Risk Advisor for the Australian Department of Health & Ageing and Directorships with Citadel Group (a \$60 million organization selected by BRW as Australia's 3rd fastest growing business), the Washington DC based Security Analysis and RIsk Managment Association (SARMA), the Risk Management Institution of Australasia (RMIA) and the Australian Institute of Professional Intelligence Officers (AIPIO).



## Climate change ... You are responsible too!



# Chem News

#### **Two Hood Type NBC Respirators**

Source: http://www.asanltr.com/ASANews-97/Respirator\_hood.html

individual NBC respiratory In todav's technology, there are two design approaches. The most common is the "face-fit" mask, e.g., the conventional military style respirator; the second is the hood style respirator that covers the wearer's entire head. Face-fit respirators are necessarily expensive due to the extensive ergonometrics required for their successful design and effective development. Face-fit respirators must consider facial physiognomy and variations peculiar to applicable populations. Face-seal problems include challenges posed by facial hair growth, variations in oronasal shape, conformation and dimension considerations (seal contact area), and vision requirements.

Interestingly, the "whole-head hood" style respirator is one of the oldest concepts employed in the "modern" era of CB warfare; an early example was the British PH Helmet WWI. Until relatively recently, most respirator R&D has been dedicated to the face-fit style mask. Only after the 1991 Southwest Asian"Gulf War" renewed awareness of the importance of providing adequate, quick donning and easy to use civilian protection equipment was more thoughtful reflection given to the need for development of well-designed, durable and cost-effective individual respiratory protection that could fit a wide range of head sizes. While a small number of the fully headenveloping NBC respirators have been available over the past several decades, the advantages offered by the whole-head respirator today assume increased importance as the world faces an energing NBC threat posed by extremists and terrorists. This threat assumes even greater importance because biological agents are perceived as today's preferred terrorist weapon, fostering concerns of potentially providing effective civilian respiratory protection for large numbers of individuals.

Two hood type protective designs, eminently suited for use by a diverse range of civilians

and age groups, exemplify current design concepts, the American ILC Dover, Inc. D.E.R.P (Disposable Eye Respiratory Protection) and the Finnish KEMIRA SAFETY Civic Chemi-Hood. Although both share marked similarities in providing civilians with easy to use protection against CB attack, the ILC Dover product was developed as a disposable, single use item that meets all of the immediate requirements for protecting the wearer against all concventional CBW agents. The Kemira Chemi-Hood, which may also be considered "theoretically disposable", was designed to give somewhat more prolonged protection capability--an observation underscored by its acceptance of a standard screw-thread type NBC filter. The disposable ILC DERP, by contrast, has twin, fixed bilateral filters, making it a bit less capable of providing potential multiple exposure usage. Despite



these differences, both designs provide excellent emergency protection, based upon an examination of their performance specifications, and both offer considerable versatility across a broad demographic spectrum. Further, both the DERP and the

Chemi-Hood respirators are extremely well conceived, researched, engineered, and economically produced solutions to providing mass individual protection of the highest level at a relatively low cost outlay.

Originally designed in cooperation with the US Army, as emergency supplemental NBC protection for civilian workers, the ILC Dover DERP shares many similarities with other pioneering ILC hood style designs. It provides up to two hours of protection against nerve and blister agents, may be used effectively by individuals with long hair and beards, and is capable of being donned in less than 15 seconds. The DERP comes in a sealed impermeable plastic bag and may be used up to 30 days after the bag is opened. Shelf life of the sealed DERP is given at 10 years. The mask and its construction materials were specifically designed to provide complete protection while resisting high temperatures; the DERP may be stored at temperatures exceeding 165°F, without impairing functional service capability, and is capable of providing full protection in temperatures as low as -20°F. The field of vision is excellent due to the transparent broad face section and the oronasal nosecup portion of the mask provides very low internal deadspace with consequent low CO2 accumulation. Additionally, the total weight of the DERP respirator is only 1.4 pounds, which makes it extremely lightweight and easy to carry.

The **Chemi-Hood** by Kemira Safety Oy of Finland is visually very similar to the DERP, although the Kemira respirator uses a conventional screw-thread NBC filter (Kemira Combined NBC Filter ABEK P 15, but the unit accepts any NATO spec filter). Both whole head hoods use a neck-sealing dam and are "un blown". Like the DERP, the Chemi-Hood provides excellent, unimpaired vision, and accommodates a wide range of potential users-from 12 year old adolescents through adults. The Kemira Chemi-hood has a specified shelfstorage life of 10 years and the material used for the hood has high temperature resisting characteristics. The plastic hood material also resists mustard agent for more than 24 h. The Chemi-Hood comes packed in a plastic hardshell container fitted with a carrying strap, which provides storage protection, as well as ease of portability. As with the DERP, the Chemi-Hood is quick and easy to don. Both the DERP and the Chemi-Hood feature secondary protection to the shoulders through draping of the hood skirt material.

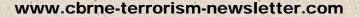


These two excellent examples of the "notactively blown" hood type NBC respirator are noteworthy in that they provide the highest protection possible at an extremely low cost per unit for the broadest range of individuals. Furthermore, they can be considered expendable emergency protection in either normal, unusually warm, or severely cold climates.

#### Nanowire-based sensors detect volatile organic compounds

Source: http://www.homelandsecuritynewswire.com/nanowire-based-sensors-detect-volatile-organic-compounds

A team of researchers from the National Institute of Standards and Technology (NIST), George Mason University, and the University of Maryland has made nano-sized sensors that detect volatile organic compounds — harmful pollutants released from paints, cleaners, pesticides, and other products — which offer several advantages over today's commercial gas sensors, including low-power roomtemperature operation and the ability to detect one or several compounds over a wide range of concentrations.





# THE ULTIMATE PROTECTION

# THE BOSS Model 4098

AirBoss-Defense CBRN Fire Boot









→ Steel toe.
Steel plate.

→ Partial tibia protector. → Pull on opening.

0



# smiths detection

Fire Rescuences and Sandros Sandros 100 - 12-10 Sandros Manual Sandros 100 - 12-10 - 12-10 Sandros 100 - 12-10

RadSeeker CS

bringing technology to life

# find the source identify the threat

#### NEW RadSeeker"

handheld radioisotope identifier

RadSeeker quickly and accurately detects, identifies and locates radioactive material including radioisotopes associated with a dirty bomb. RadSeeker gives responders the highest level of confidence by providing best-in-class results when assessing vehicles, people, or unidentified packages for gamma and neutron radioactivity.

RadSeeker features:

- Advanced algorithms for superior identification performance
- Automatic stabilization, no field calibration required
- Ruggedized ability to survive 3ft drop to concrete
- Provides a threat assessment for each isotope identified
- Detect mode assists with locating radioisotope placement

For more information: call +1 888 473 6747 [USA toll-free] or +1 203 207 2700 +44 1923 658000 (EMEA) +65 6 466 1700 (Asia Pac) email globalsales@smithsdetection.com

# www.smithsdetection.com

The recently published work is proof of concept for a gas sensor made of a single nanowire and metal oxide nanoclusters chosen to react to a specific organic compound. This work is the most recent of several efforts at NIST that take advantage of the unique properties of nanowires and metal oxide elements for sensing dangerous substances.

A NIST release reports that modern commercial gas sensors are made of thin, conductive films of metal oxides. When a volatile organic compound like benzene interacts with titanium dioxide, for example, a reaction alters the current running through the film, triggering an alarm. While thin-film sensors are effective, many must operate at temperatures of 200° C (392° F) or higher. Frequent heating can degrade the materials that make up the films and contacts, causing reliability problems. In addition, most thin-film sensors work within a narrow range: one might catch a small amount of toluene in the air, but fail to sniff out a massive release of the gas. The range of the new nanowire sensors runs from just 50 parts per billion up to 1 part per 100, or 1 percent of the air in a room.

These new sensors, built using the same fabrication processes that are commonly used for silicon computer chips, operate using the same basic principle, but on a much smaller scale: the gallium nitride wires are less than 500 nanometers across and less than 10 micrometers in length. Despite their microscopic size, the nanowires and titanium dioxide nanoclusters they're coated with have a high surface-to-volume ratio that makes them exquisitely sensitive.

"The electrical current flowing through our nanosensors is in the microamps range, while traditional sensors require milliamps," explains NIST's Abhishek Motayed. "So we're sensing with a lot less power and energy. The nanosensors also offer greater reliability and smaller size. They're so small that you can put them anywhere." Ultraviolet light, rather than heat, promotes the titanium dioxide to react in the presence of a volatile organic compound.

Further, each nanowire is a defect-free single crystal, rather than the conglomeration of crystal grains in thin-film sensors, so they're less prone to degradation. In reliability tests over the last year, the nano-sized sensors have not experienced failures. While the team's current experimental sensors are tuned to detect benzene as well as the similar volatile organic compounds toluene, ethylbenzene and xylene, their goal is to build a device that includes an array of nanowires and various metal oxide nanoclusters for analyzing mixtures of compounds. They plan to collaborate with other NIST teams to combine their ultraviolet light approach with heatinduced nanowire sensing technologies. The portion of this work conducted at George

Mason University was funded by the National Science Foundation.

Read more in G. S. Aluri et al., "Highly selective GaN-nanowire/TiO2-nanocluster hybrid sensors for detection of benzene and related environment pollutants," Nanotechnology 22 (22 July 2011)

### Enzyme Might Hold Key to Countering Nerve Agents

Source: http://gsn.nti.org/gsn/nw\_20110706\_4245.php

Drugs produced from a natural enzyme could one day be used to protect people exposed to lethal nerve agents, the U.S. National Institutes of Health said.

The health agency is providing funding for work by Israel's Weizmann Institute of Science to develop medications that could disassemble organophosphate chemicals used in "G-type" nerve agents such as sarin and soman. "Drugs based on [this] approach would be a valuable addition to our nation's ability to mount an effective medical response in the event of a chemical emergency," David Jett, head contact for the NIH Countermeasures Against Chemical Threats program, said in a press release.

Sarin was notably used by the Japanese Aum Shinrikyo cult in two attacks that killed 20 people in 1994 and 1995.

The U.S. chemical arsenal, which is due to be fully eliminated in about 10 years, also includes sarin.

In addition, organophosphate-based insecticides could prove dangerous if released in large amounts through an act of terrorism or industrial accident, according to an NIH press release.

The chemicals impair the human nervous system through deactivation of the

enzyme. Significant exposure can lead to seizures, paralysis, a shutdown of the respiratory system and death. Today, the countermeasures to nerve agents are diazepam for treating seizures and the antidotes atropine and oxime compounds.

"Atropine aims at the symptoms of nerve agent exposure, and oximes minimize the damage after it has already begun," Weizmann Institute biochemist Dan Tawfik said in the release. "Our goal is to develop a drug that can intercept organophosphates before they cause damage."

Close to 10 years of research has produced a recombinant enzyme, dubbed, rePON1, that is "highly reactive" against cyclosarin, "a more toxic cousin of sarin," according to the release. RePON1 has been shown in experiments to be 100,000 times more efficient than the umodified enzyme PON1 in dismantling cyclosarin. Three-fourths of mice treated with the altered enzyme 60 minutes before being exposed to a "cyclosarin analogue" remained living 24 hours later. Sixty percent of the treated mice survived after two weeks. Meanwhile, only 22 percent of mice who received atropine and oxime five minutes prior to introduction of the agent survived after one day, and all were dead two weeks later.

One issue with the recombinant enzyme is its limited period of effectiveness. No mice survived if they were exposed to cyclosarin 24 hours after being treated with rePON1. A longer-lasting enzyme is being sought.

"We would like to see the enzyme sustained in the blood for several days and ideally two weeks," Tawfik said.

The researchers are also pursuing a countermeasure for "V-type" agents such as VX.

# Directed evolution of hydrolases for prevention of G-type nerve agent intoxication

Gupta RD, Goldsmith M, Ashani Y, Simo Y, Mullokandov G, Bar H, Ben-David M, Leader H, Margalit R, Silman I, Sussman JL, Tawfik DS.

Department of Biological Chemistry, Weizmann Institute of Science, Rehovot, Israel. Nat Chem Biol. 2011 Feb;7(2):120-5. Epub 2011 Jan 9. Source: http://www.ncbi.nlm.nih.gov/pubmed/21217689

#### Abstract

Organophosphate nerve agents are extremely lethal compounds. Rapid in vivo organophosphate clearance requires bioscavenging enzymes with catalytic efficiencies of >10(7) (M(-1) min(-1)). Although serum paraoxonase (PON1) is a leading candidate for such a treatment, it hydrolyzes the toxic S(p) isomers of G-agents with very slow rates. We improved PON1's catalytic efficiency by combining random and targeted mutagenesis with high-throughput screening using fluorogenic analogs in emulsion compartments. We thereby enhanced PON1's activity toward the coumarin analog of S(p)-cyclosarin by 10(5)-fold. We also developed a direct screen for protection of acetylcholinesterase from inactivation by nerve agents and used it to isolate variants that degrade the toxic isomer of the coumarin analog and cyclosarin itself with k(cat)/K(M) 10(7) M(-1) min(-1). We then demonstrated the in vivo prophylactic activity of an evolved variant. These evolved variants and the newly developed screens provide the basis for engineering PON1 for prophylaxis against other G-type agents.

# WMD Central - Five Years and Building

Source: http://www.fbi.gov/news/stories/2011/july/wmd\_072611/wmd\_072611

Five years ago this week, the FBI established its first Weapons of Mass Destruction (WMD) Directorate to centralize and coordinate all WMD-related investigative activities, intelligence analysis capabilities, and technical expertise from across the Bureau. Recently, FBI.gov spoke with Dr. Vahid Majidi—the head of the WMD Directorate since its launch—on his office's work over the past five years. Today, he talks about the current threat and specific focus of the directorate. Later this week, he'll discuss case examples, lessons learned, and the future of the directorate.

Q. Why was the directorate created?

**Dr. Majidi:** The FBI has been in the WMD business for quite some time, more formally since 1995 when we created a program in our Counterterrorism Division to address the WMD threat. But obviously, a lot has happened in recent years. And it became clear that our WMD response crossed operational lines and also involved our counterintelligence, criminal, and cyber programs—not to mention the response and forensics expertise in the FBI Laboratory and the render-safe capabilities of our Critical Incident Response Group. We needed a single force to coordinate all of our WMD activities. The directorate gives us that.

# Q. What does the WMD threat look like today?

**Dr. Majidi:** The nature of the threat hasn't changed all that much over the past decade. International terrorist groups are still determined to get their hands on various forms of weapons of mass destruction—chemical, biological, radiological, and nuclear. Organizations and nation states still want material and expertise for their own programs. And certain domestic groups are still trying to

# Q. What about all those white powder letters?

**Dr. Majidi:** Most turn out to be hoaxes, and they require a lot of investigative resources, but we have to investigate each and every incident. You never know when one of them will be real.

# Q. Can you briefly explain how the WMD Directorate works?

Dr. Majidi: Absolutely. The main focus of our



Dr. Vahid Majidi WMD Directorate—and the primary focus of our overall efforts—is prevention, to keep a



acquire materials needed for basic WMD applications—predominately chemical or biological in nature.

WMD attack from ever taking place. To make that happen, we have several closely integrated activities that pull together resources

from various parts of the FBI. Our countermeasures and preventions group includes a full spectrum of activities, from WMD training for domestic and international law enforcement partners...to outreach efforts to academia, industry, government, and retailers to help them spot indicators of potential WMD activity....to working with our government partners to formulate sound policies. The investigations and operations group addresses threatened or actual use of weapons of mass destruction, or the transfer of materials,



knowledge, and technology needed to create a WMD. We also can and do collect evidence in contaminated areas, disarm hazardous devices, and provide command and control support in on-scene activities. Finally, our intelligence and analysis group serves as the foundation of our proactive approach to threats. Our analysts sort through data to identify relevant WMD information, and our agents work to identify sources of valuable intelligence. And because we are part of the intelligence community, we share information routinely with our partners. Through it all, we have a lot of activities and capabilities in play, and I think we're making a real difference.

# Q. Can you provide a few examples of successful WMD investigations over the past five years?

**Dr. Majidi:** We've managed quite a few cases actually, including our first major counterproliferation investigation that involved two Iranian men and one Iranian-American who

were charged in California with conspiring to export certain technologies from the U.S. to Iran. Other examples include a Texas man charged with possessing 62 pounds of sodium cyanide; a government contractor in Tennessee charged with trying to sell restricted U.S. Department of Energy materials; and a Nevada man charged with possessing deadly ricin. (Note: see the sidebar for more examples.)

# Q. What has the FBI learned over the past five years?

**Dr. Majidi:** Quite a bit. For some time, we've had WMD coordinators in every one of our field offices. But we realize that for WMD prevention to be truly comprehensive, we need to think and act globally. So that's why—in addition to our network of legal attaché offices and agents around the world—we've recently put our first WMD coordinators overseas, in our offices in Tbilsi and Singapore. We also have personnel assigned to Interpol to help it develop an international WMD training program like ours.

# Q. What kind of work is done overseas?

**Dr. Majidi:** It runs the gamut. For instance, several years ago, after an interdiction of highly enriched uranium in Georgia in the former Soviet Union, our WMD experts performed a forensic analysis of the material and then testified in Georgian courts. And when the Russian defector in London was poisoned with a radioactive isotope in 2006, our WMD personnel shadowed London Metropolitan Police during the ensuing investigation to develop lessons learned to help us prepare for such a scenario here. Through it all, we've built some strong relationships with our global partners.

# Q. What are the WMD Directorate's plans for the next five years?

**Dr. Majidi:** The basic knowledge and material that go into making weapons of mass destruction is becoming more readily available to anyone, anywhere in the world as the Information Age matures. That's why we'll continue to be all about partnerships—locally, nationally, and internationally. We'll also to the second second

even more on threats on the horizon. For example, we'll look at emerging developments like synthetic biology from a preventative point of view. By collaborating with the synthetic biology community, we can articulate our safety and security concerns as they relate to weapons of mass destruction. We'll also be improving our threat analysis capabilities to better spot potential WMD opportunities, potential WMD vulnerabilities, and gaps in our intelligence collection.

# Q. What can the average citizen do to assist law enforcement with the WMD threat?

**Dr. Majidi:** Keep in mind that to develop weapons of mass destruction, you only need two things: the material and the know-how. So please, if you see anything suspicious or in a place where it doesn't belong, report it to local law enforcement or your closest FBI Joint Terrorism Task Force. It could be just the tip we need to stop something serious

#### Sensors printed on wetsuits detect explosives, other hazards

Source: http://www.homelandsecuritynewswire.com/sensors-printed-wetsuits-detect-explosives-other-hazards

UC Sand Diego researcher has successfully printed thick-film electrochemical sensors directly on flexible wetsuit material, paving the way for nano devices to detect underwater explosives or ocean contamination; UCSD has a full U.S. patent pending on the technology, and has begun talks on licensing the system to a Fortune 500 company. under water — and still keep functioning properly.

Joseph Wang has successfully printed thickfilm electrochemical sensors directly on flexible wetsuit material, paving the way for nano devices to detect underwater explosives or ocean contamination.

"We have a long-term interest in on-body electrochemical monitoring for medical and security applications," said Wang, a professor in the Department of NanoEngineering in UC San Diego's Jacobs School of Engineering. "In the past three years we've been working on flexible, printable sensors, and the capabilities of our group made it possible to extend these systems for use underwater."

Wang notes that some members of his team — including electricalengineering graduate student Joshua Windmiller — are surfers. Given the group's continued funding from the U.S. Navy, and its location in La Jolla, it was a logical leap to see if it would be possible to

print sensors on neoprene, the synthetic-rubber fabric typically used in wetsuits for divers and surfers.

A university of California-San Diego release reports that the result is the development of "wearable electrochemical sensors for in situ analysis in marine environments." The paper, published last month in the journal Analyst, was co-authored by UCSD's Wang, Windmiller, and visiting scholar Gabriela Valdés-Ramírez.



Flexible sensors printed on neoprene wetsuit sleeve // Source: calit2.net

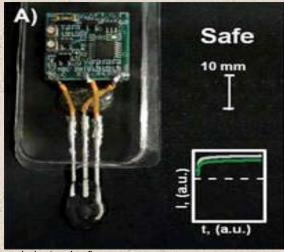
Breakthroughs in nanoengineering often involve building new materials or tiny circuits. A professor at the University of California, San Diego, however, is proving that he can make materials and circuits so flexible that they can be pulled, pushed, and contorted — even

from Mexico, as well as Michael J. Schöning and Kerstin Malzahn from the Institute of Nanoand Biotechnologies of Germany's Aachen University of Applied Sciences.

UCSD has a full U.S. patent pending on the technology, and has begun talks on licensing the system to a Fortune 500 company.

Wang's 20-person research group is a world leader in the field of printable sensors. To prove that the sensors printed on neoprene could take a beating and continue working, some of Wang's colleagues took to the water.

"Anyone trying to take chemical readings under the water will typically have to carry a portable analyzer if they want to detect pollutants," said Wang, whose group is based in the California Institute for Telecommunications and Information Technology (Calit2) at UCSD. "Instead, we printed a three-electrode sensor directly on the arm of the wetsuit, and inside the neoprene we embedded a 3-volt battery



#### and electronics."

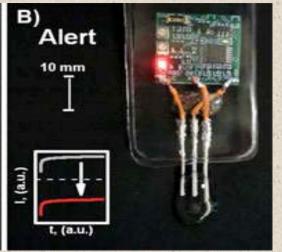
The electrochemical sensors are based on applying voltage to drive a reduction-oxidation (redox) reaction in a target threat or contaminant — which loses or gains electrons — then measuring the current output. The wearable microsystem provides a visual indication and alert if the levels of harmful contaminants or explosives exceed a predefined threshold. It does so by mixing different enzymes into the carbon ink layer before printing on the fabric. (For example, if the enzyme tyrosinase interacts with the pollutant phenol, the LED light switches from green to red.)

The release notes that the electronics are packed into a device known as a potentiostat that is barely 19 mm by 19 mm (the battery is stored on the reverse side of the circuit board.)

In the experiments described in the Analyst article, Wang and his team tested sensors for three potential hazards: a toxic metal (copper); a common industrial pollutant, phenol; and an explosive (TNT). The device also has the potential to detect multiple hazards. "In the paper we used only one electrode," noted Wang, "but you can have an array of electrodes, each with its own reagent to detect simultaneously multiple contaminants."

The researchers believe that neoprene is a particularly good fabric on which to print sensors because it is elastic and repels water. It permits high-resolution printing with no apparent defects.

The UCSD team tested the sensor for explosives because of the security hazard highlighted by the 2000 attack on the USS Cole in Yemen. The Navy commonly checks for underwater explosives using a bulky device that a diver must carry underwater to scan the



ship's hull. Using the microsystem developed by Wang and his team, the sensor printed on a wetsuit can quickly and easily alert the diver to nearby explosives.

Wang's lab has extensive experience printing sensors on flexible fabrics, most recently demonstrating that biosensors printed on the rubber waistband of underwear can be used continuously to monitor the vital signs of soldiers or athletes. The researchers were uncertain, however, about whether bending the printed sensors under water – and in seawater – would still let them continue functioning properly.

In the end, even underwater, and with bending and other deformations, the sensors continued to perform well. "We still need to validate and test it with the Navy," said Wang. "While the primary security interest will be in the detection

of explosives, the Navy in San Diego bay has also detected large concentrations of toxic metals from the paint on Navy ships, so in principle we should be able to print sensors that can detect metals and explosives simultaneously." Wang's work in flexible sensors grew out of twenty years of experience with innovations in glucose monitoring, ultimately in the form of flexible glucose strips that now account for a \$10 billion market worldwide. Work on the underwater sensors was supported by the Office of Naval Research.

— Read more in Kerstin Malzahn et al., "Wearable electrochemical sensors for in situ analysis in marine environments," <u>Analyst</u> 136 (2 June 2011):2912-17

#### Natural enzyme can defend against terrorists' nerve agents

Source:http://www.homelandsecuritynewswire.com/natural-enzyme-can-defend-against-terrorists-nerve-agents



Chemicals called organo-phosphates, found in common household insecticides, can be just as harmful to people as to insects. That fact did not escape the notice of German scientists during the Second World War, who used organophosphates to make a collection of deadly liquids and gases that can cause lethal damage to the nervous system. These nerve agents still exist, and they pose a potential threat to people around the world.

A National Institute of Health (NIH) release reports that the good news is that the United States is working with other governments to destroy nerve agent stockpiles. Meanwhile, scientists are devising drugs to treat and prevent the toxic effects of organophosphates and related chemicals.

Biochemist Dan S. Tawfik, Ph.D., and his colleagues at the Weizmann Institute of Science in Rehovot, Israel are working to turn a natural enzyme into a drug capable of breaking down organophosphates. His research is

# 1995 Tokyo sarin attack killed twelve // Source: semp.us

supported by the NIH Countermeasures Against Chemical Threats (CounterACT) program, which aims to enhance medical responsiveness to chemical disasters.

"Drugs based on Dr. Tawfik's approach would be a valuable addition to our nation's ability to mount an effective medical response in the event of a chemical emergency," said David A. Jett, Ph.D., the lead contact for

CounterACT and a program director at the National Institute of Neurological Disorders and Stroke (NINDS).

German, or "G-type," nerve agents were never deployed during the Second World War, but they have been used for malicious ends. In 1995, a terrorist group in Tokyo released the G-type agent sarin into the subway system, killing twelve people and causing thousands to seek medical attention.

Although not as lethal as nerve agents, organophosphate insecticides can be harmful in large or prolonged doses. Moreover, they could be released on an industrial scale, through an act of terror or accident.

The release notes that organophosphates attack the nervous system by inactivating an enzyme called acetylcholinesterase (AChE). AChE controls levels of the chemical acetylcholine (ACh), which regulates brain function, muscle contraction, heartbeat and breathing. When AChE is inactivated, ACh bombards nerve cells and muscles. At lower,

doses, exposure to organophosphates can therefore cause difficulty concentrating, muscle spasms and asthma-like symptoms. At higher doses — such as might occur in a terrorist attack or large-scale accident — they cause seizures, paralysis, respiratory failure, and death.

There are limited drug treatments for nerve agent exposure. Diazepam is the only drug currently approved for nerve agent-induced seizures. Two other treatments – atropine and compounds called oximes – are meant to work as antidotes. Atropine prevents nerve and muscle cells from responding to ACh, and oximes reduce ACh levels by re-activating AChE. Unfortunately, these two drugs may not prevent lasting damage to the nervous system, Dr. Tawfik said.

"Atropine aims at the symptoms of nerve agent exposure, and oximes minimize the damage after it has already begun," he said. "Our goal is to develop a drug that can intercept organophosphates before they cause damage." In Nature Chemical Biology, Dr. Tawfik and his team report progress toward a drug based on an enzyme called serum paraoxonase (PON1). The normal business of PON1 is to break down

 $R = \begin{cases} \begin{cases} \frac{1}{2} - 0 & \frac{1}{2} \\ 0 - Cyclohexyl & 0 - Isopropyl \\ 0 - Cyclohexyl & 0 - Isopropyl \\ 0 - Isopropyl & 0 - Pinacolyl \\ 0 - Isopropyl \\ 0 - Isopropyl \\ 0 - Isopropyl \\ 0 - Pinacolyl \\ 0 - Pinaco$ 

biochemists like to say, it is promiscuous. It occasionally hooks up with and destroys organophosphates. The researchers theorized that they could amplify this behavior to turn PON1 into an organo-phosphatebusting machine.

The researchers have now succeeded in making rePON1 highly reactive against cyclosarin, a more toxic cousin of sarin. In test tube experiments, they show that rePON1 can break down cyclosarin with an efficiency 100,000 times higher than that of natural PON1.

The release notes that one drawback of rePON1 is that it has a short time window of effectiveness. If cyclosarin exposure was delayed until twenty-four hours after the lab mice received the enzyme, none of the mice lived. By that point, the enzyme had been almost completely cleared from their blood. To protect people against a nerve agent attack or accident, the enzyme needs to be hardier.

"We would like to see the enzyme sustained in the blood for several days and ideally two weeks," he said. His team is collaborating with others to tinker further with the protein's chemistry and increase its longevity. There is

> also hope of using rePON1 to treat people after they are exposed to cyclosarin and related compounds, he said. The release also reports that Dr. Tawfik and his team are working to develop a drug that can protect against Vtype agents, a class of organophosphate-based toxins developed nerve during the cold war era. VX is the most potent of all the organophosphate-based nerve agents. Less than one drop can be lethal.

compounds derived from fats, but as

— Read more in Rinkoo D Gupta, "Directed evolution of hydrolases for prevention of G-type nerve agent intoxication," <u>Nature Chemical Biology</u> 7 (9 January 2011): 120–25

# School Safety Plans Must Include Terrorism Response Procedures

Source:http://www.emergency-response-planning.com/blog/bid/39154/School-Safety-Plans-Must-Include-Terrorism-Response-Procedures?utm\_campaign=EmailMarketing\_Weekly+Blog+Highlight\_20110801



# STAT SAND

# Are You Ready?"

You only need to work one emergency response event to immediately understand the challenges of quickly triaging, tagging, and tracking multiple patients and all their belongings. StatBand triage, EMS, evacuation, and everyday emergency response tags make these tasks easier than ever by offering:

- Uniquely numbered barcode labels and triage tag facilitate quick and accurate identification and tracking of multiple victims and belongings
  - Fast tear-and-go design streamlines the triage process unlike difficult plastic sleeve tags
- Durable polymer construction withstands emergency conditions better than paper-and-string tags
- Patented one-piece tag and wristband combination with adhesive closure provides easy and secure application

SB-TRIAGE Triage Tags

- Meets <u>FEMA's Authorized Equipment List (AEL)</u> requirements and is allowable under 10 grant programs
- Fulfills multiple uses under U.S. Department of Health & <u>Human Services (HHS)</u> Hospital Preparedness Program (HPP), which was recently awarded more than \$352 million

Milling.

SB-EMS EMS Tags



SB-EVAC Evacuation Wristbands



SB-RAPID Rapid ID Tags SNAP THIS QR CODE WITH YOUR MOBILE PHONE

2010 EMSW&RLD INNOVATION

AWARD

STATIETA NO

Contact us to learn more about StatBand



www.statband.com

800 238.0870

info@statband.com

The process of developing a campus emergency plan to adddress terrorism can be overwhelming for school administrations. However, the potential for terrorist attacks makes it imperative that emergency plans include strategies to protect campuses, students, and staff. All schools should build on existing plans, work closely with local emergency agencies, and rehearse their plans accordingly.

Two key factors that must be considered in planning include the nature of terrorist threats and the available warning time allotted. According to FEMA, the weapons most likely to be used by terrorists fall into the following categories:

**Conventional** weapons include bombs and other explosive devices. The goal is to place inhabitants in a protected space and/or increase the distance from the potential explosive area. The following actions should be considered:

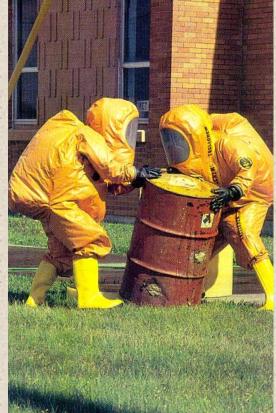
- Use basement areas
- Move to interior hallways away from windows
- Practice 'duck and cover' drill
- Shut off gas utilities
- Evacuate students and staff
- Release students to parents/guardians

<u>Chemical</u> weapons may be poisonous gases, liquids, or solids. The following actions should be considered:

- Secure doors/windows
- Turn off all ventilation, including furnaces, air conditioners, vents, and fans
- Seek shelter in an internal room
- Make decisions based on reliable information from public safety officials on the location of the chemical release and wind speed and direction
- Develop reunification procedures that minimize the penetration of airborne substances
- Communicate with medical personnel (intervene as appropriate or instructed)

**Biological** agents are organisms or toxins that have the potential to incapacitate people, livestock, and crops. They can be dispersed as aerosols, airborne particles or by contaminating food and water. These agents may not cause symptoms for days or weeks following an exposure. The following actions should be considered:

- Mitigate exposure (includes getting everyone into buildings)
- Secure avenues of penetration to include closing doors/windows and shutting down the heating ventilation, and air conditioning systems



- Develop reunification procedures that mitigate risks
- Develop a recovery plan in light of the highly contagious nature of these weapons
- Communicate with medical personnel

<u>Nuclear</u> weapons have special considerations, given the potential exposure to radiation. The overarching concern is to get individuals to a protected space or to increase the distance from the blast area. FEMA recommends taking shelter immediately as the three protective factors include distance, shielding, and time. Issues for consideration include, but are not limited to:

• Potential magnitude



- Emotional implications
- Contamination
- Casualties
- Unavailability of emergency resources
- Need for long-term sheltering
- Hazard analysis (proximity to nuclear power plant, military installation, chemical plants)
- Identification of at-risk persons or populations
- Safe evacuation procedures and routes
- Short-term and long-term recovery

It is essential that the roles and responsibilities of educators, law enforcement, fire officials, and other first responders are clearly described, reviewed, and updated. Communication procedures should detail methods of information distribution, including social media tools, between those on and off the site, parents, emergency responders, the community, and the media.

**NOTE:** Download the full guide (2003 Emergency Planning Guidelines for Local School Systems and Schools) from the Newsletter's website ("CBRNE-CT Papers" section)

# New Multi-Threat Portable Gas-Detection Monitors Now Available Following Extensive Field Testing

Source:http://www.marketwire.com/press-release/new-multi-threat-portable-gas-detection-monitors-now-available-following-extensive-field-1543001.htm

RAE Systems Inc. today announced its new portable MultiRAE instruments with unmatched sensor versatility have been field tested in responder, government and industrial environments, and are now available worldwide. The new MultiRAE monitors reliably give safety professionals unprecedented visibility and control of chemical and radiation threat data to enhance safety for workers, responders and the people they protect. The MultiRAE family of portable multi-threat monitors combines optional wireless functionality with best-in-class detection capabilities for continuous monitoring of toxic and combustible gases, volatile organic compounds, and radiation. The new MultiRAE monitors help reduce operation downtime, increase safety and improve incident-response times.

The new instruments were field tested in a range of environments worldwide, including oil and gas facilities and other industrial sites, U.S.



National Guard Civil Support Teams, and firefighting and HazMat teams, including the Aurora Fire Department in Illinois.

"During our testing of the new MultiRAE, we found the instrument to be easy to read and use, and extremely adaptable in meeting more



of our threat-detection needs in one portable instrument," said Don Davids, battalion chief for the Aurora Fire Department and co-chair for the Hazardous Materials Steering Committee for MABAS-Illinois. "With protection for up to six threats at a time, we can get gamma radiation, a PID and four-gas detection in one unit instead of carrying three different devices downrange."

#### Six Threats, One Instrument

The MultiRAE monitors are the world's first wireless multi-threat instruments that can be configured to detect and monitor more than 300 volatile organic compounds (VOCs), gamma radiation, 55 combustible gases and vapors, and 25 specific toxic gases -- up to six threats at a time -- all in a single, highly versatile monitor.

The MultiRAE monitors provide both personaland point-detection capabilities for a broad range of applications, including HazMat response, military, homeland security, and industrial safety and industrial hygiene.

When deployed on RAE Systems' Dedicated Wireless Network, MultiRAE instruments use a five-way notification system for gas, radiation and man-down alarms to provide immediate and unmistakable on-scene alerts while warning safety officers at a remote command center.

#### Availability

Non-wireless versions of the MultiRAE family of instruments, complete with all sensor options, are available now and can be purchased through authorized RAE Systems' distributors. Wireless-enabled versions of the MultiRAE monitors are expected to be available later this year. Non-wireless versions of the MultiRAE family can be updated to include wireless functionality with the purchase of a factory upgrade when it's available later this year.

#### **Chemical Weapons Terrorism on eBay**

Source: http://www.mediastory.net/2011/07/chemical-weapons-terrorism-on-ebay/



Norwegian terrorist Anders Breivik purchased most of the material he used in this attacks on .. eBay! Although he was under surveillance by the Norwegian security services, Anders managed to purchase chemical products that he used to manufacture the explosives.

According to a few sources, most materials used in the Oslo, Norway attack and in the massacre on the Utoya island were **purchased on eBay and from multiple manufacturers in the United Kingdom.** Breivik's online purchases caused no suspicions, although the man was monitored by the secret service for four months after he purchased.

chemical fertilizer from Poland.

Investigators announced that Anders Breivik initially had a more ambitious plan: he planned to commit multiple attacks using trap cars and his targets would have been the headquarters of the Labor Party and the Royal Palace.

However Breivik created only one bomb because he lacked the required materials. Breivik was questioned by the police for 10 hours and he told investigators that he initially had multiple targets. According to the Oslo Chief of Police, Anders was calm and he cooperated with the investigators. The final conclusions of the investigation will be presented in a few weeks. The two psychiatrists tasked with verifying Breivik's mental health are to file a report on November 1. His trial will probably start next year.

**US Department of Defense Contract Award for Avon Filters** 

Source: http://www.avon-protection.com/

Avon Protection has announced (8 Aug 2011) that it has been awarded a 3 year IDIQ (indefinite delivery indefinite quantity) contract from the US Department of Defense for the continued supply of M61 filters for use with Avon's M50 respirator.



The maximum contract value is approximately \$38 million with an initial order value of \$11 million which Avon expects to fulfill in this financial year.



Commenting on the news, Peter Slabbert, Chief Executive said: "As we anticipated when investing in additional production capacity in 2010 at our Cadillac, US manufacturing base, we are seeing growing demand for consumable filters as increasing numbers of

Avon mask systems are supplied and issued to the troops in the field. As the sole source supplier of this unique conformal filter, we believe this growth will continue."

# THE FIRST LINE OF DEFENSE FOR THOSE WHO SERVE

# RSD Neutralizes or Removes Known Chemical Warfare

**Agents From The Skin.** 

FAST • SAFE on SKIN • PROVEN ASSURANCE\*



IMPORTANT SAFETY INFORMATION: For external use only. Contact with eyes and mucous membranes should be avoided. In emergency conditions, RSDL does not require immediate removal from the skin and can be left on under protective clothing, but should be rinsed as soon as it is safe to do so. An ingredient of RSDL is absorbed. Studies with RSDL left on the skin for 24 hours showed minimal adverse effects. Avoid prolonged skin contact.

\* U.S. Army Medical Research Institute of Chemical Defense (USAMRICD); E.H. Braue Jr. et. al.; (2008); Efficacy Comparison of RSDL, M291 SDK, 0.5% Bleach and 1% Soapy Water Challenged with Soman, Cyclosarin, VX, and Russian VX (VR)

Additional information is available at:

# www.RSDecon.com

107 College Road East, Princeton, NJ 08540 USA Phone 1.888.773.3266 • Int'l calls 1.631.226.2090 RSDecon is a Business Unit of Bracco Diagnostics Inc. ©2010 RSDecon.

# OUR FOUNDATION IS OUR TECHNOLOGIES OUR MISSION IS EXPANDING YOUR CAPABILITIES

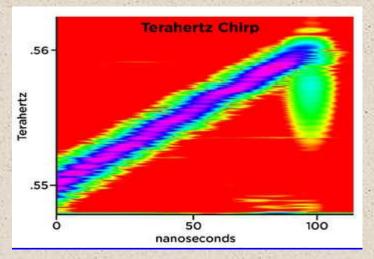


Scott Safety, formerly Scott Health and Safety, are world leaders in the design and development of Respiratory Protection Equipment (RPE). We have a detailed understanding of the physiological and physiological burden RPE can place on users. That is why we test in the field. And we apply what we learn there – as well as emerging research and technologies to every design to ensure capability, functionality and comfort. Irrespective of whether your requirement is for CBRN protection, Breathing Apparatus for EOD, USAR, damage control, fire-fighting or for specialist applications Scott can meet your requirements – comfortably.

# The Secret Behind NIST's New Gas Detector? Chirp Before Sniffing

Source: http://www.nist.gov/pml/div685/chirp-051011.cfm

Trace gas detection, the ability to detect a scant quantity of a particular molecule—a whiff



Graph shows the NIST detector's linear increase in frequency as a function of time, sweeping from 550-561 Gigahertz in frequency over 100 nanoseconds. Click on the image to see an animation of the process, slowed to 5 seconds and using an audio chirp as an analogy to the terahertz chirp.

Credit: Douglass, NIST

of formaldehyde or a hint of acetone—in a vast sea of others, underlies many important applications, from medical tests to air pollution detectors to bomb sniffers. Now, a sensor recently developed\* at the National Institute of Standards and Technology (NIST) that is hundreds of times faster and more sensitive than other similar technologies may make such detectors portable, economical and fast enough to be used everywhere.

According to the NIST investigators, the new sensor overcomes many of the difficulties associated with trace gas detection, a technique also used widely in industry to measure contaminants and ensure quality in manufacturing. A trace level of a particular gas can indicate a problem exists nearby, but many sensors are only able to spot a specific type of gas, and some only after a long time spent analyzing a sample. The NIST sensor, however, works quickly and efficiently. "This new sensor can simultaneously detect many

different trace gases at very fast rates and with high sensitivity," says NIST chemist Kevin

Douglass. "It's also built from offthe-shelf technology that you can carry in your hands. We feel it has great commercial potential."

The key to the new sensor is the use of radiation at "terahertz" frequencies-between infrared and microwaves. Terahertz waves can make gas molecules rotate at rates unique to each type of gas, which implies the waves hold great promise for identifying gases and measuring how much gas is present. The NIST team has developed the technology to rotate the molecules "in phase"-imagine synchronized swimmers-and detect the spinning molecules easily as they gradually fall out of phase with each other.

A major hurdle the new technology overcomes is that it is now possible to look at nearly all possible gas

molecules instantly using terahertz frequencies. Previously, it was necessary to expose molecules to a vast range of terahertz frequencies—slowly, one after another. Because no technology existed that could run through the entire frequency band quickly and easily, the NIST team had to teach their off-theshelf equipment to "chirp."

"The sensor sends a quick series of waves that run the range from low frequency to high, sort of like the 'chirp' of a bird call," says Douglass. "No other terahertz sensor can do this, and it's why ours works so fast. Teaching it to chirp in a repeatable way has been one of our team's main innovations, along with the mathematical analysis tools that help it figure out what gas you're looking at."

The NIST team has applied for a patent on its creation, which can plug into a power outlet and should be robust enough to survive in a real-world working environment.

- E. Gerecht, K.O. Douglass and D.F. Plusquellic. Chirped-pulse terahertz spectroscopy for broadband trace gas sensing. Optics Express, April 22, 2011, Vol. 19, Issue 9, pp. 8973-8984 (2011)



# FIRST RESPONDERS NEED TO BE PREPARED FOR ANYTHING....

For expert and informed discussion on how to face your CBRN threat contact:

- USA Tel: +1 540 604 4478 Email: frontline@remploy.com
- UK Tel: +44 (0)845 241 2990 Email: frontline@remploy.co.uk

# www.remployfrontline.com

# SO DO DUR SUITS Remploy<sub>Frontline</sub>

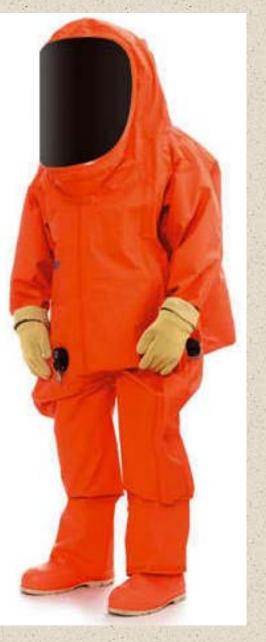
# New chemical protection suit

## Dräger CPS 7900

Source:http://www.draeger.com/UK/en/products/personal\_protection/body/gastight\_suits/cre\_c ps\_7900.jsp

The gas-tight suit Dräger CPS 7900 provides excellent protection against industrial chemicals, biological agents, and other toxic substances. Its innovative material qualifies the CPS 7900 equally well for work in explosive areas and for handling cryogenic substances.

The chemical protective suit Dräger CPS 7900 was developed to protect its wearer when handling toxic or hazardous materials and to provide much needed support for a

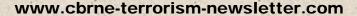


variety of dangerous tasks. The suit material D-mex offers unique resistance to various substances as well excellent protection against mechanical effects, liquefied gases, and flash fires. The Dräger CPS 7900 meets and exceeds the requirements of international standards of fire departments, search and rescue organizations, and industry for reusable protection suits.

The suit's innovative and unique material D-mex<sup>™</sup> consists of five layers. An especially sturdy elastomer layer as well as a barrier layer resistant to chemicals is on the inside as well as the outside. This allows the suit to retain its full protective capacity even when the material on the outside becomes damaged. Its electrostatic properties make it possible to use the suit in all explosive areas. If a spark occurs in spite of this remarkable fabric, the flameretardant and self-extinguishing material protects its wearer from serious burns. The flexibility of D-mex<sup>™</sup> even makes it possible to handle liquefied gases such as ammonia at a contact temperature of -80°C.

The chemical protective suit reduces the stress during the already difficult work in hazard zones and danger areas. With its new, ergonomic cut and five available sizes, the suit offers its wearers with a body height of 1.50 m to 2.10 m the highest degree of mobility during a wide variety of activities and tasks. Moreover, the clearly lighter weight and better drape of the suit material adjusts to the wearer's movements and offers the full range of flexibility.

Innovative materials and new service concepts made it possible to significantly reduce time and expenses for regular testing and expenses. In addition, the suit can be easily cleaned and disinfected. This means the time and expense spent over



the 15 years of service life of the suit is much less.

hazardous atmospheres. The route to the deployment location and the

### CHEMICAL TESTS

Chemical	Breakdown time in min*	Chemical	Breakdown time in min*	Chemical	Breakdown time in min*
Acetone	>540	Ethyl acetate	>540	Sarin (GB)**	>1440
Acetonitrile	>540	Ethylene oxide	>540	Sodium hydroxide 40%	>540
Ammonia	>540	Hydrogen chloride	>540	Soman (GD)**	>1440
1,3-Butadiene	>540	Lewisite (L)**	>180	Sulfuric acid 96%	>480
Carbon disulfide	>540	Methanol	>540	Tetrachlorethylene	>540
Chlorine	>540	Methyl chloride	>540	Tetrahydrofuran	>540
Dichloromethane	>540	Mustard gas (HD)**	>1440	Toluene	>540
Diethylamine	>540	n-Heptane	>540	VX**	>1440

A continuously updated database is available to stay informed about chemical resistances and decontamination processes.

\* breakthrough time according to EN 943 Part 2.

 $^{\star\star}$  breath through time according to FINABEL 0.7.C

Accessories are available to customize the chemical protective suit to meet your specific needs and requirements, thereby expanding your range of application options. Including pressure gauge holder, height adjustment, anti-fog visor and D-Connect.

decontamination location must be bridged. The actual tasks must be completed. This is followed by a careful decontamination so that suits can be removed. The amount of air available in a compressed air breathing apparatus often is insufficient to cover both activities. For this reason the suit can be



Breathing air is a scarce commodity when it comes to runs involving toxic materials or

equipped with optional pass thrus.





CBRNe Enterprise Virtual Conference Series New & Emerging Technologies Expo October 5, 2011 10am - 6pm (EST)

ome Schedule of Events Attendee Information Sponsor Information Sign Up Today! Contact



You still have time to register!!!

## 1st Detect receives U.S. patent for chemical detector

Source: http://www.1stdetect.com/PR\_1st\_Detect\_Patent\_Issued.pdf

A portable mass spectrometry detector, capable of detecting residues and vapors from explosives, chemical warfare agents, toxic chemicals, food and beverage contamination,



illicit drugs and pollution, is awarded U.S. patent

Austin, Texas-based 1st Detect Corporation, a subsidiary of Astrotech Corporation, said yesterday that that the U.S. Patent and Trademark Office (USPTO) has issued a patent for the company's method to drive a mass spectrometer ion trap used for chemical detection and identification. "We are extremely pleased that the USPTO has issued this highly significant patent covering our unique ion trap technology," said John Porter,the company's CEO. "We continue to make considerable progress in our development of the 1st Detect Miniature Chemical Detector (MCD) and this patent is an important component of our intellectual property portfolio."

The patent, entitled "Driving a Mass Spectrometer Ion Trap or Mass Filter," represents an important technological advantage for 1st Detect.

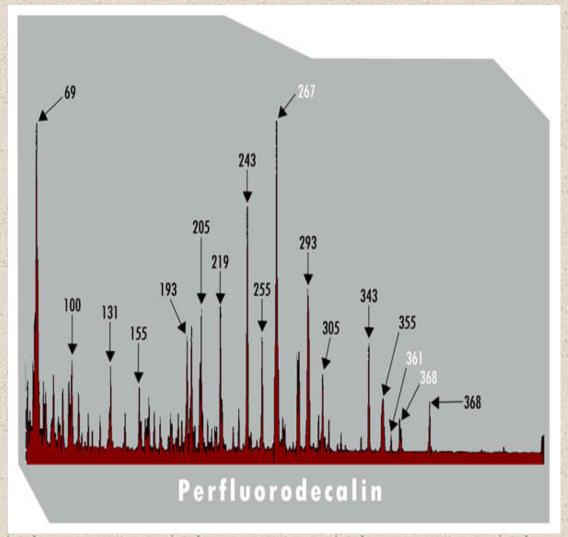
"The technology protected by this patent supports our objective to offer the most affordable, high performance mass spectrometer for both laboratory and field applications," added David Rafferty, the inventor of the patent (U.S. 7,973,277) and president of the Company.

1st Detect Corporation has developed the Miniature Chemical Detector, a product that offers lab performance mass spectrometry in a small, portable package. The company says the capabilities of the instrument makes MCD a suitable detection tool for a variety of applications, including security, industrial and healthcare markets.

The company says that Miniature Chemical Detector is capable of detecting residues and vapors from explosives, chemical warfare agents, toxic chemicals, food and beverage contamination, illicit drugs and pollution

The 1st Detect Chemical Detector offers the

mass range, low detection limit, MS<sup>n</sup> capability



capabilities and performance of a large laboratory mass spectrometer, including a wide

and a membrane inlet in a low power portable instrument.

- Weight:
  - 12 lb / 6 kg on 12/24 VDC or 110 / 220 VAC
  - o 15 lb / 7 kg on supplied battery
- Mass Range: 10 450 amu
- Chemicals Detected (examples):
  - o CWAs: GA, GB, VX, mustards, cyanides
  - Explosives: TATP, PETN, TNT, DNT, RDX
  - TICs per NIJ Guide 100-00 and per ITF-40
  - o Contraband: THC, cocaine, amphetamine
- Resolution: <1 amu</li>
- Detection Limit / Analysis Time:
  - ppb / ng @ < 5 sec operation (continuous sampling & analysis)</li>
  - ppt / pg @ < 30 sec operation (5 sec. sampling / 25 sec. analysis)</li>
- Power Supply: 120/240VAC, 12/24VDC or supplied battery
  - Low False Alarm Rate: True Mass Spectrometer (not IMS) and MSn Capability
    - MS: 10x the informing power of IMS.
    - o MS/MS: 10000x the informing power of IMS.
- SAFETY Act
  - Awarded Developmental Testing and Evaluation (DT&E) Designation from the U.9.
     Department of Homeland Security

# A WORLD LEADER IN CBRN RESPIRATORY PROTECTION EQUIPMENT.



# Helping the military breathe easy on land, air and sea for more than 80 years.

Ambition 2011 22nd - 23rd June The International Centre, Telford, West Midlands Stand# C17 & C24

# Visit Avon Protection at:

JIIM-IA CBRN Regimental Week and Conference 21st - 23rd June Ft. Leonard Wood, MO LAUSA ILW Army Medical Symposium & Exposition 27th - 30th June San Antonio, TX

Please visit the information desk for stand number

Joint Service General Purpose Mask (JSGPM) and other PPE available through GSA



© 2011 Avon Protection Systems, Inc.

For inquiries in The Americas: t: 1 888 286 6440 e: customerservice@avon-protection.com

For inquiries in Europe, Middle East, Asia: t: +44 (0) 1225 896705 e: protection@avon-rubber.com www.avon-protection.com





# FULL SPECTRUM PROTECTION WE GO BEYOND

VISIT US AT DSEI 2011 (13-16 September) STAND NO. S7-250

BLÜCHER GmbH +49 211 9244 0 phone +49 211 9244 211 fax infoldbluecher.com www.bluecher.com BLÜCHER SYSTEMS GmbH +49 2153 9540 0 phone +49 2153 9540 70 fax info@bluechersystems.com www.bluechersystems.com BLUECHER UK Ltd. +44 1507 451 443 phone info@bluecheruk.com www.bluecher.com



# Libya: Securing Stockpiles Promotes Security



Office of the Spokesperson Washington, DC August 26, 2011 Source: http://www.state.gov/r/pa/prs/ps/2011/08/171101.htm

Libya has been a country of proliferation concern and attention by the United States for many years. Since the beginning of the crisis in Libya this year, the United States has focused on the potential that increased insecurity on the ground could increase proliferation risks, including with the country's remaining stockpiles of uranium, chemical agents, and conventional weapons. We have remained intensely focused on preventing proliferation as the crisis has evolved. Monitoring relevant facilities and supporting Libya's efforts to secure those arms and materials have been and remain key priorities.

The United States has stressed the importance of securing these materials and arms stockpiles and has taken action to prevent their proliferation. Secretary of State Hillary Rodham Clinton, Assistant Secretary Jeffrey Feltman, Ambassador Gene Cretz, and Special Representative Chris Stevens have raised these issues with Libya's Transitional National Council (TNC), which has made clear that it recognizes the importance of securing all proliferation-sensitive materials and weapons. Libya is a state-party to non-proliferation agreements, including the Nuclear Nonproliferation Treaty, the Chemical Weapons Convention, and the Biological Weapons Convention. We welcome the assurances that we have received from the TNC that Libya will meet all of its international commitments. The United States is supporting Libya in upholding these obligations and stands ready to assist in securing or safely eliminating materials and arms that pose proliferation risks.

### **Nuclear-Related Sites**

- All sensitive elements of Libya's nuclear program, including those received from the A.Q. Khan network, were removed in early 2004.
- Libya's remaining inventory of highly enriched uranium was completely removed as of December 2009, marking the end of a five-year effort to convert the research reactor at the Tajura nuclear research center to run on low enriched uranium fuel. Nevertheless, we continue to closely monitor the facility.
- We also continue to monitor Libya's stockpile of uranium yellowcake. This material would need to go through an extensive industrial process, including enrichment, before it could be used in building a bomb. Such processes do not exist in Libya.



#### **Chemical Agents**

 All of Libya's remaining chemical stocks – 11.3 metric tons of mustard agent and 845 metric tons of chemical precursors – are located together in non weapons-useable form in a remote area far removed from the fighting, inside steel containers placed within bunkers accountable to the Organization for the Prohibition of Chemical Weapons (OPCW). Based on all our current information, we assess that this facility is secure.

- These extremely hazardous materials are in a bulk form, and require a high-level of expertise, sophistication, and proper equipment in order to utilize the bulk agent in a usable weapon. We continue to monitor these materials.
- The Qadhafi regime destroyed the aerial bombs manufactured to deliver its chemical weapons in 2004 under the supervision of international inspectors from the Chemical Weapons Convention implementing organization, the OPCW.

#### **Ballistic Missiles/Scuds**

- Prior to the crisis, Libya had an estimated force of 400 aging Scud ballistic missiles, a majority of which are assessed not to be operational.
- These missiles have a limited range of 300 kilometers.

#### **Conventional Weapons**

- Since the beginning of the crisis, we have been actively engaged with our allies and partners to help prevent the proliferation of Libya's conventional weapons. Our main concern is Libya's inventory of shoulder-fired anti-aircraft missiles, also known as Man-Portable Air-Defense Systems (MANPADS).
- The United States is working with NATO to provide all known locations of such weapons so that the TNC can secure and eventually dispose of these weapons.
- The United States is providing \$3 million in support to two NGOs, MAG International and the Swiss Foundation for Demining to recruit and train staff local explosive ordnance disposal teams. The teams have been operating in the east since May, but will move to areas in western Libya as the security situation improves. These teams also are providing assistance and guidance to the TNC in the routine recovery of potentially unstable munitions and classifying these for safe storage or destruction. To date teams have cleared over 450,000 square meters of land and destroyed over 5.8 tons of munitions, including five MANPADS.
- The State Department-led MANPADS Task Force has led two teams of experts to the region where they consulted with Libya's neighbors over ways to counter possible proliferation of MANPADS and conventional weapons. The inter-agency teams visited Mauritania, Egypt, Algeria, Tunisia, Mali, Morocco, Niger, and Chad.
- The State Department and other international actors have emphasized to the Transitional National Council that the Libya's future leaders must effectively secure MANPADS and other conventional weapons. In early August, State Department experts met with TNC representatives in Malta to convey concerns over potential MANPADS proliferation.

# Hospital Emergency Response Teams

Triage for Optimal Disaster Response Authors Jan Glarum, Emergency Response Consultant, Alcoa, TN, USA, Don Birou and Ed Cetaruk

Paperback, 256 Pages Published: DEC-2009 ISBN 13: 978-1-85617-701-6 Imprint: Butterworth Heinemann

A hospital can continue to function during a disaster or terrorist attack if a Hospital Emergency Response Team (HERT) protects the facility by the establishing and staffing of an Emergency Treatment Area. For the first time, here is an entire text dedicated to developing a free-standing operational team capable of protecting the healthcare center and its employees. This unit, if properly designed, is mobile enough to operate at a remote site, offering services to less prepared facilities. Not only does the hospital gain operational capacity by creating such a team, it also goes a long way toward meeting JCAHO's accreditation requirements.





# HOSPITAL EMERGENCY **RESPONSE TEAMS**



Jan Glarum Don Birou Edward Cetaruk, HD

This book covers information that in an emergency is crucial to emergency medical service personnel and hospital staff in the emergency department, nursing, clinician, and other technical or support positions. It is also required reading for community public safety personnel and those charged with community-level planning, allowing them to better understand hospital capabilities and needs in times of disaster.

#### Contents

- Chapter 1: Command and Control •
- Chapter 2: Assessment of Likely Mass Casualty . Events and Potential Hospital Impact Planning
- Chapter 3: Personal Protective Equipment (PPE) •
- Chapter 4: Emergency Treatment Area •
- **Chapter 5: Triage Principles** .
- Chapter 6: Decontamination .
- **Chapter 7: Special Circumstances** .

"...an excellent starting point for someone about to embark on the process of building a decontamination program in his or her facility."--Anjanette Hebert, Director of Security and Safety, Lafayette General Medical Center, Lafayette, LA

## General Dynamics to integrate CBRN device in Army radios

Source:http://www.homelandsecuritynewswire.com/general-dynamics-integrate-cbrn-device-armyradios

General **Dynamics** C4 Systems announced last week that it will work with U.S. Army researchers to install wirelessnetworking chips on radios that can also detect the presence of dangerous chemicals on the battlefield.

The plan comes as part of the Army's efforts to develop advanced infantry radios capable of rapid detection and warning of chemical, biological, radiological, and nuclear threats. The Army hopes that the radios will also be capable of mapping the hazards to



provide situational awareness and transmit the data to those on the battlefield as well as commanders.

The company's chips will be embedded in the Army's AN/PRC-154 Rifleman radio system.

Army Research Development and **Engineering Contracting Center officials** will negotiate a contract with General Dynamics for its Joint Warning and Reporting Network (JWARN) Component Interface Device (JCID)-ona-Chip (JoaC).

Army officials say that General Dynamics is the only firm capable of integrating the chips into the radio in eight months.



# Bio News

# Innovative duct tape strategy saves hospitals time, money; improves infection prevention

Source: http://www.sciencedaily.com/releases/2011/06/110627095644.htm

A simple roll of duct tape has proven to be an



inexpensive solution to the costly and timeconsuming problem of communicating with hospital patients who are isolated with dangerous infections.

A 504-bed Midwestern health system saved up to 2,700 hours and \$110,000 a year by creating a "Red Box" safe zone, a three-foot square of red duct tape extending from the threshold of the door, to facilitate communication with patients on isolation or "Contact Precautions," according to an abstract presented today at the 38th Annual Educational Conference and International Meeting of the Association for Professionals in Infection Control and Epidemiology (APIC).

Conducted by the infection prevention team at the Trinity Medical Center in the Quad Cities on the Iowa/Illinois border, the study revealed that by utilizing this safe zone, their hospitals were able to save time, money in unused gowns and gloves, and that the quality and frequency of communication between healthcare professionals (HCP) and isolated patients increased. Typically, HCPs must don personal protective equipment (PPE) before entering an isolated room before any type patient's of communication. Dressing in gowns and gloves before each interaction is time-consuming, costly and creates communication barriers with patients. The study showed that HCPs could safely enter the Red Box area without PPE for quick communication and assessment. At Trinity, approximately 30 percent of interactions with patients on Contact Precautions were performed in the Red Box.

In a satisfaction survey, 67% of healthcare workers said that the Red Box lessened barriers when communicating with patients. Also, 79.2% reported that the Red Box saved time in not having to put on and remove PPE. The same number said healthcare workers could assess and communicate with patients more easily. The box also serves as an additional visual cue to remind HCPs that they are entering an isolation room, which is usually only indicated by a sign outside the patient's room.

"This is an innovative strategy that could be of great value to other hospitals," said study author Janet Nau Franck, RN, MBA, CIC. "It costs as much as a roll of tape, and yet pays off with significant savings in time, money and increased satisfaction for both patients and staff."

"This is a simple but very effective mechanism to conserve resources and yet remain in touch with the patient," said APIC 2011 President Russell N. Olmsted, MPH, CIC. "It can serve as a model for healthcare providers who strive to deliver better care and reduce costs." The

study took place from January 2009 to

December 2010.

# House introduces new biological weapons legislation

Source:http://www.homelandsecuritynewswire.com/house-introduces-new-biological-weapons-legislation

Last Thursday lawmakers from the House Homeland Security Committee unveiled new legislation designed to help bolster federal efforts to prevent bioterror attacks and the use of other weapons of mass destruction.

Under the proposed bill, a new special assistant to the president for biodefense would be created. The position is tasked with guiding national efforts to combat biological threats and would coordinate federal agencies in crafting and executing strategic plans.

In particular, the special assistant would be responsible for creating a national strategy for biosurveillance, identifying data and distributing it to relevant federal agencies, spearheading information sharing initiatives across federal, state, and local law enforcement and public health agencies, and increasing the government's ability to track and respond to a biological event.

The new position would replace DHS's National Biosurveillance Integration Center, which was created in 2008 to detect biological incidents.

The bill comes in response to many of the recommendations made by the Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism, a panel created by Congress in 2009.

The commission found that the United States was currently unprepared for a WMD attack and gave the Obama administration an "F" on preparedness citing its failure to develop a

comprehensive strategy to prevent and respond to a biological or chemical attack.

"Weapons of mass destruction create a risk of catastrophic consequence but they are of low probability," said Representative Dan Lungren (R-California), the chairman of the Homeland Security Cybersecurity, Infrastructure Protection and Security Technologies Subcommittee.

"In such circumstances perhaps it's not surprising complacency and inactivity are our biggest vulnerabilities," he added.

Former Senator Jim Talent (R-Missouri), who co-chaired the WMD commission, welcomed the proposed bill and said current efforts are "not real time enough."

"We cannot have confidence today we will know an attack has occurred within the period of time [needed] to respond," he said.

Talent also pointed out that the new special assistant position was critical as someone "with clout and the ear of the president" needed to be in place to continue to spur the White House and Congress to address urgent WMD issues.

The legislation was formally introduced on Friday by Representatives Bill Pascrell (D – New Jersey) and Peter King (R – New York). The bill is called the "WMD Prevention and Preparedness Act of 2011" and Senator Joe Lieberman (I-Connecticut) says he plans to introduce a similar piece of legislation in the Senate soon.

# Singapore Health Sciences Authority Approves Emergent BioSolutions Anthrax Vaccine, BioThrax

Source: http://www.medicalnewstoday.com/releases/229572.php

Emergent BioSolutions Inc. announced today that the Singapore Health Sciences Authority (HSA) has approved Emergent's product license application for the marketing and sale of BioThrax® (Anthrax Vaccine Adsorbed) in Singapore. BioThrax is the only vaccine licensed by the U.S. Food and Drug Administration (FDA) to protect against anthrax infection.

BioThrax BioThrax ANTHRAS A "Emergent is pleased with this development as it continues to grow its presence in the Pacific Rim," said Daniel J. Abdun-Nabi, president and chief operating officer of Emergent BioSolutions. "With HSA approval of BioThrax, we look forward to initiating discussions with the government of Singapore, as well as other allied governments that recognize HSA registered products such as Brunei, to help

sm-newsletter.com

www

protect their constituents against the threat of anthrax as a biological weapon."

HSA is the statutory board of the Singapore Ministry of Health that administers the country's regulatory framework for pharmaceuticals,

About BioThrax

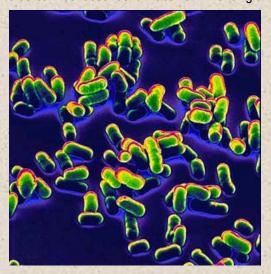
complementary medicines, medical devices and other health products. Its vision is to be the leading innovative authority that protects and advances national health and safety in Singapore.

BioThrax is the **only FDA-licensed vaccine for the prevention of anthrax** infection. It is indicated for the active immunization of adults who are at high risk of exposure to anthrax. BioThrax is manufactured from a culture filtrate, made from a non-virulent strain of *Bacillus anthracis*. To date, Emergent has delivered over 42 million doses of BioThrax to the U.S. government and continues to deliver additional doses under active procurement contracts. Since 1998, over 10 million doses have been administered to more than 2.5 million military personnel.

# New Discovery In Battle Against Plague And Bacterial Pneumonias

Source: http://www.medicalnewstoday.com/releases/229790.php

Researchers from the Smiley lab at the Trudeau Institute have now identified a single component of the plague causing bacterium that can be used as a vaccine. This single



"subunit" could potentially be used to create a safer form of a T cell-stimulating plague vaccine. The new data is featured in the July issue of The Journal of Immunology. "To date, there has been little progress in the development of safe and effective vaccines for plague or similar bio-weapons," said Dr. Stephen Smiley, a leading plague researcher and Trudeau Institute faculty member. "Our data identifies a single component of the plague causing bacterium seen by T cells. This could be a key discovery as we seek to develop a plague vaccine." The lab envisions that this subunit might be added to others already being studied for their ability to induce antibody responses. Together, these multiple subunits might safely induce both antibody and T cell responses, thereby better combating plague. According to Dr. Smiley, there is no licensed plague vaccine in the United States. Together with postdoctoral associate Jr-Shiuan Lin, he is working to develop a vaccine that will protect members of the armed services and public from a "plague bomb."

Plague is caused by Yersinia pestis, arguably the most deadly bacteria known to man. Yersinia pestis (photo) infections of the lung, known as pneumonic plague, are extremely lethal and usually lead to death within a week of infection. This could be a major discovery in the ongoing battle between scientists working to develop a vaccine to protect against plague and the terrorists who seek to use plague as a weapon. Many of the highest priority bio-terror concerns are caused by bacteria that acutely infect the lung. These include anthrax, tularemia and plague. Most of the plague vaccine candidates that have been studied aim to stimulate B cells to produce plague-fighting antibodies. However, animal studies suggest that antibodies may not be enough to protect humans from pneumonic plague. The Smiley laboratory has shown that T cells can also fight. plague. The lab previously demonstrated the

an immunization with an experimental vaccine stimulates the production of T cells that provide partial protection against pneumonic plague. This vaccine consisted of a live but weakened version of the plague causing bacterium.

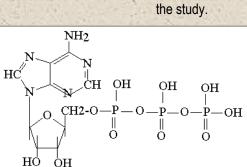
Live vaccines are often effective, but they can be difficult to license because they have the potential to grow within immunocompromised recipients and inadvertently cause disease. Additionally, Dr. Smiley believes these studies may help us learn to combat other kinds of pneumonia: "Bacterial pneumonia is one of the most common causes of death in hospitals and, like plague, many of these pneumonias are caused by bacteria that we may need to combat with both antibodies and T cells." Dr. Smiley's studies are funded by the Trudeau Institute and grants from the National Institutes of Health.

# How The Immune System Fights Back Against Anthrax Infections

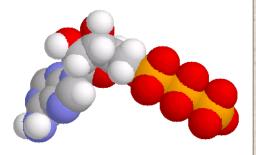
Source: http://www.medicalnewstoday.com/releases/228791.php

Scientists at the University of California, San Diego School of Medicine and Skaggs School of Pharmacy and Pharmaceutical Sciences have uncovered how the body's immune system launches its survival response to the notorious and deadly bacterium anthrax. The findings, reported online today and published in the June 22 issue of the journal Immunity, describe key emergency signals the body sends out when challenged by a lifethreatening infection.

Exposure to anthrax often proves deadly. anthrax The bacterium can invade immune cells called macrophages and release potent toxins that paralyze key biochemical pathways, causing rapid death. cell Unchecked. the process may completely collapse the body's immune defenses, allowing the bacteria to proliferate. and ultimately lead to septic shock and high mortality.



adenosine triphosphate (ATP)



the alarm and develop a survival strategy. Remarkably, the key signalling molecule involved in the survival response is adenosine triphosphate or ATP (photo), a basic currency of energy transfer used by all organisms. "The warning alarm sounded during anthrax infection is elegant, complex and can be effective in slowing spread of the pathogen," said Michael Karin, PhD, distinguished professor of pharmacology and senior author of the study.

> Karin explained that ATP is released from macrophages infected and poisoned with anthrax toxins through a special channel in the cell membrane. This ATP is then sensed by a receptor on a second macrophage, which assembles and activates a complex of molecules known as the inflammasome. The inflammasome then releases the into bloodstream an immuneactivating molecule known as interleukin-1beta (IL-1beta), which alerts macrophages throughout

the body to mobilize and increase their resistance to anthrax-induced cell death.

Researchers confirmed the importance of this complex signal transduction pathway in fighting anthrax in a series of experiments using genetically altered mice or inhibitor drugs.

The researchers discovered that the fight against invading anthrax bacteria begins with the first infected cell. They found that initially impacted macro-phages immediately communicate with other immune cells to sound

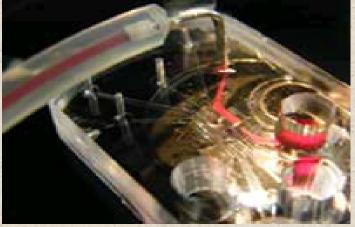
Whenever the researchers interfered with the ATP channel, the ATP receptor, inflammasome proteins or the IL-1beta molecule, they found that the macrophages could not survive, anthrax bacteria grew unchecked or the infected mouse died rapidly. They also noted that the immune response pathway responded only to the most dangerous bacterial pathogens. Infections using a mutant anthrax bacterium lacking the deadly toxins did not set off the alarm system in test animals.

"We hope these findings can be exploited for the design of new treatments to help the body combat serious bacterial pathogens," said Victor Nizet, MD, professor of pediatrics and pharmacy, whose infectious disease research laboratory contributed to the study. "Supporting the survival of macrophages and preserving their immune function may buy patients precious time until antibiotic therapy is brought on board to clear the infection."

#### Nano detector spots deadly anthrax

Source: http://www.eurekalert.org/pub\_releases/2011-07/ip-ndf070611.php

An automatic and portable detector that takes just fifteen minutes to analyze a sample suspected of contamination with anthrax is being developed by researchers in the United States. The technology amplifies any anthrax DNA present in the sample and can reveal the presence of just forty microscopic cells of the



#### deadly bacteria Bacillus anthracis.

*B. anthracis*, commonly known as anthrax, is a potentially lethal microbe that might be used intentionally to infect victims through contamination of food and water supplies, aerosolized particles, or even dried powders, such as those used in bioterrorist attacks in the United States in fall 2001. Detection is crucial to preventing widespread fatalities in the event of an anthrax attack.

The complexity of the microbe's biology have so far made it difficult to build a portable system that can be employed quickly in the field. That said, there are several systems available that use PCR to amplify a particular component of the genetic material present in anthrax and then to flag this amplified signal. These systems are fast and sensitive but do not integrate sample preparation and so are not as convenient as a single detector unit would be.

EurekAlet, citing Inderscience publishers, reports that Nathaniel Cady of the College of Nanoscale Science and Engineering (CNSE) of the University at Albany and colleagues there

> and at Cornell University, writing in International Journal the of **Biomedical** Nanoscience and Nanotechnology this month, explain they have constructed how nanofabricated fluidic cartridges that can be used to carry out detection of anthrax. The device is a so-called "lab-on-a-chip" device, or more properly a 3D microfluidic network that contains nanofabricated pillar structures.

The device has fluidic inputs for adding sample and reagents,

removing waste, for carrying out DNA purification, and critically an integrated chamber for amplifying only the target DNA in the sample using the polymerase chain reaction (PCR) system. The chip also contains a wave guide for the fluorescence-based identification of the amplified DNA and thus the target microbe. Importantly, the system works without manual intervention other than loading a droplet of sample into the detector.

"The average time required for DNA purification during these experiments was approximately 15 min, and when combined with real-time PCR analysis, this resulted in an average time to detection of 60 min," the team says. The system can detect as few as forty B. anthracis cells. "Due to its small size and low power requirements, this system can be further.

developed as a truly portable, hand-held

device," the researchers conclude.

— Read more in Nathaniel C. Cady et al., "PCR-based detection of Bacillus anthracis using an integrated microfluidic platform," International Journal of Biomedical Nanoscience and Nanotechnology 2, no. 2 (2011): 152-66

### Natural antibody brings universal flu vaccine closer

Source:http://www.homelandsecuritynewswire.com/natural-antibody-brings-universal-flu-vaccine-closer?page=0,1

Annually changing flu vaccines with their hitand-miss effectiveness may soon give way to a single, near-universal flu vaccine, according to a new report from scientists at the Scripps Research Institute and the Dutch biopharmaceutical company Crucell. They describe an antibody which, in animal tests, can prevent or cure infections with a broad variety of influenza viruses, including seasonal and potentially pandemic strains. The finding, published in the journal Science Express on 7 July 2011, shows the influenza subtypes neutralized with the new antibody include H3N2, strains of which killed an estimated one million people in Asia in the late 1960s.

"Together this antibody and the one we

reported in 2009 have the potential to protect people against most influenza viruses," said Ian Wilson, who is the Hansen Professor of Structural Biology and a member of the Skaggs Institute for Chemical



www.cbrne-terrorism-newsletter.com

Biology at Scripps Research, as well as senior author of the new paper with Crucell's chief scientific officer Jaap Goudsmit.

A Scripps Research Institute's release reports that Wilson's laboratory has been working with Crucell scientists since 2008 to help them overcome the major shortcoming of current influenza vaccines: They work only against the narrow set of flu strains that the vaccine makers predict will dominate in a given year, so their effectiveness is temporary. In addition, current influenza vaccines provide little or no protection against unforeseen strains.

These shortcomings reflect a basic flu-virus defense mechanism. The viruses come packaged in spherical or filamentous envelopes that are studded with mushroom-

shaped hemaglutinin (HA) proteins, whose more accessible outer structures effectively serve as decoys for a normal antibody response. "The outer loops on the HA head seem to draw most of the antibodies, but in a given strain these loops can mutate to evade an antibody response within months," said Wilson. Antiviral drugs aimed at these and other viral targets also lose effectiveness as flu virus populations evolve.

"The major goal of this research has been to find and attack relatively unvarying and functionally important structures on flu viruses," said Damian Ekiert, a graduate student in the Scripps Research Kellogg School of Science and Technology who is working in the Wilson

> laboratory. Ekiert and Crucell's Vice President for Antibody Discovery Robert H. E. Friesen are co-first authors of the Science Express report.

> By sifting through the blood of people who had been immunized with flu vaccines, Goudsmit and his colleagues several years ago discovered an antibody that bound to

one such vulnerable structure. In mice, an injection of the antibody, CR6261, could prevent or cure an otherwise-lethal infection by about half of flu viruses, including H1 viruses such as H1N1, strains of which caused deadly global pandemics in 1918 and 2009.

The Crucell researchers approached Wilson, whose structural biology lab has world-class expertise at characterizing antibodies and their viral targets. Ekiert, Wilson, and their colleagues soon determined the threedimensional molecular structure of CR6261 and its binding site on HA, as they reported in Science in 2009. That binding site, or "epitope," turned out to be on HA's lower, less-accessible stalk portion. The binding of CR6261 to that region apparently interferes with flu views ability to deliver their genetic material into host cells and start a new infection. That antibody is about to begin tests in human volunteers.

The release notes that Crucell researchers subsequently searched for an antibody that could neutralize some or all of the remaining flu viruses unaffected by CR6261, and recently found one, CR8020, that fits this description. As the team now reports in the Science Express paper, CR8020 powerfully neutralizes a range of human-affecting flu viruses in labdish tests and in mice. The affected viruses include H3 and H7, two subtypes of great concern for human health that have already caused a pandemic (H3) or sporadic human infections (H7).

As with the CR6261 project, Ekiert and colleagues were able to grow crystals of the new antibody bound to an HA protein from a deadly strain of H3N2, and to use X-ray crystallography techniques to determine the antibody's structure and its precise epitope on

the viral HA protein.

"It's even lower on the HA stalk than the CR6261 epitope; in fact it's closer to the viral envelope than any other influenza antibody epitope we've ever seen," said Ekiert.

Crucell is about to begin initial clinical trials of CR6261 in human volunteers, and the company expects eventually to begin similar trials of CR8020. If those trials succeed, aside from a vaccine the two antibodies could be combined and used in а "passive immunotherapy" approach. "This would mainly be useful as a fast-acting therapy against epidemic or pandemic influenza viruses," said Wilson. "The ultimate goal is an active vaccine that elicits a robust, long-term antibody response against those vulnerable epitopes; but developing that is going to be a challenging task."

6,000,000 DEATHS	
FROM INFLUENZA	<ul> <li>••••••••••••••••••••••••••••••••••••</li></ul>
This Is Estimate For World For Past 12 Weeks:	3
RECALLS BLACK DEATH	•
"Flu" Five Times Deadlier Than World War.	SAAR
LONDON, Dec. 18 Canadian Press.	

tia Reuter's )-The Times' medical correspondent says that it asems reasonable to believe that about 5,000 persons perished from influence pneumories during the past 13 weeks. It has been retimated that the war caused the death of 20,000,000 persons in four and a half years.

Thus, the correspondent points out, ur printense has proved itself five times ch we deadlier than war, because, in the same s. N

INFLUE	IZA DE	ATH
	IN ON	
KAIE	IN UNI	ALIO
Landan's Fala	11. L.I. 126	ter 100,000
10	Population.	
Statistics orr	and a second second second	J. W. B.
Methallough, ch	the other of	penith for,
Ontario, Indira		on of the
etting to this		abe death
rate from Spa	oven inflicence	and com-
purcations as a Mintes centers In given as 3	creat an in t	in tratted
Singlerie - Constants	Torophore	Math rate
is given as 33 was the bard rate beind \$49 suffered the so	and bla lin C	a scingeton
trata lating 640	100,000	Winniper
suffered the m	uni of any Ca	nation city.
according to U	he figures nor	e available.
	a the stand lotter.	Add 144 Det.
100.000	dan. Ohip. w	- 18 600
Carpp Privers	an mond. has	d the heav.
moldiers were	e of all it be	1.9 2.651 1.9
The Daures.	urlait Hnn	
The further,	which eyes	angeoprosi-
mate period o	Destine from	• <b>***</b>
	Influence inom	Denth
	compilies tions.	6 Rate
(211) and -	of The Law Plan.	1 Pille 100 000
	Pressoopta.	
		234
Sault Str. Mit	the second se	646 K.
Port Arthur		1 B 161
W Indone		104
SCIPHER SER		8 844
London		1 12
Terante	6	3 111
Winnipeg	5	1 744
Montreal	and a second	2 489
Hallfax	1	1 8 8 8 4 S
Hamilton	d States Pla	1 110
Units	d States 710	UT-100 311
Boston	1	791
·····································	1.1. A 10	2 210.
<ol> <li>1.357 marking 5 m art (2007)</li> </ol>		501
Camp bherl	Gan, CL. 842	2.561



Published Online 7 July 201 Science DOI: 10.1126/science.1204839

#### A Highly Conserved Neutralizing Epitope on Group 2 Influenza A Viruses

Damian C. Ekiert<sup>1</sup>, Robert H. E. Friesen<sup>2</sup>, Gira Bhabha<sup>1</sup>, Ted Kwaks<sup>2</sup>, Mandy Jongeneelen<sup>2</sup>, Wenli u<sup>1</sup>, Carla Ophorst<sup>2</sup>, Freek Cox<sup>2</sup>, Hans J.W.M. Korse<sup>2</sup>, Boerries Brandenburg<sup>2</sup>, Ronald Vogels<sup>2</sup>, Just P.J. Brakenhoff<sup>2</sup>, Ronald Kompier<sup>2</sup>, Martin H. Koldijk<sup>2</sup>, Lisette A.H.M. Cornelissen<sup>3</sup>, Leo L. M. Poon<sup>4</sup>, Malik Peiris<sup>4</sup>, Wouter Koudstaal<sup>2</sup>, Ian A. Wilson<sup>1</sup>,<sup>5</sup>, Jaap Goudsmit<sup>2</sup>

<sup>1</sup>Department of Molecular Biology, The Scripps Research Institute, 10550 North Torrey Pines Road, La Jolla, CA 92037, USA.

<sup>2</sup>Crucell Holland BV, Archimedesweg 4-6, 2301 CA Leiden, The Netherlands.

<sup>3</sup>Central Veterinary Institute, Wageningen University, Lelystad, the Netherlands.

<sup>4</sup>Department of Microbiology, The University of Hong Kong, Queen Mary Hospital, Hong Kong Special Administrative Region, People's Republic of China.

<sup>5</sup>The Skaggs Institute for Chemical Biology, The Scripps Research Institute, 10550 North Torrey Pines Road, La Jolla, CA 92037, USA.

### Abstract

Current flu vaccines provide only limited coverage against seasonal strains of influenza viruses. The identification of  $V_H1-69$  antibodies that broadly neutralize almost all influenza A group 1 viruses constituted a breakthrough in the influenza field. Here, we report the isolation and characterization of a human monoclonal antibody CR8020 with broad neutralizing activity against most group 2 viruses, including H3N2 and H7N7, which cause severe human infection. The crystal structure of Fab CR8020 with the 1968 pandemic H3 hemagglutinin (HA) reveals a highly conserved epitope in the HA stalk distinct from the epitope recognized by the  $V_H1-69$  group 1 antibodies. Thus, a cocktail of two antibodies may be sufficient to neutralize most influenza A subtypes and, hence, enable development of a universal flu vaccine and broad-spectrum antibody therapies.



# RELIABLE

## **BOBLETECTON** RAZOR<sup>®</sup> EX The Complete Field BioThreat Solution

0

www.RAZOREX.info





390 Wakara Way, Salt Lake City, UT, 84108, USA | 1-800-735-6544 | www.idahotech.com

#### Satellites could predict next cholera outbreak

Source: http://www.homelandsecuritynewswire.com/satellites-could-predict-next-cholera-outbreak

With cholera making an unlikely resurgence, catching countries like Haiti and Pakistan by surprise, public health officials are exploring the potential for new technology to help stem the spread of future outbreaks. The threat from cholera has been largely reduced, but the disease still poses a significant threat to many communities. Each year the disease affects three to five million people and claims more than 100,000 lives.

Most recently, cholera has begun to plague Haiti and Pakistan once more. The two countries had not seen a case of the disease in at least a century. Cholera causes extreme diarrhea and those infected face a 50 percent chance of death due to dehydration if they do not receive immediate treatment.

To combat cholera outbreaks, researchers believe that satellite images of the world's oceans could help forecast when a cholera outbreak is likely to strike.

#### Image: NASA

Shafiqul Islam, an environmental engineering and water diplomacy expert at Tufts University, and a team of scientists recently published a study in Water Resources Research that examines how large-scale environmental conditions can affect the initiation, transmission and propagation of cholera.

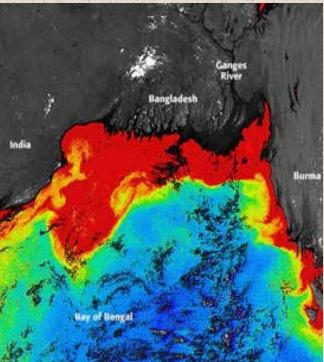
Islam's team examined data from cholera outbreaks in Bangladesh's Bengal Delta and found two annual peaks in cholera cases that occurred in the spring and fall. They found that the

first spike seemed result from "low flow," where long term drought conditions led to a mix of salt and fresh water off the Bangladeshi coast.

The bacteria that causes cholera thrives in these brackish conditions and can rapidly multiply in a few months. The bacteria's growth is particularly quick if there is an algae bloom as zooplankton feeding on algae carry the bacteria. Once in the water, cholera can easily enter a coastal city through seafood or drinking water.

In the Bengal Delta, after the initial outbreak has begun to wane, heavy rains and flooding

from the area's monsoon season revives and spreads cholera inland. Areas with poor water and sewer systems are often hit the hardest. Based on these findings, Islam believes that the conditions that lead to cholera outbreaks can be applied to areas beyond Bangladesh. Using satellites to identify the chlorophyll laden phytoplankton in the Earth's oceans, which zooplankton that carry the cholera bacteria feed on, researchers can develop prediction models that can forecast cholera outbreaks as far as two to three months in advance. "If you want to make predictions, three days or even three weeks in advance is not enough," Islam said. "You need at least two to three months in order to warn the public and allow



professionals enough time to get ready." "If you can use this information to make a prediction, then you can mobilize the necessary resources," he said.

As evidence Islam points to Haiti, which suffered a cholera outbreak following the devastating earthquake that struck the country in January 2010. More than 6 percent of those initially infected in Haiti eventually died from the disease. In contrast, only 0.1 percent of victims die in Bangladesh.

Islam says that if Haiti had a few months warning to prepare, the effect of the epidemic.

would have been far less severe as the effects of the disease can be mitigated with a simple solution of clean water with some sugar and salt.

Islam added that satellite monitoring will become even more crucial in the future as

#### Concerns over third outbreak of AIDS in Iran

Source: http://www.terrorism-info.org.il/site/home/default.asp

Dr. Abbas Sedaqat, the head of the AIDS Department of the Health Ministry, issued a warning about a third outbreak of AIDS in Iran, primarily among women and young people. Sedagat noted an increase in the number of people who have contracted the disease through unprotected sex, as well as in the rate of infection among women. He reported that a third strategic program for combating AIDS will soon be approved by the Supreme Council for Health and Nutrition Safety. The program emphasizes fighting the spread of AIDS through unprotected sex and inappropriate use of psychotropic substances, given the change in the dynamics of AIDS transmission in Iran in recent years. The program also includes efforts to continue fighting the spread of the disease through drug use, particularly among convicts, building on the earlier success of the second anti-AIDS program in dealing with the phenomenon.

Sedaqat commended the increased cooperation between the Health Ministry and Iran Broadcasting in the fight against AIDS, expressing his hope that the Education Ministry



will also take a serious part in the anti-AIDS program (Aftab, July 24).

Dr. Abbas Sedaqat visiting the Behavioral Diseases Consultation Center in south Tehran (from the website of the Tehran University of Medical Sciences) climate change models project increased drought and more severe flooding. "If these models are correct, then cholera will get more intense," he said.

Official data released by the Iranian Health Ministry put the number of AIDS cases in Iran at 21 thousand (as at May 2010), 92.6 percent of them men and 7.4 percent women. Estimates made by international health organizations are considerably higher, ranging between 60 and 100 thousand. Health Ministry figures show that nearly 70 percent of AIDS sufferers contracted the disease through contaminated needles, some 9 percent due to unprotected sex, 1.2 percent from infected blood transfusions, and 0.6 percent as a result of mother-to-child HIV transmission. The infection cause was not diagnosed in 20 percent of cases.

The Health Ministry figures support Iranian health experts' assessment that in recent years there has been a change in the transmission dynamics of AIDS in Iran, and that unlike in the past, most newly-discovered cases of AIDS have to do with unprotected sex rather than the use of contaminated needles by drug addicts or infected blood transfusions.

The first outbreak of the disease in Iran took place in 1986, when a number of patients received infected blood transfusions imported to Iran. The second outbreak took place in 1995 and mostly affected drug addicts. In recent years Iranian authorities have become more aware of the disease, recognizing that, even in Iran, dangerous sexual behavior is a considerable risk factor for AIDS infection.

While there are now several dozen safe sex counseling centers operating in Iran, Iow AIDS awareness means that they remain largely unknown to much of the population. Dr. Hamid Reza Sha'eri, the president of Iran's AIDS Association, has recently called for more comprehensive sex education in schools and universities to limit the spread of the disease through sex. He said that as long as young Iranians can't look up information on AIDS on the internet, as it is one of the terms filtered by the authorities, they cannot be expected to

Agency, July 21).

#### Global Bioterrorism Threat Analyzed For World Animal Health Office

Source: http://www.medicalnewstoday.com/releases/231757.php

Around the globe, many nations are realizing that the potential for bioterrorism isn't just about the U.S., officials say. And because an intentional introduction of bacteria, a virus or a toxin could happen anywhere, the World Organization for Animal Health is issuing a paper aimed at prevention. "Any emerging country that is beginning to think about maintaining international trade needs to be aware of the potential for bioterrorism," said Dr. Neville Clarke, special assistant to the Texas A&M University System's vice chancellor of agriculture. Clarke is lead author of "Bioterrorism: intentional introduction of animal disease," which appears in the animal health organization's journal Scientific and Technical Review this month.

#### Preventing bioterrorism worldwide

Around the globe, many nations are realizing that the potential for bioterrorism isn't just about the U.S., officials say. First off, bioterrorism is not new. The intentional introduction of animal disease dates to the Middle Ages when "diseased carcasses and bodies were catapulted over enemy walls in attempts to induce sickness in humans or animals," Clarke wrote with co-author Jennifer L. Rinderknecht, Texas AgriLife Research assistant. Throughout time, similar practices ensued until 1975, when more than 160 countries at the Biological and Toxic Weapons Convention agreed to prohibit biological warfare programs, the article noted. But, the authors say, evidence around the world indicates that the "development of biological agents continues in some countries." Clarke said that those farthest away from being prepared are the developing nations such as in Sub-Saharan Africa and Indonesia. He said the article would be helpful for nations that are wanting to protect their markets as they grow globally. The article discusses potential perpetrators and their methods, priority diseases, modern biology, trade and regulatory restraints as listed by the World Organization for Animal Health, which is headquartered in Paris and known as OIE for Office International des Epizooties. Clarke pointed to the live animal and fresh meat restrictions on imports from Brazil that are in place because there are still pockets of Foot-and-Mouth Disease in that South American country. "That impairs their ability to export to the U.S.," he said. "Trade restriction is one of the most important underlying issues that face countries. That makes bioterrorism everyone's business." While the article deals specifically with intentional introductions. Clarke said the "clean up and control is same" for either type event. "The only difference is in attribution," he said. "If an act is intentional, then the focus goes to finding out who did it."

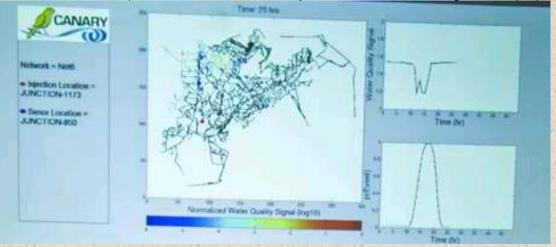
## Protecting water utilities from terrorist attacks and contaminants

Source:http://www.homelandsecuritynewswire.com/protecting-water-utilities-terrorist-attacks-and-contaminants

In 1993, a cryptosporidiosis outbreak in Milwaukee contaminated the city's water supplies, hastened the deaths of dozens of citizens, made more than 400,000 residents ill, and cost more than \$96 million in medical expenses and lost productivity; Sandia's CANARY software protects water utilities from terrorist attacks and contaminants Americans are used to drinking from the kitchen tap without fear of harm, even though water utilities might be vulnerable to terrorist attacks or natural contaminants.



Now, thanks to CANARY Event Detection Software — an open-source software "If you don't have a detection system, the way you find out about these things is when people



developed by Sandia National Laboratories in partnership with the Environmental Protection Agency (EPA) — public water systems can be protected through enhanced detection of such threats.

"People are excited about it because it's free and because we've shown that it works really well. We would love to have more utilities using it," said Regan Murray, acting associate division director of the EPA's Water Infrastructure Protection Division at the National Homeland Security Research Center.

A Sandia Lab release reports that the software tells utility operators within minutes whether something is wrong with their water, giving them time to warn and protect the public. It is also improving water quality by giving utility managers more comprehensive real-time data about changes in their water.

CANARY is being used in Cincinnati and Singapore, and Philadelphia is testing the software system. A number of other U.S. utilities also are evaluating CANARY for future use.

Sean McKenna, the Sandia researcher who led the team that developed CANARY, said people began to pay attention to the security of the U.S. water systems after 9/11.

McKenna and Murray said CANARY could have lessened the impact of the U.S. largest public water contamination. In 1993, a cryptosporidiosis outbreak in Milwaukee hastened the deaths of dozens of citizens, made more than 400,000 residents ill and cost more than \$96 million in medical expenses and lost productivity, according to reports about the tragedy. get sick," Murray said.

The release notes that Sandia, a national security laboratory, had worked on water security before the 9/11 attacks. So when the EPA was looking for help early in the last decade to better monitor water utilities, they contacted Sandia.

A Sandia-developed, risk-assessment methodology for water focused on physical security of the utility infrastructure, but did not address detection and assessment of the impact of contamination within the water itself. CANARY was designed to meet that need for better assessment, McKenna said.

CANARY, which runs on a desktop computer, can be customized for individual water utilities, working with existing sensors and software, McKenna said.

While some utilities monitor their water using real-time sensors, many still send operators out once a week to take samples, said David Hart, the lead Sandia software developer for CANARY.

Compared to weekly samples, CANARY works at lightning speed.

"From the start of an event — when a contaminant reaches the first sensor — to an event alarm would be 20-40 minutes, depending on how the utility has CANARY configured," McKenna said.

The challenge for any contamination detection system is reducing the number of false alarms and making data meaningful amidst a "noisy" background of information caused by the environment and the utility infrastructure itself. CANARY researchers used specially designed numerical algorithms to analyze data coming from multiple sensors and differentiate between

natural variability and unusual patterns that indicate a problem. For example, the Multivariate-Nearest Neighbor algorithm groups data into clusters based on time and distance, explained Kate Klise, a numerical analyst at Sandia. When new data is received, CANARY decides whether it is close enough to a known cluster to be considered normal or whether it's far enough away to be deemed anomalous. In the latter case, CANARY alerts the utility operator, Klise said.

The computer program uses a moving 1.5- to 2-day window of past data to detect abnormal events by comparing predicted water characteristics with current observations. But a single outlier won't trigger the alarm, which helps to avoid costly and inefficient false alarms. CANARY aggregates information over multiple 2- to 5-minute time steps to build evidence that water quality has undergone a significant change, McKenna said.

"We've taken techniques from different fields and put those together in a way they haven't been put together before; certainly the application of those techniques to water quality monitoring hasn't been done before," McKenna said.

CANARY also provides information about gradual changes in the water, McKenna said.

One unintended benefit of the software is that when utility operators better understood the data being sent by their sensors, they could

Water purification unit generates its own energy

Source: http://www.siemens.com/entry/cc/en/

A new biological water purification facility developed by Siemens generates enough methane gas to power its own operations. It also produces much less sludge than conventional systems. The pilot facility for this process, which is located at a site run by Singapore's Public Utilities Board, has been operating in an energy- neutral manner since June 2010. Now, the city state is building a much larger pilot facility — one that will process 300 times more effluent than its predecessor, or about as much sewage water as is produced by around 1,000 people.

Siemens says that a typical urban biological water purification facility accommodates water from 10,000 to 100,000 residents. Today an aerobic (ventilated) process is used in which bacteria break down impurities in water by

make changes to the management of the water systems to improve its overall quality, McKenna said.

"What we found from utilities we work with is that a better managed system is more secure, and a more secure system is better managed," McKenna said.

Harry Seah, director of the Technology and Water Quality Office at the Public Utilities Board (PUB), Singapore's national water authority, wrote in a letter supporting CANARY that the software provided a "quantum leap" in the utility's practice.

In the past, Seah wrote, the utility depended on preset limits of three water characteristics to determine water quality.

"With the implementation of CANARY, relative changes in the patterns of these three parameters can be used to uncover water quality events, even if each individual parameter lies within the alarm limits," Seah wrote. "This dramatically improves PUB's ability to respond to water quality changes, and allows PUB to arrest poor quality water before [it reaches] the consumers."

As more versions of the software are installed at water utilities, researchers are working on new application areas for CANARY, such as computer network traffic logs and geophysical log analysis used by petroleum drillers to analyze rocks at different depths.

digesting them and converting them into new bacterial substances. This produced bacteria flakes filled with impurities - forming sludge that is then separated and either deposited in landfills or burned. The organic impurities, however, contain ten times more energy than needed to do the cleaning itself. They can therefore be used to generate methane, which could be used in gas-fired power plants or combined heat-and-power plants. Sludge concentrations in municipal sewage systems, are low however. too to produce methane economically.

With this in mind, development engineers from Siemens Water Technologies have developed a technology for charging bacteria flakes with organic impurities for an extremely short time during ventilation. As a result, bacterial.

reproduction is minimized. After most of the water is separated, the bacteria ferment the impurities into methane in an anaerobic process step. After two aerobic steps and one anaerobic step, the sludge has been broken down so that the least possible amount of sludge remains and the largest possible amount of methane is available.

The pilot facility now in operation cleans around half a cubic meter of wastewater per day. A conventional water treatment plant requires a little less than 0.25 kilowatt-hours of energy to do this, so the pilot unit needs to generate roughly that amount of energy in the form of methane. A bigger facility could be run in an energy- neutral manner. Market launch of the technology is scheduled for 2012.

#### Lung damage found in Iraq, Afghanistan veterans

Source:http://www.msnbc.msn.com/id/43832153/ns/health-health\_care/t/lung-damage-found-iragafghanistan-veterans/

Shortness of breath and reduced fitness among some military veterans returning from Irag and Afghanistan may be caused by lung damage from smoke, sandstorms and toxins, a new study suggests.

Researchers who performed lung biopsies on 38 veterans with unexplained breathing problems found a form of tissue damage - called constrictive bronchiolitis - that is rare in young adults and doesn't show up in standard tests.

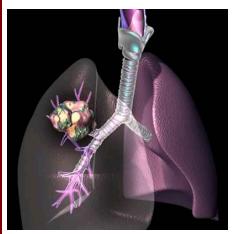
In all but one case, a "lacy black pigment" also coated the delicate lung surfaces.

Dr. Robert Miller of the Vanderbilt University Medical Center said the cases, which he has been gathering for years, are apparently caused by exposure to airborne toxins during deployment.

"We believe they're deployed to some pretty toxic environments. They're exposed to burning solid waste, burning human waste (particularly in Iraq), and consistently exposed to fine particulate matter that's easily inhaled deep into the lungs at a level that's above what's desirable," Miller told Reuters Health in a telephone interview.

Dust storms and combat smoke may also be a factor. Previous research has suggested that service in the Middle East increases the risk of breathing problems.

Among the volunteers examined in the new study — primarily members of the 101st Airborne Division in Fort Campbell, Kentucky — most had long-term exposure to a sulfur-mine fire that burned for 30 days in



2003 near Mosul, Irag, Miller and his colleagues write in the New England Journal of Medicine. In all, Miller's team tested 80 previously fit soldiers who no longer met the Army's physical fitness standards.

Forty-nine agreed to undergo an invasive lung biopsy procedure after chest X-rays and other standard tests did not reveal the cause of their problems. All 49 had tissue samples that were judged to be abnormal. The diagnosis of **constrictive bronchiolitis** — a thickening of the walls of the smallest lung passages, the bronchioles — was made in 38 cases (35 men and three women). Seven were active smokers and six were former smokers.

The condition doesn't show up in standard tests of breathing capacity, according to Miller, because the soldiers probably

begin their deployment with so much extra lung function — perhaps 115 percent of normal — that their damaged lungs still perform in a range that's considered normal for non-athletes.

But when compared to a sample of 69 unaffected active duty soldiers, the soldiers Miller examined had weaker lung function — averaging 87 percent in a test of how much of the air in their lungs they could expel in one second, compared with 99 percent in the control group.

Of the 38 diagnosed with constrictive bronchiolitis, half left the service with a disability rating and 58 percent reported having shortness of breath after climbing one flight of stairs. "My concern is there are too many people whose symptoms are being dismissed because their X-rays and pulmonary function

tests are normal or near normal," he said. "My personal agenda is to get these guys seriously evaluated."

The lung biopsies performed in Miller's study require more than a month of recovery time and cost \$50,000 to \$60,000. And there is no treatment for the soldiers' condition, Miller said. "It's a fixed scarring of the small airway. It's not irritation, inflammation or swelling."

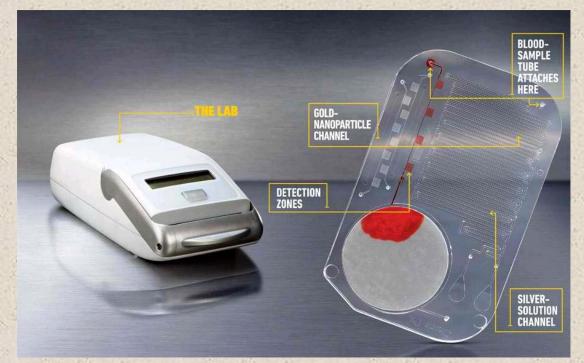
Nonetheless, Miller wants doctors to keep his findings in mind. "If you have someone with unexplained shortness of breath who served in the Middle East, you have to consider constrictive bronchiolitis as a possible cause, even if X-rays and pulmonary function tests are normal," he said.

Earlier results with a smaller number of cases were reported in 2008 at a meeting of the American Thoracic Society. "Now we feel we have enough patients to say, 'This is real," Miller said.

## Engineering Innovative Hand-Held Lab-On-A-Chip Could Streamline Blood Testing Worldwide

Source: http://www.sciencedaily.com/releases/2011/07/110731170009.htm

Samuel K. Sia, assistant professor of biomedical engineering at Columbia Engineering, has developed an innovative strategy for an integrated microfluidic-based diagnostic device -- in effect, a lab-on-a-chip -that can perform complex laboratory assays, and do so with such simplicity that these tests can be carried out in the most remote regions of the world. In a paper published in Nature Medicine online on July 31, Sia presents the Sia and his team performed testing in Rwanda over the last four years in partnership with Columbia's Mailman School of Public Health and three local non-government organizations in Rwanda, targeting hundreds of patients. His device, known as mChip (mobile microfluidic chip), requires only a tiny finger prick of blood, effective even for a newborn, and gives -- in less than 15 minutes -- quantitative objective results that are not subject to user



first published field results on how microfluidics -- the manipulation of small amounts of fluids -and nanoparticles can be successfully leveraged to produce a functional low-cost diagnostic device in extreme resource-limited settings. interpretation. This new technology significantly reduces the time between testing patients and treating them, providing medical workers in the field results that are much easier to read at a much lower cost. New low-cost diagnostics like the mChip could revolutionize medical care around the world.

"We have engineered a disposable credit card-sized device that can produce blood-

diagnostic based results in minutes," said Sia. "The idea is to make a large class of diagnostic tests accessible to patients in any setting in the world, rather than forcing them to go to a clinic to draw blood and then wait days for their results." Sia's lab at Columbia Engineering has developed the mChip devices in collaboration with Claros Diagnostics Inc., a venture capitalbacked startup that Sia



co-founded in 2004. (The company has recently been named by MIT's Technology Review as one of the 50 most innovative companies in the world.) The microchip inside the device is formed through injection molding and holds miniature forms of test tubes and chemicals; the cost of the chip is about \$1 and the entire instrument about \$100.

Sia hopes to use the mChip to help pregnant women in Rwanda who, while they may be suffering from AIDS and sexually transmitted diseases, cannot be diagnosed with any certainty because they live too far away from a clinic or hospital with a lab. "Diagnosis of infectious diseases is very important in the developing world," said Sia. "When you're in these villages, you may have the drugs for many STDs, but you don't know who to give treatments to, so the challenge really comes

down to diagnostics." A version of the mChip that tests for prostate cancer has also been developed by Claros Diagnostics and was approved in 2010 for use in Europe.

Sia's work also focuses on developing new high-resolution tools to control the extracellular environments around cells, in order to study how they interact to form human tissues

and organs. His lab uses techniques from a number of different fields, including biochemistry, molecular biology, microfabrication, microfluidics, materials chemistry, and cell and tissue biology.

The mChip project has been supported by funding from the National Institutes of Health and Wallace Coulter Foundation.

#### Portable detector can ID anthrax in one hour

Source: http://www.news.cornell.edu/stories/July11/AnthraxDetector.html

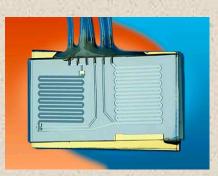
Researchers have developed a portable device can detect the presence of the anthrax



bacterium in about one hour from a sample

containing as few as forty microscopic spores; the basic design, which is small enough to fit in the overhead compartment of an airplane, potentially could be tailored to detect countless other pathogens, such as salmonella, or be used in the field for DNA forensics

A portable device can detect the presence of the anthrax bacterium in about one hour from a sample containing as few as forty microscopic spores, report Cornell and University of Albany researchers who invented it. The device could provide early detection in the case of an anthrax attack, saving many lives.



This photograph shows the device's microfluidic chip, which measures approximately one centimeter by 3 centimeters and integrates sample purification and real-time PCR analysis chambers.

The basic design, which is small enough to fit in the overhead compartment of an airplane, potentially could be tailored to detect countless other pathogens, such as salmonella, or be used in the field for DNA forensics.

"It was built with the notion of being portable," said Carl Batt, Liberty Hyde Bailey Professor in the Department of Food Science at Cornell and a co-author of the paper published in July in the International Journal of Biomedical Nanoscience and Nanotechnology. Nathaniel Cady, Ph.D. '06, a nano scale engineer at the University of Albany, is the paper's lead author. A Cornell University release reports that the detector, seven years in the making, requires that a sample be inserted into the device. From there the machine automatically recovers cells, collects and purifies DNA and then conducts real-time polymerase chain reactions (PCR) to identify if anthrax is present. PCR can amplify extremely small amounts of DNA and is a wellestablished platform for rapidly detecting biological material.

The researchers began by acquiring what amounts to a small suitcase-sized plastic box with the notion that, "whatever we do, it has to fit in here. It was a line in the sand, an engineering challenge where everything had to fit in the box," Batt said.

The shape of a heavily reinforced suitcase, the device is complete with pumps, heating and cooling elements, and optical and computational circuitry.

By tailoring different assays to the portable real-time PCR platform, the device could be used for a variety of applications in addition to anthrax detection, such as at a crime scene for forensics. For example, if detectives were to find a sample they believe belongs to a



perpetrator, they might use such a device to rapidly and broadly determine the gender or eye color of the suspect.

The researchers are currently working to develop new strategies for pumping fluids in the device, a system that now occupies the majority of the space and most of the power. Novel pumping systems based on silicon processing are being created, which could allow engineers to fabricate most of the components of the system on a single chip.

The research was funded by KRAFT foods, the U. S. Department of Agriculture, National Institute of Justice, and the Food and Drug Administration.

#### India to open Bio Safety Level-4 lab

Source: http://www.expressindia.com/latest-news/niv-builds-hitech-virus-lab/825947/

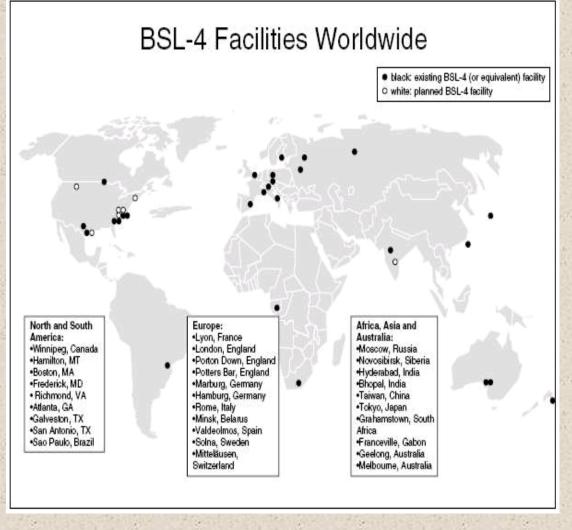
India's National Institute of Virology is in the final stages of completing a Bio Safety Level-4 laboratory on its Pashan campus in order to study dangerous diseases that could be used in a bioterrorist attack.

The levels of containment range from BSL-1 to BSL-4. BSL-4 labs are capable of safely containing the some of the world's most deadly

agents for study, according to ExpressIndia.com.

The laboratory at NIV's microbial containment complex at Pashan is expected to be fully functional by November and will hold an assortment of diseases, including ebola, anthrax, lassa and smallpox. NIV has imported a total of 12 biosafety suits with dedicated

oxygen lines from Italy. Seven NIV scientists are scheduled to return from rigorous training in the United States that taught them how to safely operate a BSL-4 lab. "This laboratory will not just be the first in the country but the only one in entire South East Asia," NIV director Dr. core group will be responsible for training other engineers to run various BSL-3 facilities around the country. "Virologists are always the first responders in case of any outbreak. Viruses can be used as a bioterrorism agent and the BSL-4 laboratory has been designed in such a



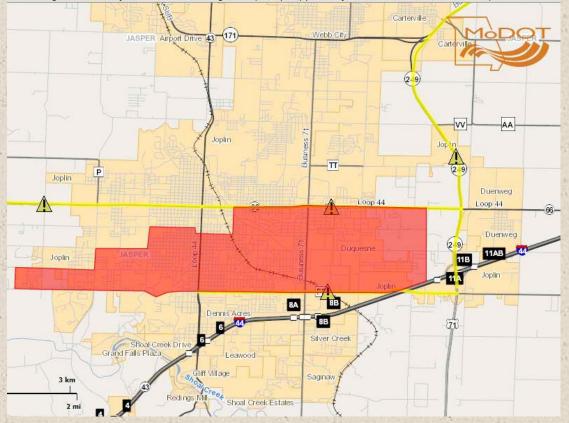
A. C. Mishra said, ExpressIndia.com reports. The Indian Council of Medical Research has, according to Mishra, set up a special group of engineers who will manage the facility. The way that it can detect the virus and counter any bio-terror attack," Mishra said, ExpressIndia.com reports.

#### Five Joplin survivors die of mysterious fungal infection

Source: http://www.homelandsecuritynewswire.com/five-joplin-survivors-die-mysterious-fungal-infection

After being hit by a massive tornado that destroyed much of Joplin, Missouri, several residents suffered from a fungal infection that killed five people.





Following the 22 May twister that ravaged Joplin (map), many residents suffered from splinters, cuts,

and other minor injuries that eventually resulted in a rare fungus infection. The Centers for Disease Control and Prevention (CDC) is still investigating the causes of the infection, but believe that thirteen people contracted the mucormycetes-borne illness.

The CDC has said that it most often sees this type of infection after natural disasters like hurricanes, but has yet to see it occur after a tornado. The fungus that infected the injured is typically found in soil, decaying wood, and other organic matter.

On the CDC's blog, Molly Gayden, explains, "When people sustain massive traumatic injuries, it puts so much stress on the body that it becomes difficult to fight off infections. This paves the way for germs also called pathogens—which can infect humans when the body's natural defenses are weakened. Cuts, scrapes, burns, and even a splinter can allow pathogens to enter the body through the skin."

She continues, "The events that occurred in Joplin created the perfect environment for exposure to these pathogens, and some injured survivors began showing signs of an unusual wound infection."

The CDC's investigation found that none of the fungal infection victims sustained their injuries, which Rob Chappel, the Jasper County coroner, said is a relief. "It's about what we expected," he said. Of the thirteen infected, each had an average of four wounds. Ten patients required intensive care and of those five died. The ages of the infected ranged widely from thirteen to seventy-six years old.

#### Gold nanoparticles help to diagnose flu in minutes

Source: http://www.homelandsecuritynewswire.com/gold-nanoparticles-help-diagnose-flu-minutes

Arriving at a rapid and accurate diagnosis is critical during flu outbreaks, but until now, physicians and public health officials have had to choose between a highly accurate yet timeconsuming test or a rapid but error-prone test. A new detection method developed at the University of Georgia and detailed in the August edition of the journal Analyst, however, offers the best of both worlds. By coating gold nanoparticles with antibodies that bind to specific strains of the flu virus and then measuring how the particles scatter laser light, the technology can detect influenza in minutes at a cost of only a fraction of a penny per exam.



"We've known for a long time that you can use antibodies to capture viruses and that nanoparticles have different traits based on



their size," said study co-author Ralph Tripp, Georgia Research Alliance Eminent Scholar in Vaccine Development in the UGA College of Veterinary Medicine. "What we've done is combine the two to create a diagnostic test that is rapid and highly sensitive."

A University of Georgia release reports that Tripp and co-author Jeremy Driskell, working in the UGA Nanoscale Science and Engineering Center, linked immune system proteins known as antibodies with gold nanoparticles. The gold nanoparticle-antibody complex aggregates with any virus present in a sample, and a commercially available device measures the intensity with which the solution scatters light. Driskell explained that gold nanoparticles, which are roughly a tenth of the width of a human hair, are extremely efficient at scattering light. Biological molecules such as viruses, on the other hand, are intrinsically weak light scatterers. The clustering of the virus with the gold nanoparticles causes the scattered light to fluctuate in a predictable and measurable pattern. "The test is something that can be done literally at the point-of-care," said Driskell, who worked on the technology as an assistant research scientist in Tripp's lab. "You take your sample, put it in the instrument, hit a button and get your results." Gold is often thought of as a costly metal, but the new diagnostic test uses such a small amount less than what would fit on the head of the pin - that the cost is one-hundredth of a cent per test. The researchers noted that the current

standard for definitively diagnosing flu is a test known as PCR, for polymerase chain reaction. PCR can only be done in highly specialized labs and requires that specially trained personnel incubate the sample for three days, extract the DNA and then amplify it many times. The entire process, from sample collection to result, takes about a week and is too costly for routine testing.

The alternative is a rapid test known as a lateral flow assay. The test is cost effective and can be used at the point-of-care, but it can't identify the specific viral strain. It also misses up to 50 percent of infections and is especially error-prone when small quantities of virus are present, Driskell added.

The release notes that by overcoming the weaknesses of existing diagnostic tests, the researchers hope to enable more timely diagnoses that can help halt the spread of flu by accurately identifying infections and allowing physicians to begin treatment early, when antiviral drugs, such as Tamiflu, are most effective.

Tripp and Driskell are planning to compare the new diagnostic test with another that Tripp and his colleagues developed that measures the change in frequency of a laser as it scatters off viral DNA or RNA. Tripp also is working to adapt the new technique so that poultry producers can rapidly detect levels of salmonella in bath water during processing. Poultry is the largest agricultural industry in Georgia, he pointed out, so the technology could have a significant impact on the state's economy. "This test offers tremendous advantages for influenza, but we really don't want to stop there," Tripp said.

"Theoretically, all we have to do is exchange our anti-influenza antibody out with an antibody for another pathogen that may be of interest, and we can do the same test for any number of infectious agents."

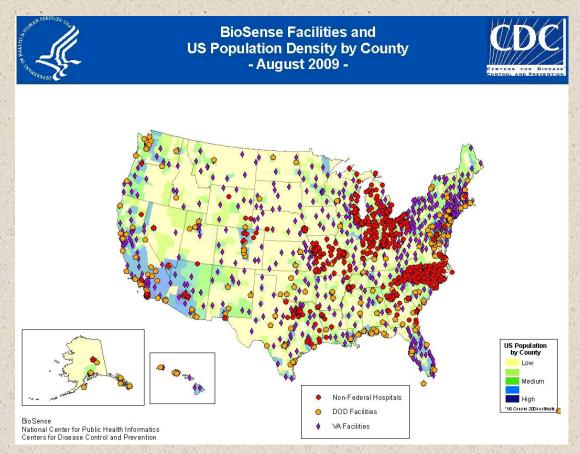
#### CDC moves disease surveillance system to the cloud

#### By William Jackson

Source:http://www.silobreaker.com/cdc-moves-disease-surveillance-system-to-the-cloud-5\_22647424 73219702886

The BioSense program, created by the Centers for Disease Control and Prevention in the wake of the 2001 terrorist attacks, is remaking itself to provide a cloud-based collaboration platform for federal, state and local health officials. "It essentially is for the rapid, automated collection and dissemination of data," said Dr.

Taha Kass-Hout, BioSense program manager at CDC's Public Health Surveillance Program Office. "The original mandate was to look at security firm. Securing data, managing identities and controlling access are different in the cloud but not necessarily more difficult. In



bioterrorism incidents," but that is being expanded to include all human health-related conditions. Making a broader range of information available will help public health officials spot, predict, prepare for and respond to outbreaks and events. In the course of this change, CDC has decided that maintaining a centralized infrastructure for gathering and using data no longer makes sense. Details of the new model still are being worked out, but it was decided that the program was an ideal candidate for deployment in the cloud. "It supports the business model," Kass-Hout said. "And you end up saving quite a bit." That means money can be shifted from IT acquisition and maintenance to lowering the cost of participation for state and local offices. However, the cloud also comes with its own set of security concerns as resources, including hardware, software and data, are moved to a third-party environment.

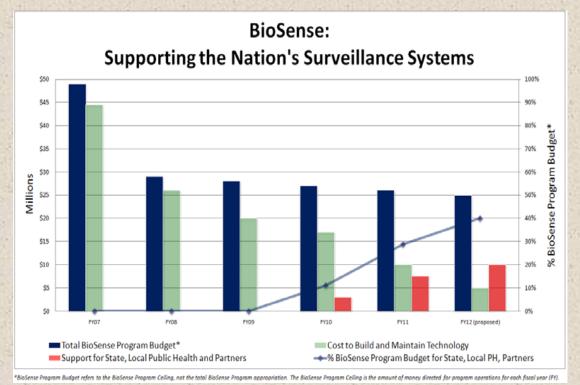
There is a saying, "you can outsource security, but you can't outsource responsibility," said Jon Geater, director of technical strategy at Thales e-Security, an electronics and systems theory, the economy of scale and centralized management in a cloud environment could make best security practices such as real-time monitoring, patch management and configuration management easier — if the service provider is doing these things, that is. Not all of them are. "The cloud is a marketplace," Geater said. "Some people will be better than others."

#### **BioSense security**

Security and access control are among the criteria that will be considered when the BioSense community makes its decision on a cloud provider later this year. Both the customer and the provider will have to work together to ensure that the appropriate levels of security are maintained to safeguard public but sensitive health data. "There is a responsibility for the organization to maintain a level of security" for the data it owns, Geater said. But the service provider also must provide appropriate information and tools to the customer. "It's a shared thing." BioSense was authorized in 2002 and established in 2003.

provide early detection and rapid assessment of illnesses and outbreaks that could be an indication of a terrorist attack. That mission is not being abandoned, but the information is being used to improve public health situational awareness by allowing threats to be detected earlier, to support public health practice, and to allow the collaboration of public health officials in different parts of the country that are facing similar situations or have information that is needed by someone else. Recent uses of the evolving BioSense program include monitoring health problems related to the Gulf oil spill in Alabama, Florida, Louisiana, Mississippi and Texas and tracking possible rabies infections and flu-like illnesses. BioSense data currently is being collected from local hospitals, health departments, laboratories and the pharmaceutical industry, as well as from federal health care providers, including the Defense and Veterans Affairs departments. "The data comes in various forms, but primarily in some electronic form," Kass-Hout said. DOD, VA and some labs have automated systems that pass the information to CDC.

Participants will have more control over and access to their data and will be able to form ad hoc teams to collaborate in developing products needed at the time. The collection system also will be standardized so that data will come to CDC from public health departments rather than directly from local hospitals. "In the new model, we are going to embrace the health department," Kass-Hout said. "They own that relationship with the hospital," and it is important that the local departments see the data as it is being passed on. The platform also will provide tools to allow state and local users to slice and dice the data as they need to. The redesign process began about two years ago, the cloud approach was selected about a year ago and discussions now are under way with service providers. Requirements for the provider will include compliance with basic Federal Information Security Management Act requirements, additional security as required to adequately protect data, and a large enough customer base to ensure the service provider will be around for a while. RTI International, a



#### Socialized health data

In the past, CDC has gathered data centrally and produced reports and other products for BioSense participants. The new model will provide a user-centric environment rich with social features for sharing information. research institute based in Research Triangle Park, N.C., has been brought in to help in the redesign while the Association of State and Territorial Health Officials is the lead representative for state and local offices. Design prototypes for the system. were developed in collaboration with stakeholder

from 22 guiding principles and still are evolving. The idea is to allow collaboration between

#### New BioSense Approach

In FY 2010, CDC started redesigning the BioSense program based on input and guidance from our local, state, and federal partners. The goal of the redesign effort is to be able to provide nationwide and regional situational awareness for all-hazard health-related threats (beyond bioterrorism) and to support national, state, and local responses to those threats. This support was achieved through improved internal contract management, with savings being applied directly to increase funding to support state and local health departments for syndromic surveillance efforts. Through these savings the BioSense program awarded funding to 16 states, 4 cities and Washington D.C.. CDC plans to continue to examine the stakeholder requirements and needs assessment, determine limitations of participating sites, assess Meaningful Use readiness, and work collaboratively with external partners on how best to meet the needs of state and local health departments.

#### **New BioSense Activities**

By integrating local and state-level information, CDC will provide a timely and cohesive picture at the regional (i.e., multistate) and national levels and improve BioSense's utility. The key components of the BioSense program redesign:

- Help build health monitoring infrastructure and workforce capacity where needed at the state, local, tribal, and territorial levels
- Facilitate the interchange of information that can be used to coordinate responses and monitor health-related outcomes routinely and during an event
- Retain the original purpose of BioSense to detect and characterize events (or health-related threats) early by building on state and local health departments systems and programs
- Expand the utility of BioSense data to multi-use [and all-hazard] beyond early event detection and to contribute information for:
- public health situational awareness
- routine public health practice
- improved health outcomes and public health
- Improve the ability to detect emergency healthrelated threats by supporting the enhancement of systems to signal alerts for potential problems
- Increasing local and state jurisdictions
   participation in BioSense
- Advances in science and technology

peers with the ability to download and save reports in a variety of formats. Kass-Hout said the new platform is expected to be up and running by November.

#### **Trust chain stretched**

Although the technology for managing identity and controlling access does not change significantly in a cloud environment, the chain of trust becomes more stretched out, Geater said. Without infrastructure being under the control of a single IT team, "things that were implicitly trusted now have to be explicitly trusted." The business model for security and access control also changes. Because the customer suffers the primary loss in the event of a breach, security becomes a secondary business consideration for the provider. "The cost/benefit calculation is different, so the investment decision is very different," Geater said. The result is caveat emptor - it is up to the customer to ensure that the service provider provides adequate controls and can demonstrate the controls for an auditor. Small organizations that cannot afford a dedicated IT team will often will be better off in a cloud environment, because a capable provider will offer better security and better identity management than the small organization can manage on its own, Geater said. But a larger organization with higher requirements will have to look much more carefully to find a provider that meets its expectations. Tools used for authentication and access control do not change in the cloud. Choice will depend on the level of assurance required, which in turn depends on the sensitivity of the information being protected and the likely impact of a breach. But although the default user ID and password combination will work in the cloud, Geater is not a fan.

"Passwords are easily guessed or stolen and they are hard to revoke," he said. And if passwords are being sent via the Internet to a cloud, "they are going to be stolen. No question."

#### PKI fan base

A flexible — but complex — alternative to passwords is public-key infrastructure, which uses cryptographic keys for authentication and protection of data. "Here at Adobe, we have been big fans of PKI since the late '90s, when we first began incorporating it into our documents," said John Landwehr, senior director of enterprise security solutions at Adobe Systems. When embedded in documents, PKI can be used to digitally sign and verify a document, as well as authentication

users through a variety of ID management sources, including Active Directory and LDAP. Although PKI has been around for guite a while, its drawback is complexity. It is a scheme that uses mathematically related cryptographic key pairs, one public and one private, to encrypt and decrypt data for a wide variety of uses. The chore of managing these keys has also given it the name painful key infrastructure, Landwehr said. "But there have been advances to ease the pain both of deployment and use." Much of the advance has come in government, in the form of the military's Common Access Card (CAC) and its civilian counterpart, the Personal Identity Verification (PIV) card, both of which incorporate keys for PKI. Tying the keys to ID cards as well as the introduction of an infrastructure that includes card readers and authorities for verifying keys are helping to make PKI a more versatile tool. One of the advantages of PKI is that it can be used not only to verify the identity of someone accessing online resources but also to authenticate the resources being accessed. This is an important consideration when using the Web to publish official public documents, as the Government Printing Office does. GPO uses digital signatures to verify that information in public documents being viewed such as legislation and public laws has not been changed, a step that can be handled by a Web browser without any effort on the part of the viewer.

#### **PKI for BioSense?**

PKI can take the process one step further in a system such as BioSense, which includes sensitive data and which goes beyond one-way publishing. PKI can verify that users are

accessing genuine data repositories and that the data has not been modified, and it also can be used to control access to that data contribution of new data. But despite advances in PKI, it remains largely a stovepipe environment with single-purpose certificates being used in closed populations, such as government employees. The ubiquity of CAC and PIV within government offers an opportunity to expand the use of PKI to new applications. "The next challenge we're going to watch is how to roll it out to more of the public," Landwehr said. The National Strategy for Trusted Identities in Cyberspace, a federal initiative to establish an "identity ecosystem" with user-friendly credentials that can be widely accepted online, could be a step in this direction. But to make credentials simple and useful, digital certificates issued by one provider would have to be accepted for a variety of uses, and this will require an infrastructure for federation that would allow verification across a variety of applications. Government has been in a leader in this area also with its Federal PKI Bridge, and the creation of standards for PIV Interoperability, which would allow the use of public digital certificates that could be accepted by government, also is a step in that direction. But the infrastructure is far from fully deployed, and "When challenges remain. properly implemented, we've seen technology like PKI bring not only cost savings but improve the privacy of the participants and the security of the transaction," Landwehr said. But the job of building out an infrastructure and managing creating a model for sharing the costs among users, "that's a tough one."

William Jackson is a senior writer for GCN and the author of the CyberEye column.

#### A natural food preservative kills food-borne bacteria

Source: http://www1.umn.edu/news/news-releases/2011/UR\_CONTENT\_349919.html

Salmonella and E. coli account for more than half of all food recalls in the United States; salmonella contributes to an estimated 28 percent of more than 3,000 U.S. deaths related to foodborne illness each year; researchers have discovered and received a patent for a naturally occurring **lantibiotic** -- a peptide produced by a harmless bacteria -- that could be added to food to kill harmful bacteria like salmonella, E. coli, and listeria.

Researchers at the University of Minnesota have discovered and received a patent for a naturally occurring lantibiotic — a peptide produced by a harmless bacteria — that could be added to food to kill harmful bacteria like salmonella, E. coli, and listeria.



The U of M lantibiotic is the first natural preservative found to kill gram-negative bacteria, typically the harmful kind. "It's aimed



at protecting foods from a broad range of bugs that cause disease," said Dan O'Sullivan, a professor of food science and nutrition in the university's College of Food, Agricultural and Natural Resource Sciences. "Of the natural preservatives, it has a broader umbrella of bugs that it can protect against."

A University of Minnesota release reports that the lantibiotic could be used to prevent harmful bacteria in meats, processed cheeses, egg and dairy products, canned foods, seafood, salad dressing, fermented beverages, and many other foods. In addition to food safety benefits, lantibiotics are easy to digest, nontoxic, do not induce allergies and are difficult for dangerous bacteria to develop resistance against.

O'Sullivan discovered the lantibiotic by chance, while researching the genome of bacteria. He then collaborated with Ju-Hoon Lee, a U of M graduate student, to continue the research. The U of M's Office for Technology Commercialization is currently seeking a licensee for the technology.

The release notes that in wake of the recent deadly salmonella outbreak, it is important for researchers to continue developing methods to protect foods from dangerous bacteria.

"Salmonella burden has increased more dramatically than any other foodborne illness," said Shaun Kennedy, director of the National Center for Food Protection and Defense. "The largest recall in 2010 for food contamination was eggs contaminated with salmonella."

Salmonella and E. coli, both gram-negative bacteria, account for more than half of all food recalls in the United States. According to the Centers for Disease Control and Prevention, salmonella contributes to an estimated 28 percent of more than 3,000 deaths related to foodborne illness each year.

#### Innovative biosensor for rapid virus field tests

Source: http://www.homelandsecuritynewswire.com/innovative-biosensor-rapid-virus-field-tests

Relying on a novel DNA-based bio-chemophysical conversion method, a new biodetection device is able to detect harmful

bacteria, such as Ε. coli. salmonella, and staphylococcus. on site, within thirty minutes; it can be adapted to cover such deadly viruses as SARS, H5N1 flu, and swine flu viruses; it can



also be designed to monitor possible biological attack from anthrax, smallpox, cholera, and more

Two researchers at the Hong Kong Polytechnic University - Professor Samuel Lo, Associate Head of the Department of Applied

> Biology and Chemical Technology, and Dr. Derek Or. Associate Professor of Department the of Electrical Engineering have jointly developed a Portable Real-time DNA< Biosensor.

The device is designed to perform speedy in situ DNA tests for biodefense and health surveillance areas suspected to be with pathogens and/or undesirable microbes.

www.cbrne-terrorism-newsletter.com

purposes

contaminated

in

A Hong Kong Polytechnic University release reports that unlike conventional laboratory tests that take at least one or two days, this handheld, battery-operated and fully automated biosensor is built upon a novel DNA-based biochemo-physical conversion method. It is able to detect harmful bacteria, such as E. coli, salmonella, and staphylococcus, on site, within thirty minutes. It can be adapted to cover such deadly viruses as SARS, H5N1 flu, and swine flu viruses. It can also be re-designed to monitor possible biological attack from anthrax, smallpox, and cholera etc.

Comprising a reaction chamber, an ultrasound core, and an electronics power board, the new biosensor can test for the presence of a specific pathogen in water and air samples by recognizing the existence of its DNA. When this pathogen is added to the reaction chamber, the further addition of both specific primer-linked thrombin and fibrinogen triggers an innovative molecular bio-chemical reaction. In the case of a DNA primer match, the enzyme will convert fibrinogen into a lump of visible gel that blocks the transmission of ultrasound signals through the reaction chamber. A drop in the ultrasound reading is then a strong indicator of the presence of the target pathogen in the sample.



This invention won a Gold Award at the 39th International Exhibition of Inventions in Geneva, Switzerland.

#### Medical silver bullet: New drug cures most viral infections

Source: http://web.mit.edu/newsoffice/2011/antiviral-0810.html

Researchers at MIT's Lincoln Lab have developed technology that may someday cure the common cold, influenza, and other ailments; the researchers tested their drug against fifteen viruses, and found it was effective against all of them — including rhinoviruses that cause the common cold, H1N1 influenza, a stomach virus, a polio virus, dengue fever, and several other types of hemorrhagic fever.

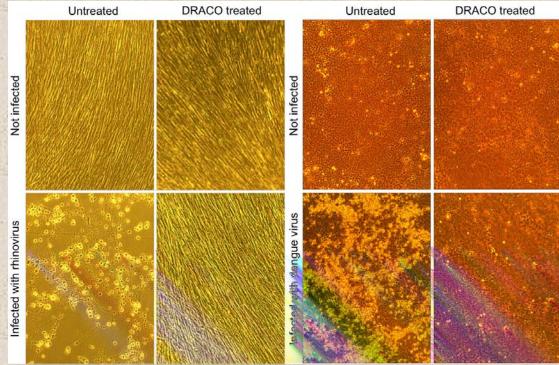
Most bacterial infections can be treated with antibiotics such as penicillin, discovered decades ago. Such drugs, however, are useless against viral infections, including

influenza, the common cold, and deadly hemorrhagic fevers such as Ebola.

An MIT release reports that now, in a development that could transform how viral infections are treated, a team of researchers at MIT's Lincoln Laboratory has designed a drug that can identify cells that have been infected by any type of virus, then kill those cells to terminate the infection. In a paper published 27 July in the journal Plos One, the researchers tested their drug against fifteen viruses, and found it was effective against all of them — including rhinoviruses that cause the common cold, H1N1 influenza, a stomach virus, a polio virus, dengue fever, and several other types of hemorrhagic fever.

viruses," says Todd Rider, a senior staff scientist in Lincoln Laboratory's Chemical, Biological, and Nanoscale Technologies Group who invented the new technology. Because the technology is so broad-spectrum, it could potentially also be used to combat outbreaks of new viruses, such as the 2003 SARS (severe acute respiratory syndrome) outbreak, Rider says. Other members of the research team are Lincoln Lab staff members Scott Wick, Christina Zook, Tara Boettcher, Jennifer Pancoast, and Benjamin Zusman.

Rider had the idea to try developing a broadspectrum antiviral therapy about eleven years ago, after inventing CANARY (Cellular Analysis and Notification of Antigen Risks and Yields), a



The microscope images above show that DRACO successfully treats viral infections. In the left set of four photos, rhinovirus (the common cold virus) kills untreated human cells (lower left), whereas DRACO has no toxicity in uninfected cells (upper right) and cures an infected cell population (lower right). Similarly, in the right set of four photos, dengue hemorrhagic fever virus kills untreated monkey cells (lower left), whereas DRACO has no toxicity in uninfected cells (upper right) and cures an infected cell population (lower right).

The drug works by targeting a type of RNA produced only in cells that have been infected by viruses. "In theory, it should work against all

biosensor that can rapidly identify pathogens. "If you detect a pathogenic bacterium in the environment, there is probably an antibiotic that could be used to treat someone exposed to that, but. I realized there are very few treatments out there for viruses," he says.

There are a handful of drugs that combat specific viruses, such as the protease inhibitors used to control HIV infection, but these are relatively few in number and susceptible to viral resistance.

Rider drew inspiration for his therapeutic agents, dubbed DRACOs (Double-stranded RNA Activated Caspase Oligomerizers), from living cells' own defense systems.

When viruses infect a cell, they take over its cellular machinery for their own purpose

is, creating more copies of the virus. During this process, the viruses create long strings of double-stranded RNA (dsRNA), which is not found in human or other animal cells.

As part of their natural defenses against viral infection, human cells have proteins that latch onto dsRNA, setting off a cascade of reactions that prevents the virus from replicating itself. Many viruses, however, can outsmart that system by blocking one of the steps further down the cascade.

Rider had the idea to combine a dsRNAbinding protein with another protein that induces cells to undergo apoptosis (programmed cell suicide) — launched, for example, when a cell determines it is en route to becoming cancerous.

Therefore, when one end of the DRACO binds to dsRNA, it signals the other end of the DRACO to initiate cell suicide.

Combining those two elements is a "great idea" and a very novel approach, says Karla Kirkegaard, professor of microbiology and immunology at Stanford University. "Viruses are pretty good at developing resistance to things we try against them, but in this case, it's hard to think of a simple pathway to drug resistance," she says.

Each DRACO also includes a "delivery tag," taken from naturally occurring proteins, that allows it to cross cell membranes and enter any human or animal cell. If no dsRNA is present, however, DRACO leaves the cell unharmed.

The release notes that most of the tests reported in this study were done in human and animal cells cultured in the lab, but the researchers also tested DRACO in mice infected with the H1N1 influenza virus. When mice were treated with DRACO, they were completely cured of the infection. The tests also showed that DRACO itself is not toxic to mice.

The researchers are now testing DRACO against more viruses in mice and beginning to get promising results. Rider says he hopes to license the technology for trials in larger animals and for eventual human clinical trials.

- Read more in Todd H. Rider et al., "Broad-Spectrum Antiviral Therapeutics," PLoS ONE 6, no. 7 (27 July 2011)

#### Qaeda Trying to Harness Toxin for Bombs, U.S. Officials Fear

#### By Eric Schmitt and Thom Shanker

Source: http://www.nytimes.com/2011/08/13/world/middleeast/13terror.html?\_r=1



Agence France-Presse — Getty Images: Yemeni soldiers sought Qaeda militants last year. Al Qaeda's Yemeni branch is said to be seeking castor beans for making ricin.



American counterterrorism officials are increasingly concerned that the most dangerous regional arm of Al Qaeda is trying to produce the lethal poison ricin, to be packed around small explosives for attacks against the United States.

For more than a year, according to classified intelligence reports, AI Qaeda's affiliate in Yemen has been making efforts to acquire large quantities of castor beans, which are required to produce ricin, a white, powdery toxin that is so deadly that just a speck can kill if it is inhaled or reaches the bloodstream.

Intelligence officials say they have collected evidence that Qaeda operatives are trying to move castor beans and processing agents to a hideaway in Shabwa Province, in one of Yemen's rugged tribal areas controlled by insurgents. The officials say the evidence points to efforts to secretly concoct batches of the poison, pack them around small explosives, and then try to explode them in contained spaces, like a shopping mall, an airport or a subway station.



Muhammad ud-Deen, via Associated Press -Anwar al-Awlaki, an American in the Qaeda branch.

President Obama and his top national security aides were first briefed on the threat last year and have received periodic updates since then, top aides said. Senior American officials say there is no indication that a ricin attack is imminent, and some experts say the Qaeda affiliate is still struggling with how to deploy ricin as an effective weapon.

These officials also note that ricin's utility as a weapon is limited because the substance loses its potency in dry, sunny conditions, and unlike many nerve agents, it is not easily absorbed through the skin. Yemen is a hot, dry country, posing an additional challenge to militants trying to produce ricin there.

But senior American officials say they are tracking the possibility of a threat very closely, given the Yemeni affiliate's proven ability to devise plots, including some thwarted only at the last minute: a bomb sewn into the underwear of a Nigerian man aboard a commercial jetliner to Detroit in December 2009, and printer cartridges packed with powerful explosives in cargo bound for Chicago 10 months later.

"The potential threat of weapons of mass destruction, likely in a simpler form than what people might imagine but still a form that would have a significant psychological impact, from Al Qaeda in the Arabian Peninsula in Yemen, is very, very real," Michael E. Leiter, who retired recently as director of the National Counterterrorism Center, said at a security conference last month. "It's not hard to develop ricin."

A range of administration officials have stated that the threat of a major attack from Al Qaeda's main leadership in Pakistan has waned after Osama bin Laden's death in May, on top of the Central Intelligence Agency's increasing drone assaults on Qaeda targets in Pakistan's tribal areas over the past three years.

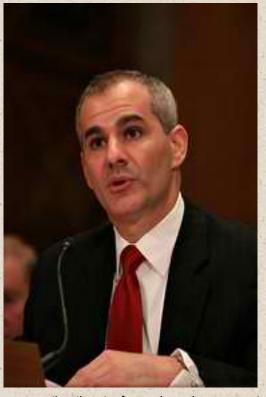
But the continuing concern over a ricin plot underscores the menace that regional Qaeda affiliates, especially AI Qaeda in the Arabian Peninsula, now pose to the United States and American interests overseas.

"That line of threat has never abated," said a senior American official, who referred to the terrorist group by its initials. "That's been taken seriously by this government. What we know about A.Q.A.P. is that they do what they say." Al Qaeda's arm in Yemen has openly discussed deploying ricin and other deadly poisons against the United States. "Brothers

with less experience in the fields of microbiology or chemistry, as long as the

possess basic scientific knowledge, would be able to develop other poisons such as ricin or cyanide," the organization posted to its online English-language journal, Inspire, last fall, in an article titled "Tips for Our Brothers in the United States of America."

Senior administration officials say ricin is



among the threats focused on by a secret government task force created after the printercartridge plot. The task force is working closely with Saudi intelligence officials and the remnants of Yemen's intelligence agencies, and it is using information gleaned from the shipboard interrogation of a Somali terrorist leader with ties to the Yemeni branch of Al Qaeda, who was captured by Navy Seal commandos in April.

The intelligence reports indicating ricin plots by Al Qaeda's Yemeni affiliate were first uncovered during reporting for a book, "Counterstrike: The Untold Story of America's Secret Campaign Against Al Qaeda." It will be published next week by Times Books, an imprint of Henry Holt & Company.

American officials now say that Al Qaeda's most direct threat to the United States comes from the Yemeni affiliate. These officials have also expressed growing alarm at the way the affiliate is capitalizing on the virtual collapse of Yemen's government to widen its area of control inside the country, and is strengthening its operational ties to the Shabab, the Islamic militancy in Somalia, to exploit the chaos in both countries.

"It continues to demonstrate its growing ambitions and strong desire to carry out attacks outside its region," Daniel Benjamin, the State Department's counterterrorism coordinator, said in a speech last month, referring to Al Qaeda's Yemeni branch.

The affiliate has also become a magnet for terrorists fleeing the increasing pressure from drone strikes in Pakistan, and is recruiting specialists in bomb-making and other skills. "These guys have got some notoriety," said a senior United States official who follows Al Qaeda and its affiliates closely. "They have a natural, charismatic attraction value for people who want to be jihadists and plot against the West."

### Allison Shelley/E.P.A. - Michael E. Leiter, a former counterterrorism official.

"A.Q.A.P.'s senior leaders are a lot like an organization that's largely a brain that exists on its own and has to recruit its arms and legs to actually execute things," the official continued. Largely because of the Americans in the Yemeni affiliate's top leadership, including Anwar al-Awlaki, a cleric born in New Mexico who is in hiding in Yemen, American counterterrorism and intelligence officials fear the affiliate's innovative agility. "The fastestlearning enemy we have is A.Q.A.P.," said the senior United States official.

In recent months, as the Yemeni government has become nearly paralyzed, the Obama administration has stepped up pressure on the Qaeda affiliate there. It has escalated a campaign of airstrikes carried out by the Pentagon's Joint Special Operations Command with the C.I.A.'s help. The C.I.A. is building a base in the region to serve as a hub for future operations in Yemen.

The Pentagon's air campaign in Yemen was renewed in May after a nearly yearlong hiatus; since then the military has carried out at least four airstrikes in the country.

The ricin plots believed to be emanating from Yemen are the latest example of terrorists' desire to obtain and deploy unconventional weapons in attacks. In 1995, the Aum Shinrikyo cult released sarin nerve gas on underground trains in Tokyo, killing 12 people and injuring more than 5,000, and nearly.

paralyzing one of the world's leading economies for weeks.

In 2003, British and French operatives broke up suspected Qaeda cells that possessed components and manuals for making ricin bombs and maps of the London subway system.

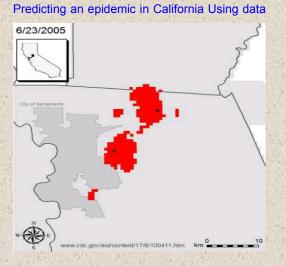
A ricin-dispersing bomb detonated in a major subway system or in a mall or at a major airport would not result in mass destruction on the scale of the attacks on Sept. 11, 2001, counterterrorism specialists said. But it could inflict disproportionate psychological terror on big-city transportation systems. "Is it going to kill many people? No," said Mr. Leiter, the former counterterrorism official. "Is it going to be a big news story and is it going to scare some people? Yes."

Months after the initial ricin intelligence reports surfaced last year, Saudi intelligence officials revealed a twist to the ricin plot: Qaeda operatives were trying to place the toxin in bottles of perfume, especially a popular local fragrance made of the resin of agarwood, and send those bottles as gifts to assassinate government officials and law enforcement and military officers. There is no indication that Al Qaeda ever succeeded with this approach, intelligence officials said.

## Software successfully predicted spread of West Nile virus in California

Source: http://news.brown.edu/pressreleases/2011/08/dycast

A computerized epidemiological model of the spread of the mosquito-borne West Nile virus in seventeen counties of California in 2005 successfully predicted where 81.6 percent of human cases of the disease would arise and defined high-risk areas where the risk of infection turned out to be thirty-nine times higher than in low-risk areas, according to newly published research. The DYCAST software used in those predictions is now open-source and is being applied to other diseases.



on the incubation of West Nile virus, the life cycle of mosquitoes, and the flight of birds, DYCAST software successfully predicted where human infections would occur. Centers for Disease Control "One of the things that really differentiates DYCAST from other approaches is that it's based on biological parameters," said Ryan Carney, a Brown University graduate student who is the lead author on a paper about DYCAST's performance that appears in the current issue of the journal Emerging Infectious Diseases, published by the Centers for Disease Control (CDC). "All of the parameters in the model are based on experimental data related to the biology and ecology of the virus, mosquito vector, and bird host."

For example, the spatial parameters of the model include how far mosquitoes and infected birds are likely to fly.

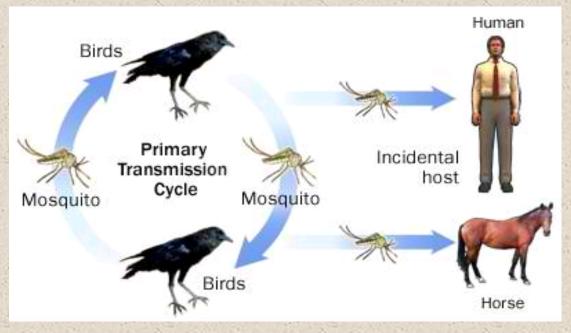
A Brown University release reports that key time parameters include how long the virus needs to incubate in mosquitoes before they become infectious and the lifespan of infected birds. Carney said that by using biology to define the geographic and temporal attributes of the model rather than county or census tract borders, which are convenient for humans but irrelevant to birds and mosquitoes, the model allowed the California Department of Public Health to provide early warnings to an area stretching from the Bay Area through Sacramento to the Nevada line, as well as regions in southern California.

Carney implemented the software when he worked for the California department in 2005 (the software was created by Constandinos Theophilides at the City University of New York). Feeding the model in 2005 were 109,358 dead bird reports phoned in or entered.

by members of the public via a state hotline and Web site.

As more dead birds were reported in close proximity, the software would generate daily maps of areas at high risk for human infection, providing an early warning to local public health officials. The software, for example, predicted and reported dead birds, along with the model's prediction rates, dropped sharply.

In 2007 Carney enrolled as a master's student at Yale and adapted the DYCAST model to track dengue fever in Brazil, using a version of the software that his CUNY collaborators had converted to an open-source platform. With the



areas as high-risk more than a month before the first human cases arose, on average.

In Sacramento County, location of the largest West Nile virus epidemic in the United States that year, DYCAST helped mosquito control officials target their testing and spraying resources — actions that ultimately reduced human illness, Carney said.

The release notes that after 2005, the department implemented the model throughout the state, although the number of human cases

specific parameters of that disease, DYCAST was able to predict its spread in the city of Riberão Preto in Brazil, Carney said, citing unpublished data.

Carney has continued his analysis and development of DYCAST and dengue at Brown, where he is a doctoral student of ecology and evolutionary biology. He said the software at its core has potential to be adapted as an early warning system for other infectious diseases or even bioterrorism attacks.

— Read more in Ryan M. Carney et al., "Early Warning System for West Nile Virus Risk Areas, California, USA," <u>Emerging Infectious Diseases</u> 17, no. 8 (August 2011)

#### Abstract

The Dynamic Continuous-Area Space-Time (DYCAST) system is a biologically based spatiotemporal model that uses public reports of dead birds to identify areas at high risk for West Nile virus (WNV) transmission to humans. In 2005, during a statewide epidemic of WNV (880 cases), the California Department of Public Health prospectively implemented DYCAST over 32,517 km<sup>2</sup> in California. Daily risk maps were made available online and used by local agencies to target public education campaigns, surveillance, and mosquito control. DYCAST had 80.8% sensitivity and 90.6% specificity for predicting human cases, and k analysis indicated moderate strength of chance-adjusted agreement for >4 weeks. High-risk grid cells (populations) were identified an average of 37.2 days before onset of human illness; relative risk for disease was >39× higher than for low-risk cells. Although prediction rates declined in subsequent years, results indicate DYCAST was a timely and effective early warning system during the severe 2005 epidemic.

#### How did H1N1 become an pandemic?

Source: http://www.homelandsecuritynewswire.com/how-did-h1n1-become-pandemic

The last century has seen two major pandemics caused by the H1N1 virus — the Spanish Flu in 1918 and 2009's Swine Flu scare, which had thousands travelling with surgical masks and clamoring for vaccination.



Scientists, however, did not know what distinguished the Swine Flu from ordinary influenza in pigs or seasonal outbreaks in humans, giving it the power to travel extensively and infect large populations.

Until now. Professor Nir Ben-Tal of Tel Aviv University's Department of Biochemistry and Molecular Biology and his graduate student Daphna Meroz, in collaboration with Dr. Tomer Hertz of Seattle's Fred Hutchinson Cancer Research Center, have developed a unique computational method to address this question. Published in the Proceedings of the National Academy of Sciences (PNAS), the research presents a valuable tool for identifying viral mutation strategies, tracking various virus strains and developing vaccinations, and antivirals which can protect the population. It may also lead to more precisely designed vaccines to combat these viral mutations.

A Tel Aviv University release reports that their method reveals that mutations in the virus's amino acids in specific positions, such as antigenic receptor sites, may explain how the new strain successfully spread throughout the population in 2009. These alterations allowed the strain to evade both existing vaccines and the immune system's defenses.

Viruses and our immune systems are constantly at war. A virus constantly mutates to escape notice, and our immune system strives to play catch-up — to recognize the virus and mobilize the body's defense system. To determine the spread of the 2009 human pandemic flu, Prof. Ben-Tal and his fellow researchers analyzed the hemagglutinin protein, which controls the virus' ability to fuse to a host cell in the body and transfer the genome which contains the information needed to make more virus. Eventually, he says, our immune system is able to recognize a virus' hemagglutinin, which triggers its reaction to fight against the virus.

Using a statistical learning algorithm, the researchers compared amino acid positions in the 2009 strain of H1N1 against the common flu and the strain of H1N1 found in Swine Flu, and discovered that major sequence changes that had occurred, altering antigenic sites and severely compromising the immune system's ability to recognize and react to the virus.

"Our new computation method showed that the main differences between the pandemic strain



and the common seasonal H1N1 strain are in some 10 amino acid positions," Prof. Ben-Tal and Meroz report.

The release notes that experiments conducted by Sun-Woo Yoon, Dr. Mariette F. Ducatez, and Thomas P. Fabrizio from Prof. Richard J. Webby's lab at St. Jude Children's Research Hospital in Memphis, Tennessee, confirmed some of the theoretical predictions.

Like its 1918 predecessor the Spanish Flu, the 2009 pandemic flu will likely go into

"hibernation" — now that this particular strain has been recognized by the immune system, its power to infect has been compromised. We were lucky, though: despite the relatively low death toll of the pandemic in 2009, similar to the number of deaths attributable to common seasonal flu, we might be facing more dangerous future outbreaks of mutated H1N1 varieties.

Because of the enormous mutation rate, says Prof. Ben-Tal, viruses can spread widely and

rapidly, and vaccines are fairly inefficient. In the future, a refined version of this computational method may ultimately be used to generically compare various strains of viruses. This indepth analysis might lead to the ability to predict how a strain will morph and determine if a pandemic could strike.

This is an important step toward revealing the amino acid determinants of the emergence of flu pandemics, but there is more work to be done, the researchers say.

#### Source of Haitian cholera outbreak identified

Source: http://www.homelandsecuritynewswire.com/source-haitian-cholera-outbreak-identified

Employing technology that reads the entire DNA code, researchers led by the Translational Genomics Research Institute (TGen) and the Technical University of Denmark (DTU) have pinpointed the source of a cholera outbreak in Haiti that killed more than 6,000 people and sickened 300,000.

Using whole genome sequencing, which spells out the billions of chemical bases in DNA, TGen and DTU provided the strongest prevent future outbreaks when international aid is rushed to disaster areas.

The study appears in the 23 August issue of mBio, a new online-only, open-access journal published by the American Society of Microbiology in partnership with the American Academy of Microbiology. "The great similarity of Haitian cholera with Nepalese cholera is based upon the highest resolution DNA methods available, and point to a probable

source of this devastating disease outbreak," said Dr. Paul Keim. Director of the TGen Pathogen Genomics and Division senior molecular biologist on the study. Dr. Keim assisted the FBI in tracking down the source of the 2001 anthrax letters case, which killed five people. He said similar genetic tracking techniques were used in investigating the Haitian cholera outbreak.

According to Dr. Keim, methods pioneered during the anthrax letter forensic

investigation and today's greatly diminished costs for whole genome sequencing make it possible to apply this powerful technology to new and critical public health challenges. Dr. Keim is a Regents Professor at Northern Arizona University (NAU), whose Center for Microbial Genetics and Genomics also contributed to the study.

Dr. Keim praised TGen's collaborators at the National Public Health Laboratory in Nepal, and at the National Food Institute in Denmark.



evidence yet that peacekeepers from Nepal, where cholera is widespread, brought the disease to Haiti, which already was reeling from a devastating earthquake in January 2010 that killed more than 300,000.

A TGen release reports that in a study titled "Population genetics of Vibrio Cholerae from Nepal: An identical clone in Nepal and the Haitian outbreak," researchers confirm the source of the cholera, and suggest how to 156

where the study's senior author, Dr. Frank M. Aarestrup, is head of the Antimicrobial Resistance and Molecular Epidemiology Unit. "This study highlights how rapidly infectious diseases might be transmitted globally through international travel, and how public health officials need to use advanced molecular tools, along with standard epidemiological analyses, to quickly and accurately determine sources of prior to deployment. This study is not about placing blame, it's about preventing such disasters in the future."

Researchers confirmed the source of the outbreak by comparing the DNA of twenty-four cholera samples (the bacterium Vibrio cholera) from five different districts in Nepal with ten samples of cholera from Haiti. All twenty-four samples from Nepal matched the samples from



outbreaks," said Dr. Aarestrup, who also is head of both the World Health Organization's Collaborating Centre for Antimicrobial Resistance among Foodborne Pathogens and of the European Union (EU) Reference Laboratory for Antimicrobial Resistance.

Dr. Lance Price, an associate professor at TGen and co-author of the new study, said the investigation into the source of Haitian cholera could help prevent such outbreaks in the future. "This effort validates the power of advanced molecular tools in investigating outbreaks of this nature," Dr. Price said. "The goal now should be finding ways to prevent such outbreaks, perhaps through screening Haiti. Some of the samples, the report said, "were almost identical."

Dr. Price said the TGen findings makes a very strong case for the source of the cholera, and aligns with a recent report by the U.S. Centers for Disease Control and Prevention, which said "evidence strongly suggests" that the Nepalese soldiers were the source of the outbreak. The CDC study was based on the fact that the first cholera infections in Haiti were downstream from the Nepalese, and occurred shortly after soldiers' arrival. the "Our studies are complementary and together make a definitive case for a Nepalese origin to the outbreak," Dr. Price said.



#### **Detecting bioterror attacks**

Source: http://www.homelandsecuritynewswire.com/detecting-bioterror-attacks

About 80 percent of the U.S. population lives in the thirty largest cities in the United States; the government has deployed a secret system of



Informatics program leader Tom Slezak gestures in front of the mobile lab Wednesday, July 13, 2011, at the Lawrence Livermore National Laboratory in Livermore, Calif. Detectors developed by Slezak and other government researchers to sniff the air for germs such as anthrax and smallpox have become a hidden fixture of the country's post-September 11 urban landscape. (AP Photo/Ben Margot)

biosensors to detect bioterror attacks; the location of the sensors, and the pathogens they search for, are kept secret so terrorists would not be able to tamper with the sensors or evade them (officially, even the list of cities where the system is deployed is kept secret). The Berkeley Lab in Livermore, California, one of the promise celd was are accessed expected.

of the premier cold war-era research centers of the U.S. government, has researchers working

on protect city dwellers from exposure to anthrax and smallpox.

The AP reports that lab researchers have created a pathogen early-warning system named Biowatch, which relies on special detectors deployed in thirty U.S. cities – sensors that can identify pathogens by sniffing the air and then alert authorities before people start becoming sick, the article said.

The AP notes that the U.S. government is keeping the location of the biosensors secret so that terrorists would not be able to evade them or tamper with them. The government also is jot saying what pathogens the sensors search for – even the list of thirty cities that have the sensors deployed is secret. The government does let it be known that about 80-percent of the U.S. population is covered by the biosensors, so we can assume that the thirty largest cities now have them.

The biosensor system's task is daunting. "We have to be able to make millions of measurements and never have a single false positive measurement," David Rakestraw, manager of the lab's weapons of mass destruction countermeasures program, told AP. There is no choice, however. "It's very clear that there's a trend toward more and more people having capabilities and more and more people having the knowledge to do these things," Rakestraw said. "I think we need to be prepared."

	Rank	City	State	Population (2010)	Land Area (square miles, 2010 data)	Population Density (per square mile of land area, 2010 data)
	1	New York	New York	8,175,133	302.6	27,016.3
	2	Los Angeles	California	3,792,621	468.7	8,091.8
	3	Chicago	Illinois	2,695,598	227.6	11,843.6
	4	Houston	Texas	2,099,451	599.6	3,501.4
	5	Philadelphia	Pennsylvania	1,526,006	134.1	11,379.6
1	6	Phoenix	Arizona	1,445,632	516.7	2,797.8
	7	San Antonio	Texas	1,327,407	460.9	2,880.0
	8	San Diego	California	1,307,402	325.2	4,020.3
	9	Dallas	Texas	1,197,816	340.5	3,517.8
	10	San Jose	California	945,942	176.5	5,359.4
						the second s

#### Thirty largest cities in the United States

	a	and the state		and the second second	The second second
11	Jacksonville	Florida	821,784	747.0	1,100.1
12	Indianapolis	Indiana	820,445	361.4	2,270.2
13	San Francisco	California	805,235	46.9	17,169.2
14	Austin	Texas	790,390	297.9	2,653.2
15	Columbus	Ohio	787,033	217.2	3,623.5
16	Fort Worth	Texas	741,206	339.8	2,181.3
17	Charlotte	North Carolina	731,424	297.7	2,456.9
18	Detroit	Michigan	713,777	138.8	5,142.5
19	El Paso	Texas	649,121	255.2	2,543.6
20	Memphis	Tennessee	646,889	315.1	2,053.0
21	Baltimore	Maryland	620,961	80.9	7,675.7
22	Boston	Massachusetts	617,594	48.3	12,786.6
23	Seattle	Washington	608,660	83.9	7,254.6
24	Washington	District of Columbia	601,723	61.0	9,864.3
25	Nashville	Tennessee	601,222	475.1	1,265.5
26	Denver	Colorado	600,158	153.0	3,922.6
27	Louisville	Kentucky	597,337	325.2	1,836.8
28	Milwaukee	Wisconsin	594,833	96.1	6,189.7
29	Portland	Oregon	583,776	133.4	4,376.1
30	Las Vegas	Nevada	583,756	135.8	4,298.6
	COURSE IN STREET, STRE		1.11. 11	·	1. 1. 01. 1

Source: http://en.wikipedia.org/wiki/List\_of\_United\_States\_cities\_by\_population

## Experts anxious about appearance of a variant strain of Bird Flu

Source:http://www.homelandsecuritynewswire.com/experts-anxious-about-appearance-variant-strainbird-flu

Since 2003 H5N1 has killed or forced the culling of more than 400 million domestic poultry and caused an estimated \$20 billion of economic damage across the globe before it was eliminated from most of the sixty-three countries infected at its peak in 2006; the UN health agency now calls for increased preparedness and surveillance against a reemerging variant strain of H5N1.

The UN Food and Agriculture Organization (FAO) on Monday urged heightened readiness and surveillance against a possible major resurgence of the H5N1 highly pathogenic avian influenza amid signs that a mutant strain of the deadly Bird Flu virus is spreading in Asia and beyond, with unpredictable risks to human health.

The H5N1 virus has infected 565 people since it first appeared in 2003, killing 331 of them, according to the World Health Organization (WHO) figures. The latest death occurred earlier this month in Cambodia, which has registered eight cases of human infection this year — all of them fatal.

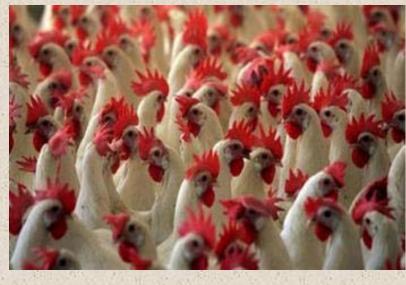
Since 2003 H5N1 has killed or forced the culling of more than 400 million domestic poultry and caused an estimated \$20 billion of economic damage across the globe before it was eliminated from most of the sixty-three countries infected at its peak in 2006.

The virus, however, remained endemic in six nations, although the number of outbreaks in domestic poultry and wild bird populations shrank steadily from an annual peak of 4000 to just 302 in mid 2008. Outbreaks have risen progressively since, however, with almost 800 cases recorded in 2010-11.

At the same time, 2008 marked the beginning of renewed geographic expansion of the H5N1 virus both in poultry and wild birds.

159

The advance appears to be associated with migratory bird movements, according to FAO chief veterinary officer Juan Lubroth. He said



migrations help the virus travel over long distances, so that H5N1 has in the past twentyfour months shown up in poultry or wild birds in countries that had been virus-free for several years. "Wild birds may introduce the virus, but peoples' actions in poultry production and marketing spread it," Lubroth noted.

Recently affected areas are to be found in Israel and the Palestinian Territories, Bulgaria, Romania, Nepal, and Mongolia.

A further cause for concern, Lubroth said, is the appearance in China and Viet Nam of a variant virus apparently able to sidestep the defenses provided by existing vaccines. In Viet Nam, which suspended its springtime poultry vaccination campaign this year, most of the northern and central parts of the country —

where H5N1 is endemic have been invaded by the new virus strain, known as H5N1-2.3.2.1.

Viet Nam's veterinary services are on high alert and reportedly considering а novel. targeted vaccination campaign this fall. Virus circulation in Viet Nam poses a direct threat to Cambodia, Thailand, and Malaysia as well as endangering the Korean peninsula and Japan further afield. Wild bird migration can also spread

the virus to other continents. "The general departure from the progressive decline observed in 2004-2008 could mean that there will be a flareup of H5N1 this fall and winter, with people unexpectedly finding the virus in their backyard," Lubroth said.

The countries where H5N1 is still firmly entrenched – Bangladesh, China, Egypt, India, Indonesia, and Vietnam – are likely to face the biggest problems but no country can consider itself safe, he said. "Preparedness and surveillance remain essential," Lubroth underlined. "This is no time for complacency. No one can let their guard down with H5N1."

#### How did the deadly plague bacterium develop?

Source: http://www.northwestern.edu/newscenter/stories/2011/08/plague-diseases-feinberg.html

In the evolutionary blink of an eye, a bacterium that causes mild stomach irritation evolved into a deadly assassin responsible for the most devastating pandemics in human history. How did the mild-mannered Yersinia pseudotuberculosis become Yersinia pestis, more commonly known as the Plague?

A Northwestern University release reports that now, scientists from Northwestern University Feinberg School of Medicine, with the use of new DNA sequencing techniques, offer long sought after evidence of how these two pathogens with virtually identical genetic matter could produce two such vastly different diseases. The Feinberg School team used the new DNA sequencing techniques to identify an unexpected source for these differences, which may help explain the Plague's rapid evolution. The findings, published 29 August in the journal Proceedings of the National Academy of Sciences (PNAS), offer a glimpse into how

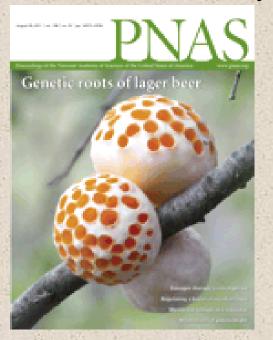
the new technology might aid in the development of therapeutics to fight deadly diseases, including the Plague. "Most people think of the Plague as a historic disease, but it's still a public health issue today, both in the human population and in animals," said Wyndham Lathem, lead author of the study and assistant professor of microbiologyimmunology at Northwestern's Feinberg School. "It's extremely dangerous and highly virulent. Without treatment, it can take as little as three to five days from infection to death?"

Globally, the World Health Organization (WHO) reports 1,000 to 3,000 cases of Plague every year, and Y. pestis exists on every continent except Antarctica. The U.S. DHS classifies Y. pestis as a Category A biological agent, a group that also includes anthrax, smallpox and Ebola.

The Plague's ancestor, Y. pseudotuberculosis, still exists and infects humans, but it causes a mild gastrointestinal disease and most people don't show symptoms.

The release notes that Lathem and colleagues have discovered the differences in disease severity between these two subspecies may have arisen from changes in small, non-coding RNAs (sRNAs), complex molecules involved in controlling many cellular processes.

The Northwestern team is the first to show that sRNAs in Yersinia affect virulence, a finding



that suggests the evolution of pathogens may also occur at the level of changes in RNA and in the way protein-coding genes are regulated. Lathem used advanced DNA sequencing technology — called high-throughput sequencing — to identify the complete set of sRNAs produced by Y. pseudotuberculosis. The technology enabled his team to study the diseases for the first time at a deeper genetic level.

"This technique enables us to really pick apart how pathogens evolve and how different species of bacteria are able to cause different types of disease," Lathem said. "It goes beyond looking at what proteins are produced by the bacteria. It's an additional layer of evolutionary analysis."

This detective work is important because if



researchers can identify unique characteristics among deadly species such as Y. pestis, they may be able to generate new therapeutics or adapt current ones.

Unlike traditional "messenger" RNA, which is copied from DNA to create proteins and is well understood by scientists, these non-coding sRNA molecules are never translated into proteins. Hundreds of noncoding RNA molecules exist inside bacterial cells, but, until recently, scientists had not determined the function of many.

"Once we identified the complete set of sRNAs for Y. pseudotuberculosis, further analysis unlocked a number of surprising discoveries about their function," Lathem said.

Among these surprising discoveries, Lathem's team identified 150 sRNAs, a majority of which are specific to the Yersinia species, and six sRNAs unique to Y. pseudotuberculosis. Those six sRNAs are missing in Y. pestis, likely lost during its rapid evolution (somewhere between 1,500 and 20,000 years ago), and thereby potentially responsible for the Plague's virulence. Lathem's team developed this explanation because they could specify exactly which genes the sRNAs control.

First author Jovanka Koo, a postdoctoral fellow in Lathem's lab at Feinberg, noted, "An important lesson is that small changes can have big effects on sRNA functions. They can affect when an RNA is expressed or produced, the way that RNA folds, and the ability of that RNA to affect the regulated protein coding RNA." Over time, those small changes can become the difference between mild, and deadly diseases.

The research was funded by a developmental projects grant from the Great Lakes Regional

Center of Excellence for Biodefense and Emerging Infectious Diseases Research.

#### Hunting for a Mass Killer in Medieval Graveyards

#### **By Nicholas Wade**

Source: http://www.nytimes.com/2011/08/30/science/30plague.html?\_r=1

Beneath the Royal Mint Court, diagonally across the street from the Tower of London, lie 1,800 mute witnesses to the foresight of the city fathers in the year 1348. Recognizing that the Black Death then scourging Europe would inevitably reach London, the authorities prepared a special cemetery in East



Sources: Univ. of Texas; "Historical Atlas," by William Shepherd; St. Nicholas Center THE NEW YORK TIMES Smithfield, outside the city walls, to receive the bodies of the stricken.

By autumn, the plague arrived. Within two years, a third or so of London's citizens had died, a proportion similar to that elsewhere in Europe. The East Smithfield cemetery held 2,400 of the victims, whose bodies were stacked five deep.

The agent of the Black Death is assumed to be *Yersinia pestis*, the microbe that causes bubonic plague today. But the epidemiology was strikingly different from that of modern outbreaks. Modern plague is carried by fleas and spreads no faster than the rats that carry them can travel. The Black

Death seems to have spread directly from one person to another. Victims sometimes emitted a deathly stench, which is not true of plague victims today. And the Black Death felled at least 30 percent of those it inflicted, whereas a modern plague in India that struck Bombay in 1904, before the advent of antibiotics, killed only 3 percent of its victims.

These differences, as well as the fear that the Black Death might re-emerge, have prompted several

(3) see aver	
Í ONDONS E	
LORD HAVE MERCY UPON US	
A true Relation of Seven modern Plagues or Visitations in London, with the number of th	
Buried of all Dileafes; Vie The fuff in the year of Queen ELIZABETH. Anno 1592. The fecond in the year a (that were to be forgotten year) to 25. The Southin Anno 2630. The fit in the year 2636. The first in the year 2627, and 2638. The formula the	603 the third in the spiciant year. 1665.
din add the Universe of Proceedings of the Control of the Control of the Control of the Control	Liberrice this year of all
	e că

attempts to retrieve DNA from Black Death cemeteries. The latest of these attempts is reported Tuesday in of The Proceedings of the National Academy of Sciences by a team led by Hendrik

Poinar of McMaster University in Ontario and Johannes Krause of the University of Tübingen in Germany.

They looked for surviving fragments of DNA in bones and teeth that archaeologists had excavated from the East Smithfield site in the 1980s. The DNA matched that of the modern-day microbe, confirming, as



have several other studies, that Yersinia pestis was indeed the agent of the Black Death. Sharon DeWitte, a member of Dr. Poinar's team, was one of several skeptics who had doubted the microbe's role. "I'm very happy to find out I was wrong," said Dr. DeWitte, a paleodemographer at the University of South Carolina. "In science, if you're open to alternative possibilities, you can change your mind."

Dr. Poinar's team also looked for the microbe's DNA in another medieval London cemetery, that of St. Nicholas Shambles, which was closed before the Black Death struck. They found no sign of it there, indicating that Yersinia pestis was not already present in the English population before the Black Death, so it must have arrived from elsewhere.

If *Yersinia pestis* was indeed the cause of the Black Death, why were the microbe's effects so different in medieval times? Its DNA sequence may hold the answer. Dr. Poinar's team has managed to reconstruct a part of the microbe's genetic endowment. Yersinia pestis has a single chromosome, containing the bulk of its genes, and three small circles of DNA known as plasmids.

The team has determined the full DNA sequence of the plasmid known as pPCP1 from the East Smithfield cemetery. But, disappointingly, it turns out to be identical to the modern-day plasmid, so it explains none of the differences in the microbe's effects. "It was probably a naïve approach to assume we'd get the smoking gun on first attempt," Dr. Poinar said.

Mark Achtman, an expert on plague who works at University College Cork in Ireland, said that the new study was "technologically interesting" but that a great deal more of the microbe's DNA needed to be sequenced to obtain scientifically important results.

This is indeed Dr. Poinar's plan. The challenge in reconstructing the microbe's DNA from the East Smithfield cemetery is that it is highly fragmented. The Yersinia pestis chromosome is 4,653,728 units of DNA in length, but the bits of DNA from the cemetery are no more than 50 to 60 units long.

Determining the order of the chemical units in such fragments has become possible only in the last few years with the development of new DNA sequencing machines that work with short fragments.

Another technical challenge is to separate the plague DNA from that of the human and other microbial DNA in the ancient bones. One technique that Dr. Poinar's team has used is to tether plasmid DNA from the ancient bones.

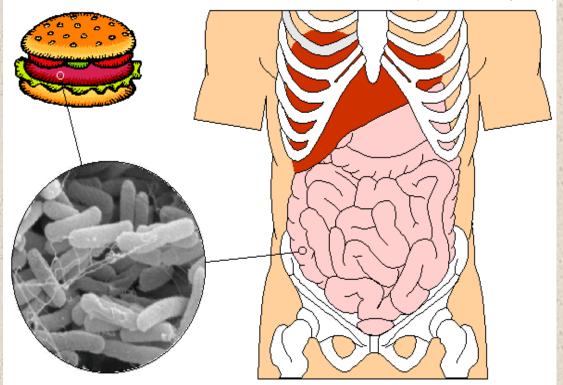
the modern plague microbe to plastic beads. DNA is quick to bind to strands of DNA of the complementary sequence, as in the DNA double helix. So the beads act as fishing rods to pull out the DNA of interest. "It's probably exceptionally important to find out what made this bug so deadly in the past," Dr. Poinar said.

#### Anthrax-like Disease Caused by Bacillus cereus

#### By Amesh A. Adalja, MD, FAC

Source: http://www.upmc-biosecurity.org/index.html

A man in Texas recently died of an anthrax-like illness that was caused by a toxin-producing strain of *Bacillus cereus*. Of the *Bacillus* species known to cause human disease, only *B. anthracis* is generally



recognized as capable of causing fulminant disease. *B. cereus*, the other major *Bacillus* species that causes human disease, is primarily associated with "food poisoning" and endopthalmitis. However, this recent report of anthrax-like disease caused by *B. cereus* illustrates that, under certain circumstances, *B. cereus* can be a deadly pathogen—a fact that has been known but often overlooked.<sup>1</sup>

#### Microbiology of Bacillus

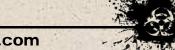
The genus *Bacillus* comprises many species, all of which are spore-forming gram-positive rods that are naturally found in soil throughout much of the world. The *B. cereus* group includes 6 species, among them *B. anthracis* and *B. cereus*, the ancestor from which *B. anthracis* is descended. The virulence of *B. anthracis* is the product of 2 plasmids: pXO1, which contains the genetic material for 2 exotoxins, and pXO2, which contains the genetic material for the antiphagocytic capsule. In the clinical setting, distinguishing the species microbiologically to identify *B.anthracis* is relatively simple.

#### Characteristics that distinguish B. anthracis:

- nonhemolytic on blood agar
- nonmotile on agar
- catalase positive
- colonies have a "whipped egg" appearance and a "comet tail" or "Medusa's head" morphology.

Importantly, antimicrobial susceptibility also differs among the species: *B. cereus* is often resistant to beta-lactam antibiotics, with the exception of carbapenems.<sup>1,2</sup>





#### Severe Disease with Naturally Occurring pXO1-containing B. cereus

Fulminant disease from *B. cereus* in immunocompromised hosts is well described, but its ability to cause severe disease in healthy hosts is not widely appreciated. However, reports dating back to at least 1965<sup>3</sup> have described cases clinically similar to anthrax that were caused by *B. cereus*. In 2004, to further characterize these strains, Hoffmaster and colleagues retrospectively identified the presence of the pXO1 plasmid in a *B. cereus* strain isolated from a patient who had a life-threatening pneumonia.<sup>4</sup> In subsequent reports, 2 fatal *B. cereus* pneumonia cases (2003 and 2004) that also harbored the pXO1 plasmid were described. Both of these patients were metal workers in Texas whose exposure to *B. cereus*-laden dust and noxious metal fumes was thought to predispose them to this infection; the same



was suspected of 2 other cases reported in 1997.  $^{5,6}$ 

#### B. cereus (left), B. anthracis (right)

A *B. cereus* strain harboring both virulence plasmids also has been isolated from fatal cases of anthrax-like disease in chimpanzees in Côte d'Ivoire.<sup>7</sup> The most recent human case, reported this year in a welder from Texas who was infected with a *B. cereus* strain containing the pOx1 plasmid, was fatal.<sup>8</sup>

#### Not Just a Contaminant

When a *Bacillus* species is recovered from a patient sample, it often is regarded as an environmental contaminant that has made its way into a sterile culture. Typically, no treatment is initiated, and the sample is discarded once it is shown not to be *B. anthracis*. The *Bacillus* is not routinely identified to the species level. Because *B. cereus* may be life-threatening if it has acquired the pOx1 plasmid, its presence in a culture collected from a patient with bacteremia, sepsis, and/or pneumonia should merit further investigation. This is particularly important because *B. cereus* is resistant to the most commonly prescribed antimicrobials for community-acquired pneumonia (standard beta-lactam antibiotics), which makes a rapid and accurate bacteriological diagnosis essential to timely initiation of appropriate antibiotic therapy. Additionally, attention to a patient's occupational history should be emphasized, as metal workers appear to be disproportionately represented among the reported cases (at least anecdotally). In recognition of this organism's pathogenicity, laboratories should consider expanding testing of *Bacillus* isolates from patients to exclude not just *B. anthracis* but also *B. cereus*.

#### References

- 1. Martin GJ, Friedlander AM. *Bacillus anthracis* (anthrax). In: Mandell GL, Bennett JE, Dolin R, eds. *Mandell, Douglas, and Bennett's Principles and Practice of Infectious Diseases*. 7th ed. Philadelphia, PA: Churchill Livingstone; 2010.
- Fekete T. Bacillus species and related genera other than Bacillus anthracis. In: Mandell GL, Bennett JE, Dolin R, eds. Mandell, Douglas, and Bennett's Principles and Practice of Infectious Diseases. 7th ed. Philadelphia, PA: Churchill Livingstone; 2010.
- 3. Stapler T, Caneuscu V, Voiculescu M. Bronchopneumonia with lethal evolution determined by a microorganism of the genus *Bacillus* (*B.cereus*). *Rom Med Rev* 1965; 2:7–9.
- Hoffmaster AR, Ravel J, Rasko DA, et al. Identification of anthrax toxin genes in a *Bacillus* cereus associated with an illness resembling inhalation anthrax. *Proc Natl Acad Sci U S A* 2004; 101: 8449-8454.
- 5. Avashia SB, Riggins WS, Lindley C, et al. Fatal pneumonia among metalworkers due to inhalation exposure to *Bacillus cereus* containing *Bacillus anthracis* toxin genes. *Clin Infect Dis* 2007; 44:414-416.
- 6. Miller JM, Hair GD, Hebert M, et al. Fulminating bacteremia and pneumonia due to *Bacillus cereus*. *J Clin Microbiol* 1997;35: 504-507.
- Klee SR, Brzuszkiewicz EB, Nattermann H, et al. The genome of a *Bacillus* isolate causing anthrax in chimpanzees combines chromosomal properties of *B.cereus* with *B.anthracis* virulence plasmids. *PLoS One.* 2010 July 9;5(7):e10986.



165

 Wright AM, Beres SB, Consamus EN, et al. Rapidly progressive, fatal, inhalation anthrax-like infection in a human. *Arch Pathol Lab Med* 2011; http://www.archivesofpathology.org/doi/pdf/10.1043/2011-0362-SAIR.1. Accessed August 29, 2011.

#### Dangerous TB spreading at alarming rate in Europe-WHO By Kate Kelland

Source: www.reutersreprints.com.

Multidrug-resistant and extensively drugresistant forms of tuberculosis (TB) are spreading at an alarming rate in Europe and will kill thousands unless health authorities halt the pandemic, the World Health Organization

- Tuberculosis has come back "with a vengeance" in Europe
- More than 80,000 cases in WHO's European region each year
- Drug-resistant strains can take years to treat, many patients die
- London has more overall cases of TB than anywhere in western Europe with 3,500 new ones reported every year. There are also high rates in Birmingham and Glasgow. Across the UK, there are around 9,000 cases a year.

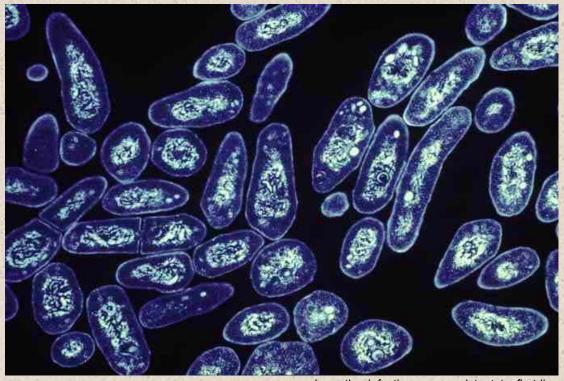
(WHO) said on Wednesday. Launching a new regional plan to find, European director warned that complacency had allowed a resurgence of TB and failure to tackle it now would mean huge human and economic costs in the future.

"TB is an old disease that never went away, and now it is evolving with a vengeance," said Zsuzsanna Jakab, the WHO's Regional Director for Europe.

"The numbers are scary," Lucica Ditiu, executive secretary of the Stop TB Partnership told a news conference in London. "This is a very dramatic situation."

TB is currently a worldwide pandemic that kills around 1.7 million people a year. The infection is caused by the bacterium Mycobacterium tuberculosis and destroys patients' lung tissue, causing them to cough up the bacteria, which then spreads through the air and can be inhaled by others.

Cases of multidrug-resistant (MDR-TB) and extensively drug-resistant TB (XDR-TB) --



diagnose and treat cases of the airborne infectious disease more effectively, the WHO's

where the infections are resistant to first-line and then second-line antibiotic treatments r

167

are spreading fast, with about 440,000 new patients every year around the world.

According to the WHO and Stop TB, 15 of the 27 countries with the highest burden of MDR-TB are in the WHO's European region, which includes 53 countries in Europe and Central Asia.

More than 80,000 MDR-TB cases occur in the region each year -- almost a fifth of the world's total. The WHO said precise figures for XDR-TB are not available because most countries lack the facilities to diagnose it, but officially reported cases of XDR-TB increased six-fold between 2008 and 2009.

Rates are highest in Eastern Europe and Central Asia, but many countries in western Europe have increasing rates of TB and drugresistant TB, Ditiu said. Britain's capital, London, has the highest TB rate of any capital city in Western Europe with around 3,500 cases a year, 2 percent of which are MDR-TB.

Treating even normal TB is a long and unpleasant process, with patients needing to take a combination of powerful antibiotics for 6 months. Many patients fail to correctly complete the course of medicines, a factor which has fueled a rise in drug-resistant forms of the disease.

Treatment regimes for MDR-TB and XDR-TB can stretch into two or more years, costing up

#### The Real Threat of 'Contagion'

By W. Ian Lipkin

Source: http://www.nytimes.com/2011/09/12/opinion/the-real-threat-of-contagion.html?\_r=1

I ADMIT I was wary when I was approached, late in 2008, about working on a movie with the director Steven Soderbergh about a flulike pandemic. It seemed that every few years a filmmaker imagined a world in which a virus transformed humans into flesh-eating zombies, or scientists discovered and delivered the cure for a lethal infectious disease in an impossibly short period of time.

Moviegoers might find fantasies like these entertaining, but for a microbe hunter like me, who spends his days trying to identify the viruses that cause dangerous diseases, the truth about the potential of global outbreaks is gripping enough.

Then I discovered that Mr. Soderbergh and the screenwriter on the project, Scott Z. Burns, agreed with me. They were determined to make a movie — "Contagion," which opened this weekend — that didn't distort reality but did

to \$16,000 in drugs alone and up to \$200,000 to \$300,000 per patient if isolation hospital costs, medical care and other resources are taken into account.

Experts say around 7 percent of patients with straightforward TB die, and that death rate rises to around 50 percent of patients with drug-resistant forms.

The WHO's action plan for tackling tuberculosis emphasizes the need for doctors and patients to be more aware of the disease and its symptoms, to diagnose and treat cases promptly with the right drugs, and follow patients up over many months or years to ensure they take their medications.

If that doesn't happen "not only are these people quietly and painfully dying, they are also spreading the disease," Ditiu said.

The WHO said that if the plan is fully implemented -- at an estimated cost of \$5 billion -- 127,000 people will be successfully treated for drug-resistant TB and 120,000 deaths will be averted by 2015.

The cost would also be recouped, since 250 000 MDR-TB and 13,000 XDR-TB cases will be prevented, saving \$7 billion in averted treatment costs, the WHO said. It added that prevention of premature deaths among TB patients would add to economic productivity in the region and generate an extra \$5 billion.

convey the risks that we all face from emerging infectious diseases. Those risks are very real — and are increasing

drastically. More than three-quarters of all emerging infectious diseases originate when microbes jump from wildlife to humans. Our vulnerability to such diseases has been heightened by the growth in international travel and the globalization of food production. In addition, deforestation and urbanization continue to displace wildlife, increasing the probability that wild creatures will come in contact with domesticated animals and humans.

When I was a kid, the launching of Sputnik made us aware that the United States was falling behind the Soviet Union in the race for space. Now all of us are in a battle that is potentially devastating, only it is not against another country, but against microbes. Could

movie like "Contagion" be an effective vehicle for sounding the alarm?



Kate Winslet plays an epidemic intelligence service officer in the new movie, "Contagion." (Courtesy Warner Bros.)

In the hope that it would, I signed on as a paid technical consultant on the film. The first order

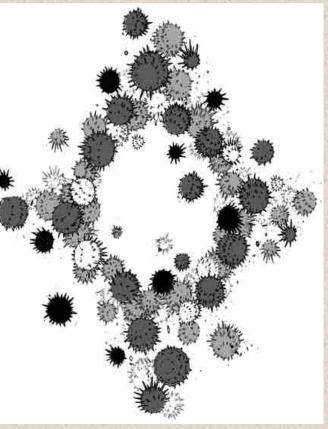
of business was a casting call for the virus itself. Together with my team at the Center for Infection and Immunity at Columbia University's Mailman School of Public Health, I devised the imaginary virus that wreaks havoc in the film. We used as our inspiration the Nipah virus, which in Malaysia in the late 1990s jumped from bats to pigs to humans, causing respiratory encephalitis disease and and resulting in more than 100 deaths contained before it was by quarantine.

My team built a 3-D model of our virus and then worked out how it would spread and evolve, how it would be discovered, how the public health and medical communities and governments would respond regionally and internationally, how vaccines would be developed and distributed. In the film, it takes the lives of millions of people.

Is this fiction? Yes. Is it real? Absolutely. During the SARS

outbreak of 2003, the first pandemic of the 21st century, I flew to Beijing at the invitation of the Chinese government to help address the situation there. My memories of deserted streets, food and supply shortages, and political instability are reflected in scenes in "Contagion." I hope the public and our lawmakers will see the movie as a cautionary tale. Pandemics have happened before. And they will happen again. What can we do to prepare ourselves? A presidential directive in 2007 led to the establishment of the National Biosurveillance Advisory Subcommittee, at the Centers for Disease Control and Prevention, to assess our biosurveillance capabilities and make recommendations for improving detection, prevention and management of biohazards. The subcommittee, which includes representatives from federal, state and local agencies, academia and industry (and on which I serve as co-chairman), has issued reports that provide a road map for steps we have to take to protect our future.

First, we need to recognize that our public health system is underfinanced and overwhelmed. We must invest in sensitive, inexpensive diagnostic tests and better ways of



manufacturing and distributing drugs and vaccines. Although new technology now allows us to design many vaccines in days, manufacturing strategies for influenza vaccines have not changed in decades. Some experts will say that the time frame within which "Contagion" introduces the film's MEV-1 vaccine is unrealistically short; however, it need not be so. We can and must reduce the several months required to create and test a

www.cbrne-terrorism-newsletter.com

168

vaccine before beginning large-scale production and distribution.

Second, more and better coordination is needed among many local, federal and international agencies. Joint effort is required to monitor human, animal and environmental health, optimize electronic health records, mine nontraditional data sources like the Internet for early signs of outbreaks and invest in a stateof-the-art work force. "Contagion" makes the case that scientists and public health professionals who put themselves on the line to fight infectious diseases are heroes. I hope that, like Sputnik, it will inspire young people to pursue these careers and help the rest of the country understand the importance of these efforts. It is what the world urgently needs.

W. Ian Lipkin is a professor of epidemiology and a professor of neurology and pathology at Columbia University.

#### University lab focuses on deadly natural biological agents

Source: http://www2.tbo.com/news/education-news/2011/sep/10/menewso1-nature-new-focus-of-usf-lab-targeting-bio-ar-256686/

In the decade since the Center for Biological Defense at the University of South Florida opened, the research facility has shifted its

focus from man-made biological agents to detecting natural biological threats.

Andrew Cannons, the lab supervisor, said nature is "a much better terrorist than man could ever be."

Opened shortly after 9/11 and the anthrax letter attacks, the lab initially received \$4 million to help create a system to prepare public health workers to deal with bioterrorism attacks.

The lab initially focused primarily on helping emergency

responders gather samples, creating a streamlined process to ensure that samples remained pure and workers were protected. The lab also developed a test to quickly determine if a substance was dangerous or not – its methods were capable of identifying anthrax spores in about fifteen minutes. From

there, the lab went on to discover new methods for genetically identifying the "bugs" and finding out whether they had been seen elsewhere and would respond to antibiotics.

So far the lab has collected about 1,500 strains of bacteria that Cannons called "a unique collection of bacteria that no one else has." Now the lab is focusing on threats stemming from nature to stay ahead of the curve. Cannons said the

University of South Florida is constantly preparing for "what's around the corner," whether it be a deadly virus, antibiotic-resistant organism, or food-borne illness.







HARVARD SCHOOL OF PUBLIC HEALTH CENTER FOR CONTINUING PROFESSIONAL EDUCATION Where theory informs practice and practice informs theory \*

The Harvard School of Public Health Center for Continuing Professional Education offers two programs

Basic Hands-On CAMEO Training And Advanced Hands-On CAMEO Training.

Basic: https://ccpe.sph.harvard.edu/CAMEO Advanced: https://ccpe.sph.harvard.edu/Advanced-CAMEO

The CAMEO program, developed by the USEPA and NOAA, helps state and local governments as well as corporate entities plan for and respond to chemical emergencies.

# POC

# Peter J. Bretton

Center for Continuing Professional Education Harvard School of Public Health 677 Huntington Ave. | Boston, MA 02115 PBretton@hsph.harvard.edu | (617) 384-8965



# Dirty News

## Flood waters threaten nuke plants along the Missouri River

Source:http://conservationreport.com/2011/06/20/nuclear-power-flood-waters-threaten-shutdown-of-nuke-plants-along-the-missouri-river/

In addition to droughts, earthquakes, and tsunamis, flooding is another threat to nuclear power plants. Both the Fort Calhoun Nuclear Power Station near Fort Calhoun, Nebraska, level and [Omaha Public Power District] OPPD officials stated that the current flood protection efforts would protect the plant to 1,010–1,012 feet (310–308 m) feet above sea level.



and the Cooper Nuclear Power Station near Brownville, Nebraska, are threatened by rising flood waters. Officials have issued a "notification of unusual event" for both plants, but an official from the Omaha Public Power District stated that "a Fukushima event will not occur at Fort Calhoun." According to the Army Corps of Engineers, "the Missouri River would not go above 1,008 feet (307 m) above sea [Furthermore,] officials indicated the spent fuel pool [at the Fort Calhoun Nuclear Power Station] is at 1,038.5 feet (316.5 m) above sea level." More via the The Plattsmouth Journal: The bloated Missouri River rose to within 18 inches of forcing the shutdown of a nuclear power plant in southeast Nebraska but stopped and ebbed slightly Monday, after several levees in northern Missouri failed to hold back



#### the surging waterway.

The Columbus-based utility sent a "notification of unusual event" to the Nuclear Regulatory Commission when the river rose to 899 feet early Sunday morning. The declaration is the least serious of four emergency notifications by the Omaha Public Power District, is about 20 miles north of Omaha. It issued a similar alert to the regulatory commission June 6. The river has risen at least 1.5 feet higher than Fort Calhoun's 1,004-foot elevation above sea level. The plant can handle water up to 1,014



established by the federal commission.

The nuclear plant has been preparing for the flooding since May 30. More than 5,000 tons of sand has been brought in to construct barricades around it and access roads, according to NPPD.

The Army Corps of Engineers said the river level at Brownville had surged about 2 feet from Saturday morning to Sunday morning and that it continued to rise because of heavy rain on the Nishnabotna River, which flows into the Missouri River from Iowa, and due to some erosion along a levee upstream at Hamburg, Iowa, that created a water pulse.

The Cooper Nuclear Station is one of two plants along the Missouri River in eastern Nebraska. The Fort Calhoun Station, operated feet, according to OPPD. The water is being held back by a series of protective barriers, including an 8-foot rubber wall outside the reactor building.

Its reactor already had been shut down for refueling and maintenance since April, and it won't be turned on again until the flooding subsides.

The entire plant still has full electrical power for safety systems, including those used to cool radioactive waste. It also has at least nine backup power sources.

A spokesman for the Nuclear Regulatory Commission said the NRC thinks OPPD managers have "done everything that they need to do to respond to the current conditions" at the nuclear plant.

#### Jellyfish force Torness nuclear reactor shutdown

Source: http://www.bbc.co.uk/news/uk-scotland-edinburgh-east-fife-13971005

Both reactors at the Torness nuclear power station have been shut down after huge numbers of jellyfish were found in the sea water entering the plant. The jellyfish were found obstructing cooling water filters on Tuesday. The East Lothian plant's operator, EDF Energy, said the shutdown was a precautionary measure and there was never any danger to the public.



A clean-up operation is under way, but it is understood it could be next week before Torness is operational again.

Torness has two Advanced Gas Cooled

Tuesday afternoon. It is not known why there are so many jellyfish in the area.

Water temperatures along the east coast of Scotland have been relatively normal, but it is



Reactors but also relies on supplies of sea water to ensure it operates safely. It has filters which are designed to prevent seaweed and marine animals entering the cooling system.

these If screens become clogged, the reactors are shut down to comply with safety procedures. An EDF spokesman told BBC Scotland: "At no time was there any danger to the public. There are no radiological aspects associated with this event and there has been no impact to the environment." Staff at the plant took

the decision to shut down the reactors on rescued from EDF Energy's Hinkley Point nuclear power station in Somerset after it got trapped in the inflow area chasing fish. The plant's operations were not affected.



EDITOR'S COMMENTS: (1) Guess what? The unexpected always happens! (2) Just observing the photo - it does look like Fukushima, isn't it? I mean the protection from sea waves does not look adequate... On the other hand: a tsunami in Scotland? Of course it will not happen to them!

thought higher

the North Sea be

Operations at nuclear power plants in Japan

large numbers of jellyfish in recent years. Earlier

average temperatures

in

а

been

by

this

an

Grey

was

than

may

factor.

have

month,

Seal

Atlantic

disrupted

elsewhere

#### Is NATO using dirty bombs in Libya?

Source:http://www.globalpost.com/dispatches/globalpost-blogs/the-casbah/nato-libya-dirty-bombs-depleted-uranium

When Libyan rebels requested NATO air support to help them in their fight against Libyan leader Muammar Gaddafi, they might have gotten more than they bargained for, and might be paying for it for a long time to come. Several scattered reports released since the conflict began claim that some of the missiles NATO jets are using to disable Gaddafi's army are tipped with depleted uranium, a toxic heavy metal that could have long-term negative health effects on populations exposed to it.



A French Navy firefighter looks on as he walks past a Rafale jet fighter on the flight deck of the Charles de Gaulle aircraft carrier on April 21, 2011 during NATO operations off the coast of Libya. (Alexander Klein/AFP/Getty Images)

British and American troops returning from Iraq during both the first and second Gulf wars, during which such missiles were often used, had to be tested for exposure to the toxic metal.

Depleted uranium is what is left over after enriched uranium, which is used in nuclear fuel and weapons, is extracted from natural uranium. Although depleted uranium has a low level of radioactivity, it is still toxic.

The United States, United Kingdom and a dozen other countries use missiles tipped with depleted uranium. They do this not because of its radioactivity but because of its density. A shell tipped with depleted uranium, which is very heavy, has a huge amount of momentum and can rip through a tank — for example — with ease.

It was Gaddafi's tanks that posed the biggest

problem for the rebels in the early days of the conflict.

Such missiles are good for more than just breaking through steel. Once the missile pierces the armor of its target, the depleted uranium then disintegrates and starts to burn. So a strike on a tank would likely burn its crew alive. When the dust settles, so does the depleted uranium, which has a half life of 4.4 billion years. Former U.S. congresswoman and

presidential candidate Cynthia McKinney, who is fiercely anti-war

and traveled to Libya in June, has said that she found evidence of the use of depleted uranium at hospitals she visited.

A report on Wednesday by the Centre for Research on Globalization says measurements conducted at bomb sites showed higher than normal levels of uranium, citing scientists inside Libya. The use of depleted uranium in weapons might be questionable, but it is not illegal. The International Court of Justice ruled in 1996 that only weapons that use toxic or radioactive metals for the purpose of poisoning or asphyxiating are illegal. Depleted uranium, however, is simply used for blowing stuff up. So it's okay

# **Depleted Uranium Found in Libya by Scientists**

#### By Mahdi Darius Nazemroaya

Source: http://www.globalresearch.ca/index.php?context=va&aid=25510



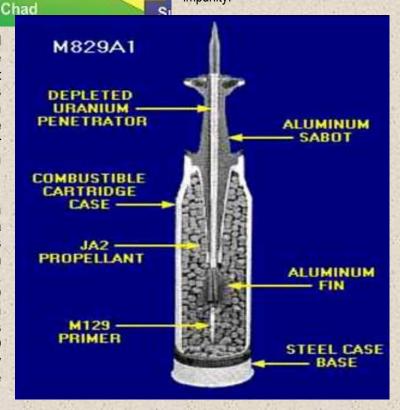
Bombed sites in Libya have been visited by professional scientists working in the Surveying and Collecting Specimens and Laboratory Measuring Group. The scientists and trained



Bab Al-Azizia and Souk Al-Ahad. The teams of scientists have found it hard to conduct their important work during the NATO bombings. They have put their health in

jeopardy and their lives at risk. Moreover, many of these sites have been bombed numerous times and again on different days. This adds an extra dimension of danger to the teams.

The U.S. and NATO are using "dirty bombs" in Libya. These are the countries that claim that Iran and Syria are attempting to make nuclear weapons. So far, however, it is these very same countries that are using weapons of mass destruction (WMD) and use nuclear technology in an irresponsible and criminal manner. An international war crimes tribunal is in order. The Obama Administration, Nicolas Sarkozy, David Cameron, and NATO cannot be allowed to stand with impunity.



Examples of bombed civilian structures:

experts have conducted field

surveys looking for radioactive isotopes (radioisotopes) at bombed sites. The samples

from these sites were then

scientifically analyzed at the

laboratories of the Nuclear Energy Institution of the Libyan

Analysis in Libya through inductively coupled plasma has shown that several sites

contain even higher than

expected doses of uranium.

radioactive measurements, as

do the fragments of NATO

ordinance. Sites analyzed by

the teams of scientists include

missiles also have

by

NATO

high

Arab Jamahiriya.

Holes caused





© Mahdi Darius Nazemroaya, CRG and Réseau Voltaire, 2011.

Mahdi Darius Nazemroaya is a Research Associate for the Centre for Research on Globalization (CRG). He is currently in Libya as an international observer and member of an international group of journalists and writers from Europe, North America and the Middle East.

# **Depleted uranium**

# Fact sheet N°257

Revised January 2003 Source: http://www.who.int/mediacentre/factsheets/fs257/en/

# World Health Organization

#### Uranium

- Metallic uranium (U) is a silver-white, lustrous, dense, weakly radioactive element. It is
  ubiquitous throughout the natural environment, and is found in varying but small amounts in
  rocks, soils, water, air, plants, animals and in all human beings.
- Natural uranium consists of a mixture of three radioactive isotopes which are identified by the mass numbers 238U (99.27% by mass), 235U (0.72%) and 234U (0.0054%).
- On average, approximately 90 µg (micrograms) of uranium exists in the human body from normal intakes of water, food and air. About 66% is found in the skeleton, 16% in the liver, 8% in the kidneys and 10% in other tissues.
- Uranium is used primarily in nuclear power plants. However, most reactors require uranium in which the 235U content is enriched from 0.72% to about 1.5-3%.

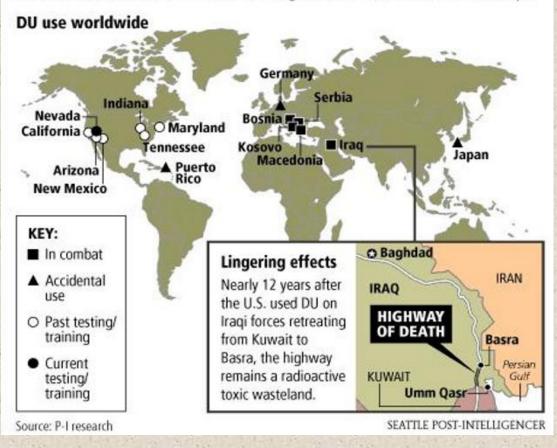
#### **Depleted uranium**

- The uranium remaining after removal of the enriched fraction contains about 99.8% 238U, 0.2% 235U and 0.001% 234U by mass; this is referred to as depleted uranium or DU.
- The main difference between DU and natural uranium is that the former contains at least three times less 235U than the latter.
- DU, consequently, is weakly radioactive and a radiation dose from it would be about 60% of that from purified natural uranium with the same mass.
- The behaviour of DU in the body is identical to that of natural uranium.
- Spent uranium fuel from nuclear reactors is sometimes reprocessed in plants for natural uranium enrichment. Some reactor-created radioisotopes can consequently contaminate the solution.

reprocessing equipment and the DU. Under these conditions another uranium isotope, 236U, may be present in the DU together with very small amounts of the transuranic elements plutonium, americium and neptunium and the fission product technetium-99. However, the additional radiation dose following intake of DU into the human body from these isotopes would be less than 1%.

# DEPLETED URANIUM

With another war in Iraq perhaps imminent, scientists and others are expressing concern that the side effects of depleted uranium (DU) munitions – still a major part of the U.S. arsenal – will result in serious illnesses or deaths to a new generation of U.S. soldiers as well as Iraqis.



#### Applications of depleted uranium

- Due to its high density, about twice that of lead, the main civilian uses of DU include counterweights in aircraft, radiation shields in medical radiation therapy machines and containers for the transport of radioactive materials. The military uses DU for defensive armour plate.
- DU is used in armour penetrating military ordnance because of its high density, and also because DU can ignite on impact if the temperature exceeds 600°C.

# Exposure to uranium and depleted uranium

- Under most circumstances, use of DU will make a negligible contribution to the overall natural background levels of uranium in the environment. Probably the greatest potential for DU exposure will follow conflict where DU munitions are used.
- A recent United Nations Environment Programme (UNEP) report giving field measurements taken around selected impact sites in Kosovo (Federal Republic of Yugoslavia) indicates that contamination by DU in the environment was localized to a few tens of metres around impact sites. Contamination by DU dusts of local vegetation and water supplies was found in the environment was localized to a few tens of metres around impact sites.

extremely low. Thus, the probability of significant exposure to local populations was considered to be very low.

- A UN expert team reported in November 2002 that they found traces of DU in three locations among 14 sites investigated in Bosnia following NATO airstrikes in 1995. A full report is expected to be published by UNEP in March 2003.
- Levels of DU may exceed background levels of uranium close to DU contaminating events. Over the days and years following such an event, the contamination normally becomes dispersed into the wider natural environment by wind and rain. People living or working in affected areas may inhale contaminated dusts or consume contaminated food and drinking water.
- People near an aircraft crash may be exposed to DU dusts if counterweights are exposed to
  prolonged intense heat. Significant exposure would be rare, as large masses of DU
  counterweights are unlikely to ignite and would oxidize only slowly. Exposures of clean-up and
  emergency workers to DU following aircraft accidents are possible, but normal occupational
  protection measures would prevent any significant exposure.

#### Intake of depleted uranium

- Average annual intakes of uranium by adults are estimated to be about 0.5mg (500 µg) from ingestion of food and water and 0.6 µg from breathing air.
- Ingestion of small amounts of DU contaminated soil by small children may occur while playing.
- Contact exposure of DU through the skin is normally very low and unimportant.
- Intake from wound contamination or embedded fragments in skin tissues may allow DU to enter the systemic circulation.

#### Absorption of depleted uranium

- About 98% of uranium entering the body via ingestion is not absorbed, but is eliminated via the faeces. Typical gut absorption rates for uranium in food and water are about 2% for soluble and about 0.2% for insoluble uranium compounds.
- The fraction of uranium absorbed into the blood is generally greater following inhalation than following ingestion of the same chemical form. The fraction will also depend on the particle size distribution. For some soluble forms, more than 20% of the inhaled material could be absorbed into blood.
- Of the uranium that is absorbed into the blood, approximately 70% will be filtered by the kidney and excreted in the urine within 24 hours; this amount increases to 90% within a few days.

#### Potential health effects of exposure to depleted uranium

- In the kidneys, the proximal tubules (the main filtering component of the kidney) are considered to be the main site of potential damage from chemical toxicity of uranium. There is limited information from human studies indicating that the severity of effects on kidney function and the time taken for renal function to return to normal both increase with the level of uranium exposure.
- In a number of studies on uranium miners, an increased risk of lung cancer was demonstrated, but this has been attributed to exposure from radon decay products. Lung tissue damage is possible leading to a risk of lung cancer that increases with increasing radiation dose. However, because DU is only weakly radioactive, very large amounts of dust (on the order of grams) would have to be inhaled for the additional risk of lung cancer to be detectable in an exposed group. Risks for other radiation-induced cancers, including leukaemia, are considered to be very much lower than for lung cancer.
- Erythema (superficial inflammation of the skin) or other effects on the skin are unlikely to occur even if DU is held against the skin for long periods (weeks).
- No consistent or confirmed adverse chemical effects of uranium have been reported for the skeleton or liver.
- No reproductive or developmental effects have been reported in humans.





Although uranium released from embedded fragments may accumulate in the central nervous

system (CNS) tissue, and some animal and human studies are suggestive of effects on CNS function, it is difficult to draw firm conclusions from the few studies reported.

# Maximum radiation exposure limits and their limited application to uranium and depleted uranium

The International Basic Safety Standards, agreed by all applicable UN agencies in 1996, provide for radiation dose limits above normal background exposure levels.

- The general public should not receive a dose of more than 1 millisievert (mSv) in a year. In special circumstances, an effective dose of up to 5 mSv in a single year is permitted provided that the average dose over five consecutive years does not exceed 1 mSv per year. An equivalent dose to the skin should not exceed 50 mSv in a year.
- Occupational exposure should not exceed an effective dose of 20 mSv per year averaged over five consecutive years or an effective dose of 50 mSv in any single year. An equivalent dose to the extremities (hands and feet) or the skin should not surpass 500 mSv in a year.
- In case of uranium or DU intake, the radiation dose limits are applied to inhaled insoluble uranium-compounds only. For all other exposure pathways and the soluble uranium-compounds, chemical toxicity is the factor that limits exposure.

#### Guidance on exposure based on chemical toxicity of uranium

WHO has guidelines for determining the values of health-based exposure limits or tolerable intakes for chemical substances. The tolerable intakes given below are applicable to long-term exposure of the general public (as opposed to workers). For single and short-term exposures, higher exposure levels may be tolerated without adverse effects.

 The general public's intake via inhalation or ingestion of soluble DU compounds should be based on a tolerable intake value of 0.5 µg per kg of body weight per day. This leads to an air concentration of 1 µg/m3 for inhalation, and about 11 mg/y for ingestion by the average adult.



- Insoluble uranium compounds with very low absorption rate are markedly less toxic to the kidney, and a tolerable intake via ingestion of 5 µg per kg of body weight per day is applicable.
- When the solubility characteristics of the uranium compounds are not known, which is often the
- case in exposure to DU, it would be prudent to apply 0.5 µg per kg of body weight per day for ingestion.

#### Monitoring and treatment of exposed individuals

- For the general population, neither civilian nor military use of DU is likely to produce exposures to DU significantly above normal background levels of uranium. Therefore, individual exposure assessments for DU will normally not be required. Exposure assessments based on environmental measurements may, however, be needed for public information and reassurance.
- When an individual is suspected of being exposed to DU at a level significantly above the normal background level, an assessment of DU exposure may be required. This is best achieved by analysis of daily urine excretion. Urine analysis can provide useful information for the prognosis of kidney pathology from uranium or DU. The proportion of DU in the urine is determined from the 235U/238U ratio, obtained using sensitive mass spectrometric techniques.
- Faecal measurement can also give useful information on DU intake. However, faecal excretion
  of natural uranium from the diet is considerable (on average 500 µg per day, but very variable)
  and this needs to be taken into account.
- External radiation measurements over the chest, using radiation monitors for determining the amount of DU in the lungs, require special facilities. This technique can measure about 10 milligrams of DU in the lungs, and (except for souble compounds) can be useful soon after exposure.
- There are no specific means to decrease the absorption of uranium from the gastrointestinal tract or lungs. Following severe internal contamination, treatment in special hospitals consists of the slow intravenous transfusion of isotonic 1.4 % sodium bicarbonate to increase excretion of uranium. DU levels in the human, however, are not expected to reach a value that would justify intravenous treatment any more than dialysis.

#### Recommendations

- Following conflict, levels of DU contamination in food and drinking water might be detected in affected areas even after a few years. This should be monitored where it is considered there is a reasonable possibility of significant quantities of DU entering the ground water or food chain.
- Where justified and possible, clean-up operations in impact zones should be undertaken if there are substantial numbers of radioactive projectiles remaining and where qualified experts deem contamination levels to be unacceptable. If high concentrations of DU dust or metal fragments are present, then areas may need to be cordoned off until removal can be accomplished. Such impact sites are likely to contain a variety of hazardous materials, in particular unexploded ordnance. Due consideration needs to be given to all hazards, and the potential hazard from DU kept in perspective.
- Small children could receive greater exposure to DU when playing in or near DU impact sites. Their typical hand-to-mouth activity could lead to high DU ingestion from contaminated soil. Necessary preventative measures should be taken.
- Disposal of DU should follow appropriate national or international recommendations.

#### Gates and tactical nuclear weapons in Europe

Source:http://www.thebulletin.org/web-edition/op-eds/parting-words-gates-and-tactical-nuclear-weapons -europe



In a recent speech in Brussels, departing Defense Secretary Robert Gates criticized European members of NATO for allowing

#### **Article Highlights**

- In June 2011 departing Defense Secretary Robert Gates decried NATO members for not bearing a greater share of the alliance defense burden.
- Gates argued that the present challenge in Europe involves deciding how "limited (and dwindling) resources are allocated and for what priorities."
- US tactical nuclear weapons in Europe provide a capability for a threat that no longer exists at a financial and opportunity cost that can no longer be justified.

defense obligations to fall increasingly upon the United States, continuing a funding imbalance that could lead Americans to question whether the costs of NATO are justified.

This is not the first time Gates that has expressed his exasperation with NATO allies for not spending more on defense, nor is he the first defense secretary to articulate such sentiments. But never has a secretary of defense been more blunt or direct in his criticism -- and by addressing the NATO funding issue SO prominently, Gates also raised questions about US nuclear policy in Europe.

Though it was likely not their intent, Gates's remarks beg a reconsideration of the logic and feasibility of the continued deployment of nearly 200 US "tactical" nuclear bombs -- low-yield warheads intended for short-range applications or even battlefield use -- in five NATO member states: Belgium, Italy, Turkey, Germany, and the Netherlands. If NATO burden-sharing is out of whack generally, it no longer makes sense in regard to these aging weapons, which US military officials

increasingly believe serve no vital military purpose.

US nuclear weapons in Europe. In his speech, Gates forecast a "dim, if not dismal" future for the alliance should European members continue to enjoy their benefits without sharing "the risks and the costs." He pointed to the NATO operation in Libya as an example of European underfunding, saying, "the mightiest military alliance in history is only 11 weeks into an operation against a poorly armed regime. ... Yet many allies are beginning to run short of munitions, requiring the US, once more, to make up the difference."

Fiscal, political, and demographic realties have restrained the capabilities -- and shrunk the defense budgets -- of many European nations, a point that Gates recognized by saying the present challenge involves deciding how "limited (and dwindling) resources are allocated



and for what priorities."

The priority now given to tactical nuclear weapons in Europe is not just open to question -- it is being questioned. US military leaders increasingly suggest that the deployment of tactical B61 nuclear bombs in Europe serves no military purpose. When asked last year if there is a military mission performed by US tactical nuclear weapons in Europe that cannot be performed by either US strategic or conventional forces, Gen. James Carburght

vice chairman of the Joint Chiefs of Staff, flatly said: "No."

Moreover, political leaders in a growing number of NATO member states, including host nations such as Germany and Belgium, have called for the removal of the weapons. Due in part to the differences that emerged over nuclear weapons policy during the formulation of NATO's 2010 Strategic Concept, the alliance is just beginning a year-long deterrence and defense posture review that, among other things, will consider the "appropriate mix" of nuclear, conventional, and missile defense forces for NATO, including the role of US tactical nuclear weapons in Europe.

One of the main justifications for keeping these weapons in Europe is that they allow NATO members to participate in shaping alliance nuclear policy. In this view, transatlantic ties are strengthened when the risks and costs of deploying and securing nuclear weapons are shared between the US and the respective host nations.

But this burden-sharing agreement appears to be coming undone in both political and practical terms.

The 2008 final report of the Air Force Blue Ribbon Review of Nuclear Weapons Policies and Procedures concluded that host nation security at "most sites" in Europe where US nuclear weapons are deployed do not meet the Defense Department's security requirements. An alarming illustration of these shortcomings occurred in early 2010, when a group of Belgian peace activists penetrated the Kleine Brogel Air Base, which is believed to house 10 to 20 B61 nuclear weapons.

According to some analysts, lax security is a function of politics: Although some European military officials still strongly support the retention of tactical nuclear weapons, political leaders in the host nations do not place a high priority on the nuclear mission, and thus do not make a strong public case for the resources necessary to sustain the mission.

Beyond security and political considerations, the financial costs of continuing the European deployment are likely to be significant for both the US and host nations, even as the global financial situation continues to constrain defense spending. The US National Nuclear Security Administration has begun a \$4 billion program to refurbish and extend the life of the B61 bomb. A recent Government Accountability Office report concluded that the broad scope of the program, which involves the study of features and designs untried during prior life extension programs, could result in a significant schedule delay.

Meanwhile, the host nations are faced with costly decisions about whether to modernize soon-to-be-obsolete, nuclear-capable aircraft. Germany is faced with the most immediate decision, as its Tornado IDS aircraft are scheduled to be retired in 2015. According to one estimate, Berlin would need to spend as much as €300 million to make new German Eurofighters nuclear-capable, a decision that would have to be made within the next two years. The German Air Force has apparently developed an interim option involving the maintenance of a small number of nuclearcapable Tornado aircraft beyond 2015, but this fix is not expected to last much beyond 2020 and could be significantly more expensive than making the Eurofighter capable of carrying a nuclear bomb. Italy, the Netherlands, and Belgium will soon be faced with similar decisions about replacing their Tornados and F-16s and could opt to replace their nuclearcapable aircraft with a nuclear-capable version of the new F-35 multi-use fighter, which has been plaqued by cost overruns and schedule delays.

Matching capabilities to threats. US tactical nuclear weapons in Europe provide a capability for a threat that no longer exists at a financial and opportunity cost that can no longer be justified.

The original rationale for deploying tactical nuclear weapons in Europe was to deter a Soviet conventional attack on Western Europe. This threat disappeared when the Soviet Union disintegrated in the early 1990s. In fact, the continued storage of tactical nuclear weapons at multiple bases in Europe increases the risk that they could be targeted for theft or sabotage by terrorists. The presence of these weapons also provides Russia with a convenient excuse to refuse to talk about its enormous non-strategic arsenal.

Given shrinking NATO defense budgets, alliance members should invest in capabilities (helicopters, transport planes, surveillance aircraft, etc.) that comport with NATO's contemporary security environment, which includes the ongoing campaigns in Afghanistan and Libya, missile defense, terrorism, cyber defense and energy security. Investments in making new aircraft nuclear-capable would draw scarce resources from military and intelligence missions far more critical to NATO's security.

The longer NATO puts off a collective decision about removing tactical nuclear weapons, the greater the odds that financial and political realities in Europe could force changes to alliance nuclear policy under circumstances not of its own choosing. For example, if the German parliament decides not to fund a nuclear capability for the Eurofighter -- a distinct possibility given the current economic climate -- the other host nations will find it difficult to pursue their own modernization programs. This could lead to a situation where the weapons are removed in a disorganized fashion, undermining alliance cohesion and effectiveness.

For all these reasons, the US should begin a consultative process with its NATO allies to ultimately remove the remaining tactical nuclear weapons in Europe. This will require that NATO think creatively about how it can best deter Russia and possible emerging nuclear threats in the future in the absence of forward-deployed tactical nuclear weapons. And this is a type of creativity the alliance can't thrive without.

# A Citizen's Radiation Dosimeter That Fits In The Wallet

Source: http://www.medicalnewstoday.com/releases/230327.php

No matter how many plastic cards currently crowd your wallet, one day you may wish to make room for one more. The Department of Homeland Security(DHS)'s Science and Technology Directorate (S&T) has developed a miniaturized version of a dosimeter, a portable device used for measuring exposure

to ionizing radiation, which can provide life-saving early detection in the unlikely event of a nuclear accident or dirty bomb. Dubbed the Citizen's Dosimeter, this high-tech plastic card would be as convenient and affordable as a subway card, with the capability to measure the

amount of radiation on a person or in a given area.

The National Urban Security Technologies Laboratory (or NUSTL, pronounced new STEEL) located in New York City and managed by DHS S&T, has been awarded a patent that covers the development of radiation dosimetry technologies - DHS's first patent. Currently, personal radiation dosimeter badges are worn in nuclear plants, but a plant individual's radiation dose. While a final prototype has not yet been built, a workable blueprint for a wallet-sized card that can detect radiation in real time is now in place. "We were inspired by the Metro cards we use every day to get around Manhattan, and

dosimeter cannot be read on the spot; it must

be sent to a processing lab to determine an

and envisioned a dosimeter with that level of convenience," savs Gladys Klemic, a NUSTL physicist who managed the project from Illinois. Klemic believes а dosimeter in this form could benefit both

emergency responders and the general public.

Klemic and her team at NUSTL set out to create a dosimeter that would meet American National Standards Institute (ANSI) requirements for personal radiation dosimeter badges, and incorporate commercially available components to decrease the size and lower the price tag.



NUSTL began by using radiation-sensitive material from Landauer, Inc., a commercial dosimetry provider in Illinois, testing materials of varying thicknesses and combinations to determine how thin they could make the card while still achieving the targeted performance. After testing nearly a half a dozen materials, the NUSTL scientists determined that using the chemical element tantalum allowed them to obtain accurate readings with minimal thickness. Combining this element in a unique double-layer, stainless steel filter helped to reduce false positives. It was this unique design that led to the patent award.

The next step is to develop a card reader to reveal the radiation dose measured by the Citizen's Dosimeter. In the event of a nuclear incident, first responders equipped with a card reader would immediately be able to measure radiation exposure for anyone carrying the Citizen's Dosimeter. While it will be years before a card and reader can be prototyped, tested, certified and wallet-ready, NUSTL has lined up a team to support the effort, including:

- Engineers at StorCard, a Californiabased group that has previously developed a prototype credit-card floppy disk and reader
- Nomadics, an Oklahoma engineering firm
- Radiation detection experts at Landauer and Oklahoma State University

The Citizen's Dosimeter represents a technological breakthrough and the next generation in radiation detection. It also demonstrates how public-private partnerships can work to produce life-saving solutions - in this case, protecting the nation from radiation resulting from an act of terrorism or natural disaster.

# Strong reactions to assassination of another Iranian scientist

Source: http://www.terrorism-info.org.il/site/home/default.asp

This week Iranian top officials and media voiced anger over the assassination of another Iranian scientist last week. In the first several hours after the assassination, the Iranian media released conflicting reports on the



identity of the scientist. Initial reports said that the victim was Daryush Reza'i, a nuclear scientist and physics professor in Ardabil University (northwestern Iran). Several hours later some news agencies reported that the victim was Daryush Reza'inejad, an Electronic Engineering Ph.D student from Tehran's Khajeh Nasireddin Tousi University, who was not involved with the nuclear program in any way.

The Iranian scientist minutes after the assassination, from www.nasimonline.ir

Senior Iranian officials voiced strong reactions to the assassination of the scientist. Majles speaker Ali Larijani blamed it on Israel and the U.S., saying that it was yet another example of the hostility faced by Iran from the U.S (ISNA, July 24).

Tehran's governor Morteza Tamadon also blamed the U.S. and Israel for the assassination of Reza'inejad, referring to it as an "American-Israeli project". Speaking at the scientist's funeral, Tamadon said that the assassinations of Iranian scientists are aimed to harm the Iranian people and turn them from the path of technological progress, but have the opposite effect (Mehr, July 24).

Basij chief Mohammad Reza Naqdi claimed that the U.S. and Israel are behind, the assassination, and announced that the parts way to deal with the assassinations of scientists and restore Iran's security is to wipe "the Zionist regime" from history (ISNA, July 25).



Daryush Reza'inejad's funeral

The Iranian press also reacted sharply to the third assassination of an Iranian scientist in two years. According to the daily Tehran Emrouz, the assassination is indicative of a change in the tactics employed by Iran's enemies to contend with its scientific progress. The enemies of Iran have come to realize that a military attack on Iran's nuclear facilities will have no effect on Iran's determination and eagerness for scientific progress, and that Iran's retaliation will have devastating effects. They also understand that a military action will at best delay the nuclear program for several weeks, just as the Iraqi attacks on the Iranian oil facilities during the Iran-Irag War did no significant damage to the petroleum industry. It was this understanding that brought about Iranian enemies' decision to assassinate Iranian scientists. Training scientists takes many years and considerable resources, and the enemy is trying to impede Iran's technological progress by assassinating them. Protecting the lives of experts and scientists has therefore become a task of high importance. The enemies of Iran should know that the Muslim nations of the region, particularly the Iranians, will avenge these crimes and assassinations. It is still too early to tell how Iran will react, but a reaction will definitely be coming. At any rate, Iran must continue working towards its scientific objectives (Tehran Emrouz, July 24).

The daily Arman also said that the assassinations of Iranian scientists cannot be allowed to go on unchecked. An article by Majles member Daryush Qanbari titled "Where is the problem?" criticized the Iranian security

services' inability to deal with the assassinations of the scientists and the escalating violence in society. It is unacceptable to sit idly by while these incidents take place, the Majles member said, and it is necessary to determine how they take place in broad daylight (Arman, July 24).

The conservative daily Khorasan also indicated a connection between the assassinations of Iranian scientists on one hand and progress of Iran's nuclear program and nuclear talks with the West on the other. The daily argued that, due to the fact that a military attack by the U.S. and its allies on Iran's nuclear facilities is unfeasible, and due to the failure of the economic sanctions against Iran, the West is using other means to compromise the nuclear program. The elimination of experts and scientists involved with the nuclear program is considered by the West a warning for Iran, but such actions only show how important it is for Iran to obtain nuclear technology. The fact that Iran's enemies are willing to carry out such actions to keep it from the realization of its capabilities only stresses the need for Iran's vigorous pursuit of its nuclear activities (Khorasan, July 24).

The Ayandeh website discussed Iran's failure to deal with the Israeli Mossad's infiltration into Iran. The website compared the failed attempt on the life of the Israeli consul in Istanbul, which the Israeli media attributed to Iran, and the successful assassination supposedly carried out by the Mossad in the center of Tehran. The website recommended a series of measures to prevent the Mossad from carrying out further operations: strengthening the Ministry of Intelligence, compromised by President Ahmadinejad's attempt to remove the intelligence minister from office several months ago; using the several months it will take the Mossad to prepare for additional actions to interfere with its activity; relocating Mossad's potential targets to safe houses and putting them under tighter security; and introducing changes in the counter-activities conducted by the Iranian intelligence to improve its ability to deal with the Mossad's infiltration. Such changes include setting up surveillance cameras in cities, offering rewards for information leading to the arrest of terrorists, stepping up monitoring of suspicious movements in countries which Mossad operatives may use to cross into Iran (such as Turkey, Azerbaijan, Thailand, and the UAE

and filing complaints against Israel with such international institutions as Interpol and the

international tribunal in The Hague (Ayandeh News, July 25).

# China developing EMP weapons

Source:http://www.upi.com/Science\_News/2011/07/22/Report-China-developing-EMP-weapons/UPI-10561311362279/?spt=hs&or=sn

China is developing electromagnetic pulse weapons Beijing could use against U.S. aircraft carriers in any future conflict over Taiwan, a U.S. report says.

The EMPs are part of China's so-called "assassin's mace" arsenal to allow a technologically inferior China to defeat U.S. military forces, the report by the National Ground Intelligence Center said. EMPs mimic a gamma-ray pulse caused by a nuclear blast and can disable all electronics, including computers and automobiles, over wide areas.

"For use against Taiwan, China could detonate at a much lower altitude (30 to 40 kilometers) ... to confine the EMP effects to Taiwan and its immediate vicinity and minimize damage to electronics on the mainland," the report said.



The declassified 2005 intelligence report provides details on China's EMPs and plans for their use, The Washington Times reported Friday. Chinese military writings have discussed building low-yield EMP warheads but "it is not known whether [the Chinese] have actually done so," the report concluded.

Funding To Develop Crystals For Detecting Nuclear Threats Source: http://www.medicalnewstoday.com/releases/231216.php



Using a crystal ball to protect homeland security might seem far-fetched, but researchers at Wake Forest University and Fisk University have partnered to develop crystals that can be used to detect nuclear threats, radioactive material or chemical bombs more accurately and affordably.

The research is made possible by a \$900,000 grant from the Office of Nuclear Nonproliferation Research and Development of the National Nuclear Security Administration, within the U.S. Department of Energy. The grant will support both universities' continued research in the area of radiation detection, which ultimately could lead to improved detector devices for screening cargo containers at ports, airports and border crossings. It would detect trace amounts of radioactive or chemical material - similar to a CT scan or PET scan detecting a tumor in the human body - and lead to better medical diagnostics. "This grant is an acknowledgement of Fisk and Wake Forest's excellence and leadership in the field of radiation detection research," said Fisk University Professor of Physics and Vice Provost Arnold Burger.

Researchers at Fisk and in national laboratories previously discovered that strontium iodide crystals doped with europium are able to detect and analyze radiation better than most other detection materials. Wake Forest researchers recently demonstrated the unexpectedly crucial role of specific parameters - electron and hole mobilities needed to predict the best energy resolution of a given detector crystal.

Currently, expense is an issue because of the large quantities of the crystalline material ultimately needed for widely deployed screening devices. However, strontium iodide already performs much better than the most affordable detectors currently used, and the scientists are optimistic that with the right calculations and adjustments, crystals of the needed quality and size can be grown and produced affordably. "Unexpected radiation situations are a fact of our modern world," said Dr. Richard Williams, Professor of Physics at Wake Forest. "By improving radiation detection and diagnostics, our research will benefit medical advancement as well as international security."

# New radiation detector unveiled, does not rely on helium-3

Source:http://www.homelandsecuritynewswire.com/new-radiation-detector-unveiled-does-not-rely-helium-3

Princeton Security Technologies, Inc. appears to have a solution to the quickly dwindling helium-3 stockpiles; on Tuesday the company announced that it had developed and delivered the first commercially available nuclear materials detector that does not rely on helium-3

Princeton Security Technologies, Inc. appears to have a solution to the quickly dwindling helium-3 stockpiles. On Tuesday the company announced that it had developed and delivered the first commercially available nuclear materials detector that does not rely on helium-3.

Demand for radiation detectors has surged as a result of increased efforts to stop nuclear proliferation and terrorism, but production of helium-3, a critical element in nuclear detection technology, has not kept pace and existing stockpiles are quickly dwindling. In response to these shortages, DHS has actively sought to investigate alternatives and explore technologies to recycle helium-3 and extend current supplies. Instead of helium-3, Princeton Security

> Technologies' detector uses sodium iodide for gamma detection and Lithium-6 for neutron monitoring.

> "The new lithium detector configuration now provides a viable, cost effective alternative for our government customers requiring Neutron detection," said Alex Palm, the

company's vice president of marketing. Neutron monitoring has been proven as an effective way to detect terrorists or other malicious actors who seek to obtain radioactive.



materials or use them in a dirty bomb attack. The company has already delivered its new radiation monitors to be used in hospitals and other security surveillance applications.

Princeton Security Technologies Inc. is part of Princeton Gamma-Tech Instruments, Inc.

(PGT), which develops X-ray and Gamma-ray Detectors, Spectroscopy systems, Radiation Detection Area Monitors and Radioactive Radioisotope Identifier products.

## NYPD pioneers system to detect 'dirty bomb'

Source:http://www.todayonline.com/World/EDC110730-0000019/NYPD-pioneers-system-to-detect-dirty-bomb

The New York Police Department (NYPD) is testing ground-breaking counter-terror technology expected to dramatically increase its ability to detect and thwart a potential radiation attack. The technology will allow a command centre in lower Manhattan to monitor 2,000 mobile radiation detectors carried by officers daily around the city. The detectors will send a wireless, real-time alert if there is a reading signalling a "dirty bomb" threat.



A "dirty bomb" - designed to spread panic by using a small explosive to create a radioactive cloud in urban settings - has never been discovered or detonated in a United States terror plot. But enforcement law officials consider them a serious threat because they are easy to build and because of intelligence that foreign terrorists want to use them against US cities. The federal authorities, monitoring tests of the system, are hoping it can be perfected and used

elsewhere. The radiation detection system is being developed as part of a US\$200 million (S\$241 million) lower Manhattan security initiative.

Police say the overall plan was inspired by the "ring of steel" encircling London's business district. However, it is broader in scope and sophistication. The initiative will rely largely on 3,000 closed-circuit security cameras carpeting the roughly 4.4 sq km south of Canal Street, the subway system and parts of midtown Manhattan. So far, about 1,800 cameras are operational, with the rest expected to come on line by the end of the year. The NYPD is also pioneering "video analytic" computer software designed to detect threats, like unattended bags, and retrieve stored images based on descriptions of terror or other criminal suspects.

#### Nuclear safety in Iran, post-Fukushima

Source: http://thebulletin.org/web-edition/op-eds/nuclear-safety-iran-post-fukushima



Although the Fukushima disaster has stalled the ambitions of some developing countries to deploy new power reactors, the Japanese crisis has not seriously affected the expansion of Iran's nuclear energy program. Among the 45 countries that are actively considering plans to build their first power reactors, Iran is farthest along in the process and claims it will connect its Bushehr nuclear power plant to the

#### **Article Highlights**

- Despite the Fukushima disaster, Iran plans to connect its first nuclear power plant to the electrical grid in August.
- Neighboring countries fear a nuclear accident at the Bushehr plant because of its troubled construction history and Iran's high level of seismic activity.
- In public, Iran has vouched for the plant's safety, but internal reports tell a different story, and the IAEA says Iran needs to sign and ratify the Convention on Nuclear Safety and improve its safety processes.

national grid and begin producing electricity in August. Leaders from Gulf Cooperation Council (GCC) countries have consistently expressed fears that a serious nuclear accident at the Bushehr plant, located at the Persian Gulf port city of Bushehr, would spread radiation throughout the region. Indeed, Bushehr is closer to six Arab capitals (Kuwait City, Riyadh, Manama, Doha, Abu Dhabi, and Muscat) than it is to Tehran. And Iran's repeated assurances about the safety of this plant have fallen on deaf ears because of widely reported concerns over the project's 37-year-long construction history and the high level of seismic activity in Iran.

Before the Fukushima disaster, Iranian officials emphatically stated that Iran was following in the footsteps of Japan by developing the full nuclear fuel cycle for peaceful purposes without pursuing a weapons with Japan. The Iranian plateau is one of the most

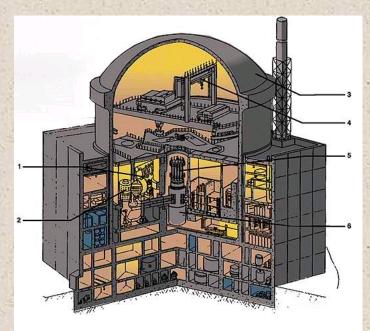


44°E 46°E 48'E 50°E 52°E 54°E 56°E 58°E 60°E 62'E 64°E seismically active areas in the world and has experienced a number of destructive earthquakes in the past century. Iran's nuclear power plants therefore need to be designed and built according to requirements for high seismicity. After the Fukushima disaster began to unfold, the Japanese model became less useful to Iranian officials, who guickly rejected concerns over the safety of the Bushehr plant. As Iran's representative to the SESAME (Synchrotron Radiation Light for Experimental Science and Applications in the Middle East) project and nuclear physicist Seved Mahmoud Reza Aga-Miri told Fars News Agency, "Iranian experts can easily tackle this [Fukushima] disaster and solve Japan's problem. This shows that maybe Iran's practical capabilities are higher than Japan's."

program. But Iran shares other similarities with Japan: The Iranian plateau is one of the most



Energy Organization of Iran (AEOI) under Shah Mohammad Reza Pahlavi, said the Bushehr plant was designed to withstand an earthquake with a 7.0 magnitude and built with a reinforced-concrete containment structure to prevent radioactive release in case of an accident. An earthquake of high magnitude, however, could crack the plant's containment dome or disrupt its electrical supply and keep



the back-up cooling system from working, as occurred at Fukushima. In February 2011, the Bushehr plant was shut down after a broken pump caused contamination of cooling water; the malfunction was blamed on aging equipment supplied by Germany in the 1970s, before Russia undertook the completion contract for the plant in 1995.

In public, Iranian and Russian officials have vouched for the safety of the Bushehr nuclear plant, but the internal view appears to be different. A May 2011 report leaked by Iranian scientists cautioned that seismic danger to Iran could lead to a disaster similar to the meltdown at Fukushima. Also according to media reports, shortly after the

Fukushima disaster, Iranian leadership conducted a review of earthquakes in Iran, which found "incontrovertible risks" of establishing nuclear sites in 20 of Iran's 31 provinces. Supreme Leader Ayatollah Ali Khamenei, however, reportedly disregarded the review's findings.

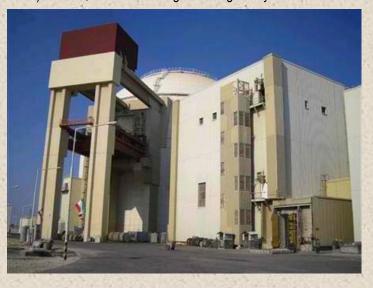


In an interview with the Iranian state-run newspaper Kayhan, Akbar Etemad, the first head of the Atomic

Despite Iranian insistence that the Bushehr plant enjoys the "highest up-to-date standards," the International Atomic Energy Agency (IAEA) emphasizes that Iran does not, in fact, follow some important safety protocols. Iran is the only country in the world with significant nuclear activities not to sign the 1994 Convention on Nuclear Safety (CNS), a crucial system of peer review and mutual oversight. (Israel, India, and Pakistan, all outside the Nuclear Non-Proliferation Treaty, have signed the CNS. India and Pakistan have both ratified.) In 2010, the IAEA's Integrated Regulatory Review Service

(IRRS) mission to the Bushehr plant recommended that Iran develop "a comprehensive system of national nuclear safety regulations," increase the number and expertise of technical staff, and sign the CNS.

On June 21 AEOI head Fereydoun Abbasi indicated that Iran has begun the process for ratifying the CNS but denounced the IAEA for relying on "unlawful" UN Security Council sanctions imposed on Iran's nuclear program, which make it difficult for Iranian experts to obtain visas from countries hosting IAEA nuclear safety meetings.



Nevertheless, Iran has ignored other opportunities for consultation on the safety of the Bushehr plant, including an IAEA offer, since 2002, to send a pre-Operational Safety and Review Team (OSART) mission to evaluate the Bushehr plant. These missions are conducted upon request but routinely carried out for IAEA member states -- and are particularly recommended for nuclear newcomers -- before nuclear power plants begin operation.

Although Bushehr is unlikely to be struck by a tsunami of the size that devastated Fukushima, the world relies on Iran to effectively regulate the Bushehr nuclear plant once it assumes responsibility for the reactor's operation. If Iran wants to minimize the risks of another nuclear disaster, it should immediately sign and ratify the Convention on Nuclear Safety, establish an independent nuclear regulatory authority, and implement all IAEA recommendations to assure the safety of the public and the long-term reliability of what will become the first commercial power reactor in the Middle East.

# Swedish police arrest man for building nuclear reactor in his kitchen

Source: http://www.homelandsecuritynewswire.com/swedish-police-arrest-man-building-nuclear-reactorhis-kitchen

A 31-year old Swede was arrested after authorities discovered he was preparing to build a nuclear reactor in his apartment's kitchen; he already had some radioactive material -- ordered from overseas -- and material acquired by taking apart a domestic fire alarm; he was discovered when he called the



Swedish Radiation Authority to inquire whether it was legal to construct a nuclear reactor at home.

Site of the Swedish kitchen nuclear reactor // Source: geek.com

Swedish police have arrested a 31-year-old man in Ängelholm, a coastal town in western Sweden, after he sought advice from Swedish government agencies on the legality of building a nuclear reactor in his kitchen. The man began his experiment with the idea six months.

ago, and apparently has not kept secret his plans to construct a nuclear reactor in his apartment. He even kept a running blog of his nuclear adventure. The Local reports that the man, who said he was drawn to nuclear physics since he was a teenager, ordered some radioactive material from overseas and acquired more by taking apart a domestic fire alarm.

Law enforcement became aware of the man's activities when, two weeks ago, he contacted the Swedish Radiation Authority (Strålsäkerhetsmyndigheten) to inquire whether it was legal to construct a nuclear reactor at home.

Agency officials told him that someone from the agency would be sent to measure the levels of radiation in his flat. "When they came they had the police with them. I have had a Geiger counter and have not detected a problem with radiation," the 31-year-old told the local Helsingborgs Dagblad (HD).

The police arrested him and took him in for questioning. The police also seized about \$950 worth of equipment. The man said that, in the future, he plans to focus on the "theoretical" aspects of nuclear physics.

# **EMPACT America**, Inc.

Source: http://www.empactamerica.org/about.php



EMPACT America is a bipartisan, non-profit (with IRS 501(c)4 status) organization for citizens concerned about protecting the American People from a nuclear or natural electromagnetic pulse (EMP) catastrophe. Two Congressional Commissions, the EMP Commission and the Strategic Posture Commission, have warned that terrorists, rogue states, China and Russia could, using a single crude nuclear weapon delivered by a primitive missile, inflict an EMP attack that would cause the collapse of critical civilian infrastructures--such as infrastructures for electric power, telecommunications, transportation, banking and finance, food and water--across the entire continental United States, that are vital alike for the sustenance of our modern society and the survival of its citizens.

Moreover, the EMP Commission and the National Academy of Sciences warn that a catastrophic EMP event can also occur naturally, from a great geomagnetic storm, with effects virtually identical to those of a nuclear EMP attack, and that such a storm is inevitable, occurring every century or so. Great geomagnetic storms have occurred in the past, but not since the advent of the modern electronic age. Some scientists estimate that the world is overdue for a great geomagnetic storm, that could occur during the next cycle of solar activity, in 2012.

Fortunately, the EMP Commission, which terminated in 2008, produced a plan that could, within 3-5 years and at modest cost, protect U.S critical infrastructures and the American People from a nuclear or natural EMP catastrophe, and would also mitigate the full spectrum of threats to the critical infrastructures-- including from cyber attack, sabotage, and common natural disasters like hurricanes.

#### EMPACT America has the following missions:

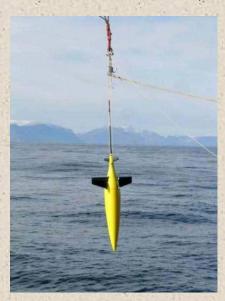
- Re-establish the EMP Commission to advise Congress and the Departments and Agencies of the U.S. government;
- ☑ Implement the EMP Commission recommendations to protect civilian critical infrastructures on an accelerated basis;
- Educate the American People on the EMP threat and solutions; Organize the American People to act effectively in furtherance of their security from the EMP threat at the federal, state, local, and individual levels; and
- ☑ Initiate pilot programs in Western New York State to increase EMP preparedness among first responders, communities, utilities, businesses, and universities, to serve as examples for the

nation, and to show that leadership on national and homeland security need not originate in Washington, that the American People can lead "from the bottom up."

#### Underwater nuke detecting drone

Source: http://www.homelandsecuritynewswire.com/underwater-nuke-detecting-drone

Unmanned underwater vehicles (UUV) could soon be prowling the nation's coastline to detect



radiological and nuclear threats; the underwater drones, developed by New Jersey based Princeton Security Technologies, Inc., are equipped with radiological isotope identification hardware to monitor any changes below the water

Unmanned underwater vehicles (UUV) could soon be prowling the nation's coastline to detect radiological and nuclear threats.

The underwater drones, developed by New Jersey based Princeton Security Technologies, Inc., are equipped with radiological isotope identification hardware to monitor any changes below the water.

The company's iRobot 1KA Seaglider UUV is capable of measuring the ocean's temperature, salinity, and radiation along with other critical data that it beams back to a command center using global satellite telemetry.

So far more than 135 Seagliders have been deployed around the world by governments and militaries including the

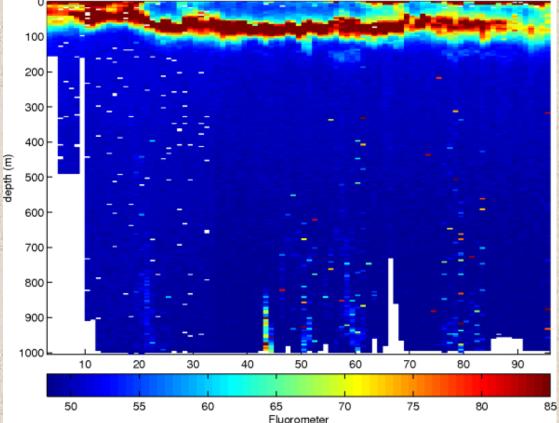
U.S. Navy. "Many nuclear power plants are located along coastlines because they are highly water-intensive,"



states Alex Palm, marketing vice president for Princeton Security Technologies. "Our technology, in."

193

concert with Seaglider, provides the ability to monitor our oceans for increased levels of radiation. This is an important capability given recent world events."



Princeton Security Technologies and its subsidiary Princeton Gamma-Tech Instruments Inc. develop Xray and gamma-ray detectors, spectroscopy systems, and radiation detection area monitors.

#### Cheap radiation detector made of PET resin developed

Source: http://www.homelandsecuritynewswire.com/cheap-radiation-detector-made-pet-resin-developed

Japanese researchers have made a major step toward developing an accurate - and cheap - radiation detector which will allow everyone to have his or her own radiation detector.



Dr. Hidehito Nakamura and Dr. Sentaro Takahashi at Kyoto University Nuclear Reactor Research Institute, Dr. Yoshiyuki Shirakawa at the National Institute of Radiological Sciences. and Mr. Hisayoshi Shimizu at Teijin Chemicals have successfully in developed a revolutionary radiation-sensitive plastic - trademarked "Scintirex" — at one-tenth the cost of current detectors. What is more, the new device outperforms plastic scintillators, important components in radiation detectors that have become widely used by stakeholders in nuclear power plants and first responders.

The new plastic resin developed by the researchers emits a fluorescent glow when exposed to radiation. The resin acts as a sensor within the radiation detectors, allowing measurements of radiation. Inhabitat reports that the new material is derived mainly from PET bottle resin, combining the strength, flexibility, and low cost of the readily

available PET resin with the radiation sensitivity of plastic scintillators, currently the dominant radiation sensing material exported to Japan by French firm Saint-Gobain



#### Figure 1: A radiation measurement element made from hardened PET bottle resin.

We succeeded for the first time in the world to measure radiation ( $\alpha$  rays,  $\beta$  rays,  $\gamma$  rays, and internal conversion electrons) discharged from a radiation source using this measurement element.

A Kyoto University release reports that radiation detectors relying on the new technology will make major contributions to radiation management important to the

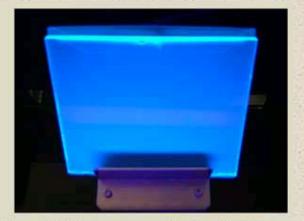
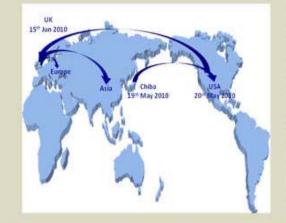


Figure 5: Fluorescence Test on Scintirex Scintirex is visibly glowing bright deep-blue.

nuclear power industry in general, contamination management in far-away locations, and to radiation management at nuclear power plants around the world. The researchers said they expect these detectors to be adopted not only by nuclear power plants, but by 6,000 radiation stations (including hospitals) in Japan. "We



#### Figure 2: A large number of corroborating experiments on PET bottle resin around the world

The day after the thesis was published, a corroborating experiment was conducted by researchers from Berkeley in the US, and a month later the results were announced via British media. (200 or more media publications.)

# **Research Results**

- ✓ We have succeeded in developing a revolutionary radiation-sensitive plastic (trademark "Scintirex") with a performance superior to plastic scintillators currently used for measuring radiation.
- Production is now possible at a greatly reduced cost of less than one-tenth the cost of existing radiation detector products in overseas monopolized markets.
- ☑ We aim to strengthen cooperation among government, industry, and academia and provide people who live near nuclear power plants in Japan and overseas with inexpensive, sturdy personal dosimeters and survey meters for contamination monitoring. At the same time, we will contribute to widespread nuclear power safety activities.

also expect them to answer a demand for inexpensive, high-performance radiation detectors among the general population," the researchers said.

These results of the research were published in the online version of Euro Physics Letters (EPL) on 29 June 2011.



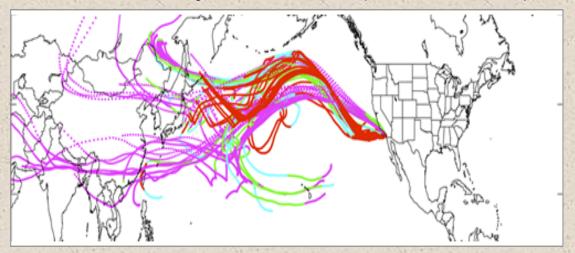
195

#### First quantitative measurements of Fukushima leakage

Source: http://www.homelandsecuritynewswire.com/first-quantitative-measurements-fukushima-leakage

Atmospheric chemists at the University of California, San Diego, report the first quantitative measurement of the amount of radiation leaked from the damaged nuclear transforming the atom to a radioactive form of sulfur.

When the water hit the hot reactors, nearly all of it vaporized into steam. To prevent



reactor in Fukushima, Japan, following the devastating earthquake and tsunami earlier this year.

Their estimate, reported 15 August in the early, online edition of the Proceedings of the National Academy of Sciences (PNAS), is based on a signal sent across the Pacific Ocean when operators of the damaged reactor had to resort to cooling overheated fuel with seawater.

"In any disaster, there's always a lot to be learned by analysis of what happened," said senior author Mark Thiemens, Dean of the Division of Physical Sciences at UC San Diego. "We were able to say how many neutrons were leaking out of that core when it was exposed."

A University of California – San Diego release reports that on 28 March 2011, fifteen days after operators began pumping seawater into the damaged reactors and pools holding spent fuel, Thiemens' group observed an unprecedented spike in the amount of radioactive sulfur in the air in La Jolla, California. They recognized that the signal came from the crippled power plant.

Neutrons and other products of the nuclear reaction leak from fuel rods when they melt. Seawater pumped into the reactor absorbed those neutrons, which collided with chloride ions in the saltwater. Each collision knocked a proton out of the nucleus of a chloride atom, explosions of the accumulating hydrogen, operators vented the steam, along with the radioactive sulfur, into the atmosphere.

In air, sulfur reacts with oxygen to form sulfur dioxide gas and then sulfate particles. Both blew across the Pacific Ocean on prevailing westerly winds to an instrument at the end of the pier at UC San Diego's Scripps Institution of Oceanography where Thiemens' group continuously monitors atmospheric sulfur.

Using a model based on NOAA's observations of atmospheric conditions at the time, the team determined the path air took on its way to the pier over the preceding ten days and found that it led back to Fukushima.

Then they calculated how much radiation must have been released. "You know how much seawater they used, how far neutrons will penetrate into the seawater and the size of the chloride ion. From that you can calculate how many neutrons must have reacted with chlorine to make radioactive sulfur," said Antra Priyadarshi, a post-doctoral researcher in Thiemens' lab and first author of the paper. Gerardo Dominguez, another member of Mark Thiemens's research group, is also an author of the report.

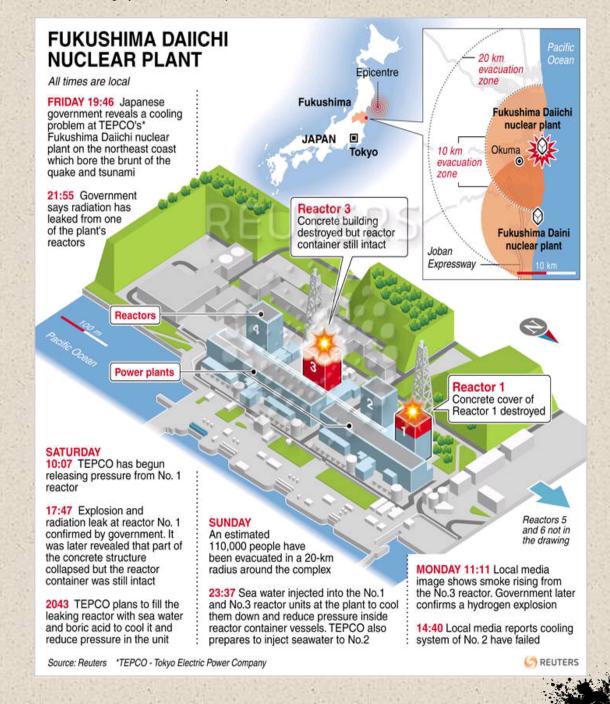
After accounting for losses along the way as the sulfate particles fell into the ocean, decayed, or eddied away from the stream of air heading toward California, the researchers calculated that 400 billion neutrons; were

released per square meter surface of the cooling pools, between 13 March, when the seawater pumping operation began, and 20 March 2011.

The trace levels of radiation that reached the California coast never posed a threat to human health. "Although the spike that we measured was very high compared to background levels of radioactive sulfur, the absolute amount of radiation that reached California was small. The levels we recorded aren't a concern for human health. In fact, it took sensitive instruments, measuring radioactive decay for hours after lengthy collection of the particles, to precisely measure the amount of radiation," Thiemens said.

Concentrations a kilometer or so above the ocean near Fukushima must have been about 365 times higher than natural levels to account for the levels they observed in California.

The radioactive sulfur that Thiemens and his team observed must have been produced by partially melted nuclear fuel in the reactors or storage ponds. Although cosmic rays can produce radioactive sulfur in the upper atmosphere, that rarely mixes down into the layer of air just above the ocean, where these measurements were made.



Over a four day period ending on 28 March, they measured 1,501 atoms of radioactive sulfur in sulfate particles per cubic meter of air, the highest they've ever seen in more than two years of recordings at the site.

Even intrusions from the stratosphere – rare events that bring naturally produced radioactive sulfur toward the Earth's surface – have produced spikes of only 950 atoms per cubic meter of air at this site.

The nuclear reaction within the cooling seawater marked sulfur that originated in a specific place for a discrete period of time. That allowed researchers to time the transformation of sulfur to sulfur dioxide gas and sulfate

#### What next: A Sunni bomb?

#### By Pervez Hoodbhoy

Source: http://thebulletin.org/web-edition/features/what-next-sunni-bomb

The Islamic Republic of Iran stands at the threshold to the bomb. In 2010 it had more than enough low-enriched uranium (some 2,152 kilograms) to make its first bomb's worth of weapons-grade uranium. The LEU would have become highly enriched uranium in roughly 10 weeks had it been fed into the 4,186 centrifuges then operating. Thousands of other centrifuges are also known to be operating at

#### **Article Highlights**

- Pakistan, a Sunni-majority country, secretly helped Shia-dominated Iran with its nuclear weapon program until the 1990s, but even then, some Pakistani elites spoke against such support.
- Shia Iran and Sunni-led Saudi Arabia have become bitter rivals for pre-eminence in the Middle East as Iran has pursued the nuclear option.
- If Iran gets a nuclear bomb, Saudi Arabia will likely try to follow, turning to Pakistan, its longtime Sunni ally, for technological help.

the Natanz secret nuclear facility. Even if Iran had not received a bomb design from the socalled father of Pakistan's nuclear weapons program, A. Q. Khan, the six-decade-old physics of implosion devices would be no mystery to Tehran's sophisticated nuclear scientists. Iran now awaits only a political decision to make the bomb. particles, and measure their transport across the ocean, both important factors for understanding how sulfate pollutants contribute to climate change.

"We've really used the injection of a radioactive element to an environment to be a tracer of a very important process in nature for which there are some big gaps in understanding," Thiemens said.

The event also created a pulse of labeled sulfur that can be traced in the streams and soils in Japan, to better understand how this element cycles through the environment, work that Thiemens and colleagues in Japan have already begun.

What if Iran chooses to cross the threshold? Among other likely consequences, an Iranian bomb would be a powerful stimulus pushing the Kingdom of Saudi Arabia to follow and seek the first Sunni bomb. The first, yes. Though also a Sunni-majority state, Pakistan built its bomb not for Islamic reasons, but to counter India's nuclear arsenal. In fact, Shiite-majority Iran enthusiastically hailed Pakistan's 1998 test of an atomic device. Clearly, the Iranian leadership did not see Pakistan's bomb as a threat.

But Sunni Saudi Arabia sees Shia Iran as its primary enemy. The two are bitter rivals that, post-Iranian revolution, have vied for influence in the Muslim world. Saudi Arabia has the world's largest petroleum reserves, Iran the second. Saudi Arabia is the biggest buyer of advanced US weapons and is run by expatriates. It is America's golden goose, protected by US military might. But fiercely nationalist Iran expelled US oil companies after the revolution and is building its own scientific base.

Both Saudi Arabia and Iran are theocracies, with their respective theologies locked in an irresolvable conflict that began with the death of the Prophet of Islam some 15 centuries ago. Saudi Arabia is Custodian of the Two Holy Mosques and the birthplace of Islam. It is the leader of the Sunni world, culturally conservative, and Arab.

On the other hand, Iran is a Persian, Shiamajority state that, after its revolution, sought to

be the leader of all Muslim revolutionaries, both Shia and Sunni, who wanted to confront the West. Iran has a large class of educated and forward-looking young people who enjoy more cultural freedom than most Arab countries allow. But Iran is run by a backward-looking Guardian Council of clerics who, although their initial revolutionary ardor has gone, still seek to project Iranian power in Iraq, Lebanon, and Palestine.

Thanks to Wikileaks, it is now well known that that King Abdullah of Saudi Arabia repeatedly urged the US to destroy Iran's nuclear program and "cut off the head of the snake" by launching military strikes. In June, the influential former head of Saudi intelligence and ambassador in London and Washington, Prince Turki bin Faisal, spoke to an audience from the British and American military and security community in England. Some parts of the speech, which has been circulated privately, are worth a careful read.

Faisal began by reminding his audience why

the Kingdom feels so confident today: "Saudi Arabia represents over 20 percent of the combined GDP of the Middle East-North Africa (MENA) region." Describing Iran as "a paper tiger with steel claws," Faisal accused Tehran of "meddling and destabilizing efforts in countries with majorities." Shiite He then went on to

express his country's position on nuclear weapons: "First, it is in our interest that Iran does not develop a nuclear weapon, for their doing so would compel Saudi Arabia, whose foreign relations are now so fully measured and well assessed, to pursue policies that could lead to untold and possibly dramatic consequences."

The Saudi opposition to Israeli nuclear weapons was characteristically mild: "A zone free of weapons of mass destruction is the best means to get Iran and Israel to give up nuclear weapons." Saudi enthusiasm for the bomb is inspired by Iran, not by nuclear-armed Israel.

#### Islam and the bomb

The concept of the "Islamic bomb" was first introduced by a Muslim leader, not a Westerner. Addressing posterity from the cell in a Rawalpindi jail where he awaited eventual execution, Zulfikar Ali Bhutto, Pakistan's former prime minister and the architect of its nuclear program, wrote in 1977: "We know that Israel and South Africa have full nuclear capability. The Christian, Jewish, and Hindu civilizations have this capability. The communist powers also possess it. Only the Islamic civilization was without it, but that position was about to change."

Pakistan made its first nuclear weapon in 1985 and now has many. Nevertheless, it is difficult, if not impossible, to envisage it -- or any Muslim state -- using an Islamic bomb for defense of the ummah against the United States or Israel. Although Khan has acknowledged transfer of nuclear materials and knowledge from Pakistan to other countries, his actions were not inspired by religion. In 2011,

> to get even with opponents, he made available documents that showing he personally transferred more than \$3 million in payments by North Korea to senior officers in the Pakistani military, who subsequently approved his sharing of technical know-how and equipment with Pyongyang. Ifthe released letter is genuine, then this episode demonstrates

corruption, not ideological sympathy.

While revolutionary Iran supported the notion of an Islamic bomb, it never benefited from the concept. The main sectarian division within Islam -- between Sunni and Shia -- was too big a hurdle.

There were times when Iran was considered among Pakistan's closest allies. It was the first country to recognize the newly independent Pakistan in 1947. In the 1965 war with India, Pakistani fighter jets flew to Iranian bases in Zahidan and Mehrabad for protection. Iran's pro-US Shah was a popular figure in Pakistan, and Iran opened its universities wide the

# been circulated acknowledged transfer knowledge from Pakist actions were not inspi

Pakistani students. Although it is 80 percent Sunni, with only a 15-20 percent Shia minority, Pakistan once considered Iran as a brother Muslim country.

In 1979, Khomenei's Islamic revolution and the Soviet invasion of Afghanistan set realignments in motion. As Iran exited the US orbit, Pakistan moved close to the Americans to fight the Soviets. With financial assistance from Saudi Arabia, Pakistan and the US created and armed the mujahideen. The CIA placed advertisements in journals and newspapers across the world, inviting the most hardened of Islamic fighters to participate in holy war against communist infidels. Although this worked brilliantly, the dynamics that eventually led to 9/11 had been put in place.

Iran too supported the mujahideen. But it supported the Northern Alliance while Pakistan supported the Pashtun Taliban. religion As assumed centrality in matters of state in both Pakistan and rifts Iran, widened. In the wake of the Soviet pullout from Afghanistan, the Taliban took over

Kabul in 1996. An initial selective killing of Shias was followed by a massacre of more than 5,000 in Bamiyan province. Iran soon amassed 300,000 troops at the Afghan border and threatened to attack the Pakistansupported Taliban government. Today Iran accuses Pakistan of harboring terrorist anti-Iran groups on its soil and allowing Sunni extremists to ravage Pakistan's Shia minority.

On the nuclear front, Pakistan has always publicly defended Iran's right to nuclear technology and secretly helped Iran's nuclear weapon program until the mid 1990's. But even at that time, subterranean voices within the Pakistani establishment spoke against giving nuclear support to Iran. The discomfort during the Musharraf regime was confirmed by confidential American cables, revealed by Wikileaks and highlighted by the Pakistani newspaper Dawn. The cables detail Pakistan's efforts to dissuade Iran from pursuing its weapons program. In late 2006, the cables say, former Pakistani Foreign Minister Khurshid Mahmud Kasuri told the Americans, "We are the only Muslim country [with such a weapon] and don't want anyone else to get it."

But Iran may acquire the bomb, Pakistani desires notwithstanding. Then what?

#### The Saudi-Pakistan connection

Former Saudi intelligence chief Prince Turki bin Sultan was on the mark when, speaking about Pakistan and Saudi Arabia, he said, "It's probably one of the closest relationships in the world between any two countries." Both countries are Sunni and conservative; both have ruling oligarchies (though one is dynastic and the other military). Their ties to the United

> States have a strong similarity: Both are American client states, but their populations deeply resent the master-client relationship. Saudi Arabia's footprint in Pakistan has steadily arown since the early 1970s. A huge migration of Pakistani workers

to newly rich Arab countries, especially Saudi Arabia, brought them into contact with a conservative brand of Islam different from the one they had grown up with. Many came back transformed. Since the 1960s, Pakistan has received more aid from Saudi Arabia than any country outside the Arab world. Major funding for Pakistan's nuclear program came from Saudi Arabia in the 1970s and '80s; it is said that suitcases of Saudi cash were brought into Pakistan.

Pakistani leaders, political and military, frequently traveled to the kingdom to pay homage. After India tested its bomb in May 1998, Pakistan mulled the appropriate response. Saudi Arabia's promise of 50,000 barrels of free oil a day helped Pakistan decide in favor of testing its own device, and Saudi oil cushioned the impact of subsequent Western sanctions.



The Pakistani quid pro quo for the Saudi oil largesse has been soldiers, airmen, and military expertise. Saudi officers are trained today at Pakistan's national defense colleges. The Pakistan Air Force helped create the Royal Saudi Air Force, and Saudi Arabia is said to have purchased ballistic missiles produced in Pakistan.

So what happens if Iran goes nuclear, and Saudi Arabia wants to follow?

For all its wealth, Saudi Arabia does not have the technical and scientific base to create a nuclear infrastructure. It has many expatriatestaffed universities, and tens of thousands of Saudi students have been sent to universities overseas. But because of an ideological attitude unsuited to the acquisition of modern scientific skills, there has been little success in producing a significant number of accomplished Saudi engineers and scientists.

Perforce, a Saudi Arabia in search of the bomb will likely turn to Pakistan for help. An outright transfer of nuclear weapons by Pakistan to Saudi Arabia is improbable. Surely this would lead to extreme reaction from the United States and Europe.

Instead, the kingdom's route to nuclear weapons is likely to be long, beginning with the acquisition of nuclear reactors for electricity generation. The spent fuel from reactors can be reprocessed for plutonium. Like Iran, Saudi Arabia will have to find creative ways for skirting various treaty obstacles. But it will doubtless take heart from the US decision to "forgive" India for its nuclear testing in 1998 and eventually reward it with a nuclear deal.

The kingdom's first step toward making nuclear weapons may soon be taken. In June 2011, it revealed plans to build 16 nuclear reactors over the next 20 years at a cost of more than \$300 billion. To create, run, and maintain the resulting nuclear infrastructure will require importing large numbers of technical workers. Some will no doubt be brought over from the West, Russia, and countries once part of the former Soviet Union.

But Saudi Arabia will likely find engineering and scientific skills from Pakistan particularly desirable. As Sunni Muslims, Pakistanis would presumably be sympathetic with the kingdom's larger goals. Having been in the business of producing nuclear weapons for nearly 30 years under difficult circumstances, they would also be familiar with supplier chains for hard-to-get items needed in a weapons program. And because salaries in Saudi Arabia far exceed those in Pakistan, many qualified people could well ask for leave from their parent institutions at the Pakistan Atomic Energy Commission, Kahuta Research Laboratories, and National Development Complex.

#### Living with Islamic bombs

Iran's present direction suggests that the historical clash between Sunni and Shia brands of Islam could move into the nuclear arena. Can anything be done to prevent this?

Any solution is deeply complicated by one unfortunate fact: The world's pre-eminent power, the United States, lacks the moral authority to act effectively in the domain of nuclear proliferation. Whereas it has periodically threatened Iran with a nuclear holocaust for trying to develop nuclear weapons, it has rewarded, to various degrees, other countries -- Israel, India, Pakistan, and North Korea -- that developed such weapons surreptitiously.

The US has tried threats and coercion with Iran, but never the power of humility. Had American leaders acknowledged having wronged Iran in 1953 by engineering the coup which brought back the Shah, Iranian nuclear nationalism might have been significantly weakened. It is now probably too late for this tack.

Short of war, every attempt must be made to dissuade Iran. But nuclear nationalism and Persian pride could still override the pain of sanctions. And what if Iran does make the bomb or get close to it? Well, then the international community must accept this state of affairs as just another nasty fact of life. The world will have yet another nuclear state, surely a bad, but not catastrophic, thing. One can see Iranians becoming steadily more pragmatic and less revolutionary since 1997; in time their nuclear weapons will become like everybody else's.

The world needs fewer nuclear weapons, not more. But attacking Iran is not an option. This rash step would unleash dynamics over which the US and Israel will have little control. Sunni-Shia divisions will be pushed aside; Muslims will unite against a common enemy. However unwelcome Iran's bomb -- and the Sunni bomb that could someday follow -- may be, it is far better to live with potential danger than to knowingly create a holocaust.

## A new way to detect secret nuclear tests: GPS

By Jihye Park, Dorota A. Grejner-Brzezinska, and Ralph von Frese Source: http://thebulletin.org/web-edition/op-eds/new-way-to-detect-secret-nuclear-tests-gps

When North Korea conducted its second known nuclear bomb test on May 25, 2009, the country's leaders took extreme care to conceal the details of the event. They detonated the bomb a kilometer or so beneath the earth, so no radiation could escape; radiation clues could have enabled member countries of the Comprehensive Nuclear Test Ban Treaty Organization to more accurately determine the type and size of the bomb tested.

What the rest of the world knows about the bomb was learned from seismic waves. Tremors registering at 4.52 on the Richter scale confirmed that the test took place just before 1 a.m. Coordinated Universal Time near the village of P'unggye and suggested that the yield was on the order of a few kilotons.

At the time, however, the May 25 bomb also

## **Article Highlights**

- North Korea's second known nuclear bomb test was conducted deep underground and in extreme secrecy.
- The May 2009 explosion disturbed the ionosphere in a way that could be detected in GPS signals at 11 receivers in the region.
- GPS could complement other nuclear test detection methods and give the US more reason to ratify the Comprehensive Test Ban Treaty.

sent a different signature, this one into the atmosphere. It did not release radioactive gas or dust, as would be the case for a bomb detonated on the Earth's surface. Rather, it released a shockwave -- a bubble of disturbed air that spread out from the test site across the planet and high into the ionosphere.

It was, in fact, as if the shockwave from the underground explosion caused the Earth to "punch up" into the atmosphere, creating another shockwave that pushed the air away from ground zero.

We hope that the discovery, which grew out of our efforts to improve the planet's global positioning system (GPS), will be useful to the test-ban organization as a supplementary means of detecting clandestine nuclear tests. It may even give the United States more reason to ratify the Comprehensive Test Ban Treaty.



GPS might at first seem like an unlikely for source nuclear test detection. But if the technology was designed for location purposes and it has

found many such purposes in the pursuit of science -- GPS signals have always been especially sensitive to atmospheric disturbances. GPS radio waves must pass from transmitters on satellites high above the planet down to ground-based receivers. Air molecules in-between -- more specifically, electrons and other charged particles in the ionosphere -- interfere with the signal, generating position error.

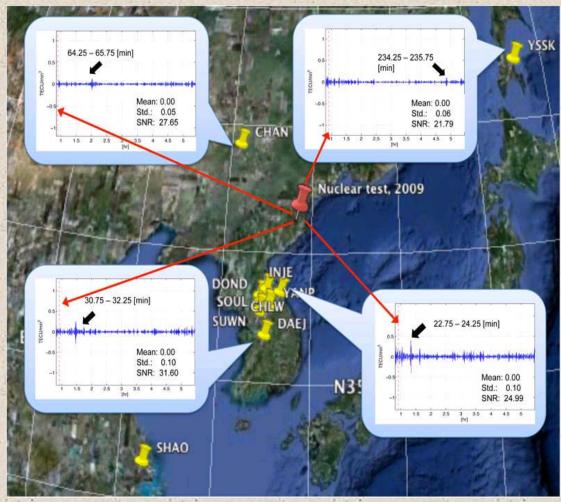
Part of our research concerns how to compensate for that interference. Whether our team is working on antenna calibration in the harsh environment of Antarctica, ionospheric modelling in the Global Navigation Satellite Systems network, or tropospheric modelling for precise and rapid GPS positioning in mountainous areas, we are working to boost GPS precision.

Over the years, we have learned that atmospheric conditions, such as the density of charged particles in the ionosphere, alter GPS signals in predictable ways. Time is the heart that drives GPS, and the presence or absence of particles in the atmosphere may speed up GPS radio signals or slow them down. By knowing how different conditions affect the signal speed, we can construct computational algorithms to compensate and maximize precision so GPS data will be useful for science.

When the bomb test occurred in 2009, we happened to be examining this problem of ionospheric disturbance. We knew that previous research had proven that

202

underground nuclear explosions disturb the ionosphere. We wondered: Could the North Korean explosion have disturbed this layer of through the air at 9 miles per minute, or 540 miles per hour. Based on the timing of the shockwave at the different receiver locations.



atmosphere to the level detectable by GPS signals? And could a sufficient number of GPS stations near North Korea be found that had continuously collected the data needed to examine the event? If so, we could take one of GPS's inherent vulnerabilities and turn it into something useful.

We quickly gathered data from 11 GPS receivers -- six belonging to the South Korean GPS network and five belonging to the International GNSS Service (IGS) and scattered around Eastern Asia. The data indicated a sudden spike in atmospheric electron density just after the underground test. We calculated that within 25 minutes, the leading edge of the shockwave had traveled 225 miles to the nearest GPS station in our study, which was located in Inje County, Gangwon Province, South Korea. By the end of the first hour, the disturbance had reached all 11 stations. The shockwave propagated

we were able to trace the origin of the explosion back to P'unggye, in agreement with the seismic data for the event.

So we believe that GPS could work as a complement to other detection methods used by the test-ban organization and could help confirm that a nuclear test has taken place -- especially when the test is underground, making its emissions into the air very subtle and otherwise nearly impossible to detect.

When the Nuclear Test Ban Treaty was formalized in 1996, the United States was among nine nations that did not ratify it. In part, US officials objected that technologies of the time were not reliable enough to ensure accurate detection of secret nuclear tests. Subsequent advances in computer science, seismology, and chemical sensors have begun to quell those objections. Perhaps the addition of GPS to the list will help to suppress them further.

## **Radiological Dispersal Device Playbook**

Source: http://www.phe.gov/Preparedness/planning/playbooks/rdd/Pages/default.aspx

#### Introduction

The purpose of this playbook is to provide guidance for executive decision makers within the Department of Health and Human Services (HHS) in the event of an actual radiological terrorist attack in a U.S. city. Specifically, it outlines key measures and options to aid the Secretary in making essential decisions and directing the HHS response to a radiological attack.

The playbook functions as a resource document to the Assistant Secretary for Preparedness and Response (ASPR) to assist in coordinating the Department's Emergency Support Function (ESF #8) with other Federal and local emergency support agencies. It is not intended to serve as an instruction manual for implementing the ESF #8 missions at the operational or tactical level; rather, it illustrates the capabilities required to meet probable mission requirements.

This playbook is a living document that must be updated periodically to reflect evolving processes and policy decisions including changes resulting from interagency plans or policies. ASPR is responsible for managing this process of bringing the playbooks up to date.

#### Radiological Dispersal Device Playbook Overview

The playbook is based on the chronology of events outlined in the Radiological Attack scenario of the National Planning Scenarios (Scenario #11). The following phases drive the actions outlined in this playbook:

- Phase 0: Pre-Incident (Situational Awareness, Credible Intelligence). Steady state operations and advance preparations are initiated for a large-scale response to a radiological attack, based upon credible intelligence of a plan to detonate a Radiological Dispersal Device (RDD) or a Radiological Explosive Device (RED) in a U.S. City. The primary strategy is to closely monitor events and begin advance preparations for an effective and timely response.
- Phase I: Early Phase (0 24 Hours Post Detonation). The primary U.S. strategy is to assess the events and deploy assets to maximize survivors, treat injured victims, and aggressively administer an effective post-exposure prophylaxis program
- Phase II: Intermediate Phase (24 72 Hours Post Detonation). The strategy is to provide surge capacity and rapidly deploy ESF #8 assets to provide assistance to State, Territorial, Tribal, or local officials in saving lives, minimizing adverse health effects, stabilizing public health, medical and human services infrastructure.
- Phase III: Late Phase (72 Hours 2 Weeks Post Detonation). The goal of this phase is to
  effect a smooth and transparent transition to long-term recovery while continuing to provide
  technical expertise to regional, state and local authorities as they rebuild their public health and
  medical infrastructure.

This Radiological Attack Playbook is prepared in accordance with the National Response Framework (NRF) and associated Federal regulating documents. There are six major sections to this Playbook including (A) introduction, (B) scenario; (C) concept of operations (CONOPs); (D) actions/issues; (E) pre-scripted mission assignments, and (F) essential elements of information (EEIs). These sections are briefly discussed below. At the end of the playbook, a list of acronyms used and their definitions is provided

 Introduction: The introduction briefly addresses the purpose of the playbook and how it is structured. This section also provides an overview of radiological dispersal devices and radiological explosive devices providing relevant information for preparedness and response.

operations. In addition, it covers some technical discussions which may be of interest primarily to subject matter experts.

- Scenario: The Homeland Security Staff Council (HSC) (now National Security Staff-(NSS)) -in concert with the Department of Homeland Security (DHS) the federal interagency, and State and local homeland security agencies- has developed fifteen all-hazards planning scenarios for use in National. Federal, State and local homeland security preparedness activities. These scenarios are designed to be the foundational structure for the development of coordinated national preparedness standards from which homeland security capabilities can be measured or assessed, The Radiological Attack scenario is an account or synopsis of a projected event. This scenario is used in policy planning within the Department of Health and Human Services (HHS) in an effort to set the conditions for conventional thought on how the department would approach, plan for, and possibly test strategies against uncertain future developments. The radiological attack scenario alerts us to different ways that future events could unfold. This scenario should not be used to forecast future events, but rather, it offers a plausible story line to account for possible future events leading toward a radiological attack as depicted in National Planning Scenario #11. The decision to use the HSC scenarios in the development of the playbooks provides a common set of conditions that provide interoperability with Federal, State and local emergency responders. It also allows HHS to work closely with our interagency partners through the National Response Framework (NRF) and the National Incident Management System (NIMS) to ensure efficiency and interoperability in responding to radiological incidents.
- Concept of Operations (CONOPs): This CONOPs evolves from a vision of actions and events and is a description of how a set of capabilities may be employed to achieve desired objectives or a particular end state for the radiological attack scenario. CONOPs take into account the steps and procedures that may be found in State, local, and Federal response plans to a radiological attack. The approaches incorporate the synchronized activities and capabilities under consideration and add the resource management details of whom, and where resources may be applied to achieve desired mitigating outcomes. The CONOPs do not describe how to conduct preparedness activities but merely serve as a discussion point for Federal, State, local, tribal, regional and territorial, planners to use as a baseline for a coordinated preparedness effort.
- Actions/Issues: This section refers to the steps associated with each phase of the event, further segmented by functional activity, including:
  - Planning and Coordination
  - o Healthcare, Emergency Response and Human Services
  - o Surveillance, Investigation, and Protective Health Measures
  - o Pharmaceuticals, Medical Supplies and Equipment
  - o Patient Evacuations, and
  - o Communications and Outreach
- The actions/issues are the heart of this document and outline the steps necessary to achieve interagency coordination effects for the Radiological Dispersal Device Playbook. They also assign lead and supporting government agency responsibilities.
- Pre-Scripted Mission Assignments (PSMA) for ESF #8: PSMAs are defined as coordinated critical tasks that must be performed with or by other departments and/or agencies in the federal government. Representative departments and agencies are supporting entities within ESF #8. Federal supporting agencies include: the Departments of Agriculture, Energy, Homeland Security, Interior, Justice, Labor, State, Transportation, Veterans Affairs, and other agencies including Environmental Protection Agency, General Services Administration, and U.S. Agency for International Development, U.S. Postal Service, and the American Red Cross.
- Essential Elements of Information (EEIs): EEIs are those critical items of information needed to
  respond appropriately to circumstances surrounding the event. EEIs provide decision makers
  at all levels insight into how and where resources should be applied to achieve maximum
  benefit for the general population in easing suffering or protecting infrastructure. In this
  playbook, information requirements are derived as they relate to the preparedness and
  response activities for a radiological dispersal device attack.

#### **Overview of Radiological Attack Devices**

This playbook is based on the chronology of events in the National Planning Scenarios (Scenario #11) Radiological Attack - Radiological Dispersal Device. Since the emergency response has generic (triage, beds, medicines, transportation) and specific components (radionuclide specific response) some of the supporting details are useful but not essential for general operations personnel. They are more practical for Subject Matter Experts and other educational purposes.

Information in a gray box contains **non-essential** supporting information and **may be bypassed** when using the playbook.

#### Essential Facts

The widespread availability of radioactive material for industrial and medical use provides a broad range of scenarios for the abuse and subsequent exposure of civilian populations to radioactive material in potential terrorist events. The types of event can be:

- RDD- Radiological Dispersal Device can be of two general types. In both, radioactive
  material is dispersed into the environment.
  - Dispersal of radioactive material via explosive detonation, i.e., a combination of an Improvised Explosive Device (IED) and radioactive material
  - **Dispersal of radioactive material via non-explosive means**, e.g., in food, water, soil, or air, etc.
- RED- Radiological Exposure Device refers to a sealed radioactive source that is placed in a
  public place and causes exposure but not contamination to those in proximity. (Note: if an RED
  were to break open, it would then be similar to an RDD)

## Exposure versus Contamination:

Matter that contains radiation-emitting atoms is radioactive material. Radiation is the energy released from radioactive material. It is critical to understand the difference between (a) exposure to radiation and (b) contamination with radiation. The medical effects and countermeasures differ significantly.

- Radiation exposure (or irradiation) occurs when radiation penetrates tissue, for example, when a patient undergoes a diagnostic X-ray. A person can be irradiated without physically contacting radioactive material. Exposure results from radiation external to the victim, and the victim is NOT radioactive. This radiation can be in the air or on the ground (groundshine). Internalized radiation can cause exposure.
- Radioactive contamination is radioactive material located in unintended places. Note: An
  exposed person is not necessarily contaminated because exposure does not require contact
  with radioactive material. However, as long as a person remains contaminated they will
  continue to be exposed to the radiation being emitted by the radioactive material with which
  they are contaminated. Contamination can be external (outside of the body) or internal (inside
  of the body) or both.
  - External contamination is radioactive material on a person's clothes, hair, or skin.
  - Internal contamination is radioactive material that has entered the body by inhalation, ingestion, or absorption through the skin or wounds.

#### Decontamination

- External decontamination: This is often readily accomplished by removing the person's clothing and shoes and washing the skin and hair with soap and water.
- Internal decontamination: Normal body-cleansing mechanisms (e.g., digestion and excretion) can often partially remove internal contamination. When medically indicated.

decorporation agents, such as laxatives or chelating compounds, are administered to speed up excretion of internal contamination. Similarly, blocking agents can be used to inhibit uptake of some radioactive materials. Knowledge of the chemical nature of the contaminant is essential in making initial treatment decisions.

Matter that contains radiation-emitting atoms is radioactive material. Radiation is the energy released from radioactive material.

## Properties of the radiation

Two properties of atoms are considered when determining how radiation affects people:

- **Element itself** (e.g. Cobalt, Cesium, Iridium, Iodine, Strontium) determines the chemical properties and biological distribution in the body.
- **The isotope** of an element determines the amount and type of radiation emitted. (Radionuclide and radioisotope, used interchangeably and refer to an unstable form of an element that decays resulting in the emission of radiation).

The selection of a medical countermeasure (e.g. decorporation, blocking agent, diuresis) is based on the element and its properties (e.g., lodine vs. Cesium), the type and amount of radiation exposure received by an individual (alpha, beta, gamma, neutron), and the specific isotope (e.g., lodine-131 vs. lodine-125) and how much was encountered.

Clinical presentation and injury:

- **Explosive RDD**. Depending of the size of the explosion, an RDD detonation could generate a modest number of patients with physical trauma, thermal burns, contamination, and (in rare cases) radiation injury. These combined injuries (radiation injury plus trauma) range from mild to severe/fatal. In this instance, the incident will be detected by physical detection devices.
- Non-explosive RDD. A non-explosive RDD (e.g. contamination of food or water, aerial dispersal, dispersal in a ventilation system), can potentially expose a modest number of people to moderate doses of radiation and many people to low doses of radiation. The event may be obvious in real time or may be subtle becoming recognized over time. In this instance, the incident can be detected by physical detection devices or by an astute clinician who recognizes the syndromes related to radiation injury. For low exposure (less than ~100 centiGrays (cGy) whole body dose) particularly with protracted exposure, there may be few telltale symptoms to suggest radiation injury.
- **RED**. An RED incident may be realized by direct discovery of an RED or by clinical recognition of an incident due to a number of people presenting at an Emergency Department, (not discovering the device per se), developing symptoms, and signs of radiation injury. As long as the radiation source remains closed and sealed, there will NOT be any contamination.

## Psychological consequences:

 For both a non-explosive RDD and an RED, many people may present for medical care out of fear of possible exposure, far greater than those actually affected. Both the psychological impact of these events and the economic factors related to a contaminated environment can be substantial and long lasting. Those who are neither exposed nor contaminated may require reassurance. Responders, too, can have profound psychological effects from participating in the response to an incident and will need assistance.



Radiation Event Medical Management (REMM):

Radiation Event Medical Management (REMM) is a web portal developed to assist health care providers to respond to mass casualty radiation events. It is collaboration between HHS/ASPR and the National Library of Medicine and contains just-in-time response algorithms, detailed event management information, and large amounts of supporting information explaining radiation and response, training and planning issues. A zip file with almost all the REMM files can be downloaded to a PC or to a PDA. Users are encouraged to join the REMM ListServ to be notified when updates are released. It can be used either online of offline. A ZIP file with almost all the REMM files can be downloaded to a personal computer or to a PDA device. Users are encouraged to join the REMM ListServ to be notified when new versions of REMM are released

## Table A1. Overview of Radiation Events

RDD - Explosive IED, etc.	RDD Non-Explosive: Air, Food, Water, Soil	RED - Exposure
<ul> <li>Immediately recognizable as "an explosive event".</li> <li>Radiation might not be detected immediately.</li> <li>Health physicists must map radiation levels in contaminated area to assess safety and determine allowable response time in various zones due to radiation.</li> <li>Casualties from explosion are immediate.</li> <li>No immediate deaths expected from radiation, but victim decontamination is essential.</li> </ul>	casualties by inhalation of contamination in ventilation or ingestion of food/water or products	<ul> <li>Time of initia exposure may not be known.</li> <li>There can be exposure but no contamination (unless the source is broken).</li> <li>Risk of mass casualty low.</li> <li>Likely only partial body dose, so radiation-related death would be low.</li> <li>Maybe difficul or impossible to sort out who was exposed to low doses.</li> </ul>

## Assessing an RDD Attack

As a weapon, an RDD or RED (AKA "Dirty Bomb") is considered as follows:

- Not a nuclear weapon
- Not a weapon of mass destruction
- A weapon of mass disruption, economic weapon, psychological weapon
- Impact depends on type of explosive, amount and type of radioactive material, and weather conditions

Source: The Armed Forces Radiobiology Research Institute



#### Initial Steps: Determining the Type of Incident

- Is this a radiological event? It takes health physicists (includes other radiation protection specialists) to detect radionuclide, interpret data from radiation monitors, determine exposure rate, initially and over time, and help manage safety issues of the response to the event on site.
- Is there exposure? Is there radioactive contamination? Is radioactive material free in the environment from the explosion or dispersal?
  - If there is environmental contamination, highly contaminated areas will have to be cordoned. If there has been population contamination, decontamination of victims will be required for their safety and to prevent contamination of transportation, medical facilities, individuals or the environment. Life-threatening injury must be treated before decontamination. Removal of outer garments, showering and superficial decontamination removes about 90% of the external contamination.
- Is there internal contamination? If patients have ingested or inhaled radioactive material, or taken that material into their body through a wound or other means, they could be internally contaminated.
  - Special medications (e.g. decorporation and blocking agents) may be needed for those who have internalized radionuclide in sufficient quantity.
  - Subject matter experts will provide recommendations for which medications will be needed based on the identified radionuclides. Some of these medications are available in the Strategic National Stockpile, some are in state/local stockpiles, and others would need to be obtained through commercial sources.
  - Both exposure and contamination will likely happen to those very near the center of an explosive RDD. Further away, victims will likely have less intense contamination and consequently a lower exposure rate.

## What Is The Size Of The Event?

- **Number of Casualties**. The number of casualties is very scenario dependent (nature of explosive, amount and type of radioactive material dispersed, location of the event, number of individuals affected, weather, etc.).
  - Serious injuries are likely to be in the hundreds; victims requiring decontamination and medical care may be in the thousands.
  - Victims requiring treatment for acute radiation syndrome (ARS) are likely in the hundreds at most. Most RDD events will have few severe ARS victims.
  - Individuals in need of counseling or consultation may be in tens of thousands, including responders.

#### Radiation doses

Unlike an IND event, an explosive RDD event produces no nuclear explosion or huge burst of radiation.

- Radiation dose is cumulative. The radiation dose from an explosive RDD can accumulate
  over time and the radiation injury depends on the duration and amount of exposure or
  contamination. The dose from an RED depends on the radionuclide used and how long any
  individual was near the radionuclide. "Committed dose" (term used to evaluate effects of the
  radiation) is a calculation of the dose an individual will receive over their lifetime from internal
  contamination. It is calculated from the knowledge of the radionuclide and from the amount a
  person has within them.
- Acute Radiation Syndrome (ARS) with nausea and vomiting can occur with doses above 0.75 Gray (Gy). However, clinically significant ARS requiring medical countermeasures for the hematological syndrome is unlikely unless victims absorb a cumulative whole body dose above 2 or 3 Gy (200 – 300 rem or higher). (rem is a radiation unit of measure and stands, for.)

"Roentgen Equivalent Man". While not precise, Roengten/hr and rem/hr are often used interchangeably.)

- Permitted dose for responders is determined by the lifetime potential risk of radiationinduced cancer. Doses above 5 rem (5,000 mrem), but especially above 25 rem (25,000 mrem) would be of concern. At a dose rate of 1,000 mrem/hr, it would take a responder 5 hours to reach 5,000 mrem (or 5 rem).
- **Concentric radiation** "response zones": will be created at the scene based on the dose rates measured at the scene. The dose rates measured will define the time people can spend in a particular location. Over time the dose rates will diminish and the perimeters of the zones will change. Weather conditions and ground topography also affect the shape and location of the zones.

#### **Radiation Response Zones**

Radiation "response zones" Determination

- Radiation "response zones" will be determined based on both data modeling and measured data by health physicists or other radiation protection experts (Military/Civil Support Teams, Interagency Advisory Team for Environment, Food and Health (A-Team) and possibly Radiation Emergency Assistance Center & Training Site (REAC/TS, in Oak Ridge, TN), and the Armed Forces Radiobiology Research Institute (AFRRI, at USUHS in Bethesda, MD)
- The "HOT" zone: perimeter at 5 rem or greater per 5 hrs (or 25 rem cumulative)
- The boundary line for the "no entry zone" will likely be about 100 meters for a small to intermediate sized device and up to 600 meters for a very large device (Harper 2007). Evacuation is recommended around 150 m and 1-15 km from the epicenter of detonation for these devices respectively.
- In the absence of real time measured radiation data, a zone of approximately 500 meters is a
  reasonable first estimate but this will be rapidly refined as measurements are obtained.
- Zone perimeters will change over time as the plume and footprint evolve. For most RDDs, the plume passage will last 20-30 minutes. Continuing on-scene measurements will be essential.
- The National Council on Radiation Protection (NCRP, Commentary 19) has made recommendations similar to those in Figure A1:
- The Inner Perimeter is 10 R/hr (similar to 10 rem/hr or 10,000 mrem/hr). (Note: "R/hr" means Roetgens/hour.)
- The Outer Perimeter is 10 mR/hr (similar to 10 mrem/hr)
- Boundaries of exclusion and short term activity are determined by local authorities, often with Federal advice. Boundaries will be refined as data are received and conditions evolve.
- Interagency Modeling and Atmospheric Assessment Center (IMAAC) models which account for event type and wind and weather data will be useful in creating response zones, but dose rate cannot be fully predicted because wind current and patterns are very complex, especially with the urban canyon effects. On ground measurements will be more accurate than modeling data.
- Illustration of prototypical "response zones" are in Figure A1 and described in Table A2 below.

## Figure A1. Example of "boundary zones"

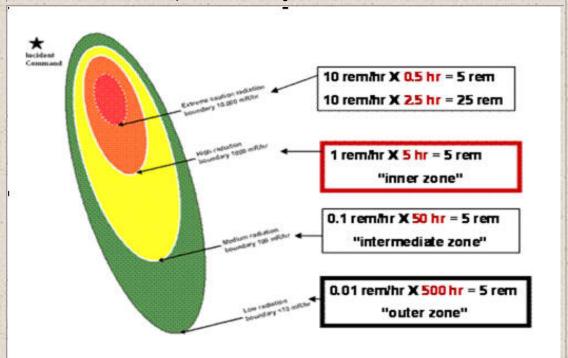
#### (Conference of Radiation Control Program Directors)

Figure A1 shows typical radiation zones (outlined in Table A2) and illustrates how boundaries could be established and how the allowed "work time in a zone" can be estimated. Concentric radiation "response zones" will be based on the dose rates measured at the scene. (The shape and location of the zones is a result of weather conditions and ground topography). The dose rates measured will define the time people can spend in a particular location. Permitted dose for responders is 5 rem. Doses above 5 rem (especially above 25 rem) are cause for concern. The Extreme Caution Boundary is the innermost perimeter which measures 10 rem/hr; the 5 rem limit is reached after 0.5 hours (and 25 rems within 2.5 hours) It is considered a "no entry zone", restricted to very short-term life saving activities only. The figure shows the successive radiation zoning from High Radiation Boundary (the "Innet Zone",

## Figure A1. Example of "boundary zones"

(Conference of Radiation Control Program Directors)

at 1 rem to Medium Radiation Boundary (the "Buffer Zone") measuring 0.1 rem to Low Radiation Boundary (the "Outer Zone") at 0.01 rem where initial decontamination may take place. The Incident Command Center (marked ê) is located outside the radiation zone. Note that over time the dose rates measured will diminish and the perimeters will change.



	2 How ce of Radiat	Radiation ion Control Pi	Zones could be determined - One Example rogram Directors)
Extreme Caution Radiation Zone	Extreme Caution Radiation Boundary	≥10,000 mR/hr (10 R/hr)	<ul> <li>Activities restricted to saving lives</li> <li>Total accumulated stay time for first 12 hours: minutes to hours.</li> </ul>
High Radiation Zone	High Radiation Boundary	1000 mR/hr	Access restricted to authorized personnel performing critical tasks: • Firefighting • Medical Assistance • Rescue • Extrication • Other time-sensitive activities
Medium Radiation Zone	Medium Radiation Boundary	100 mR/hr	<ul> <li>Access restricted to authorized personnel entering the "High Radiation Zone" to perform critical tasks such as saving of lives and property.</li> <li>Serves as a buffer zone/transition area.</li> </ul>
Low Radiation	Low Radiation	≤10 mR/hr	Access restricted to essential individuals.

Table A (Conference)		Radiation ion Control F	 	be	determined	-	One	Example
Zone	Boundary		near the Boundary' Victims wi likelihood contamina	"outer ) of this th only of prior tion, si	ation of first r boundary" area. lower body co radionuclide nce they w zone and no	(i.e., ontam inha ere	"Low ination lation a probably	Radiation have a low nd internal y exposed

## Shelter-in-Place

- Sheltering during the short-lived plume (about 20-30 min) may be beneficial, but evaluation of the incident and public messaging may not occur in time for this to be effective.
- Protection from radiation is also afforded by the building itself, but this is variable.
- Since air handling in some buildings may concentrate radiation, it is not easy to have simple guidelines for shelter-in-place recommendations during and after the plume passes by. Given the short-lived duration of most airborne radionuclides (about 20-30 min), it is not likely that shutting down a building ventilation system will be effective. After the plume has passed, the inside of some buildings may have higher air concentrations than outside, depending on the air system, filtration, etc.
- Evacuation routes from the affected zones need to be planned, with radiological monitoring of victims at exits to see which victims need decontamination and possible treatment.

#### Decontamination

- For uninjured people, ambulatory decontamination is primarily removal of outer garments and showering. The size of the event will help determine whether ambulatory decontamination will be done primarily in formal decontamination sites or at home. Contaminated garments and personal property require proper disposal for potential forensic evaluation and safety. Removed personal effects and clothes should be bagged, labeled, and kept away from people and animals.
- Injured victims also need decontamination. Some may be transported through decontamination tents on a litter. Decontamination for others will be improvised, understanding that life-saving measures always take precedence over decontamination.
- Victims with only lower body contamination have a low likelihood of prior radionuclide inhalation and internal contamination, since they were probably exposed walking across the zone and not from the plume.

## Determining the Radionuclide

Identification of the radionuclide is essential. This information will help determine the possible physical damage from the event, as isotopes can only be "weaponized" in certain ways, based on their physical properties (Harper 2007). In addition, the appropriate medical countermeasure for those who need treatment is generally radionuclide-specific.

- Health physicists/safety officers will determine the radionuclide(s).
- Multiple radionuclides may be used in one event.



- Sampling of the environment using specialized radiation detectors will ordinarily detect the radionuclide(s) involved. Various governmental agencies will do that.
- Laboratory analysis of human samples (nasal swabs, feces, urine), may be necessary to evaluate which victims need treatment and evaluate the efficacy of that treatment. State labs may be used as well as those from CDC and other resources.
- Most likely radionuclides for an RDD or RED event include Cesium chloride, Cobalt, Americium, Iridium, although others may also be used. Multiple agents may be used in a single event (Harper 2007).

TableA3-ExamplesofradioactivematerialthatmightbeusedforRDD(Armed Forces Radiobiology Research Institute)

Radionuclide	Half-Life	Typical Activity	Use
Cobalt-60	5 years	15,000Ci	Cancer Therapy
Cesium-637	30 years	1.5x106Ci 10mCi	Food Irradiation Medical Source
Iridium-192	74 days	150Ci 1mCi	Industrial Radiograph Medical Source
Plutonium-238	80 years	varies	Satellite Power Source
Strontium-90	29 years	40,000Ci	Radio-Thermal Generator (RTG)
lodine-131	8 days	0.015Ci	Cancer Therapy
Americium-241	432 years	1.5x10 <sup>-6</sup> Ci	Smoke Detector

• Amount of radionuclide is determined by disintegrations per second (Curies, Ci)

• 1 Ci (Curie) = 3.7 x 10<sup>10</sup> disintegrations per second (dps)

• 1 Ci = 3.7 x 10<sup>10</sup> Bq

- 1 Bq (Becquerel)= 2.7 x 10<sup>-11</sup> Ci
- Physical half life describes the length of time it takes for a radioactive substance to lose onehalf of its radioactivity.
- Biologic half life describes time required for the radioactivity of material taken in by a living
  organism to be reduced to half its initial value by a combination of biological elimination
  processes and radioactive decay.

## Table A4: Analysis of likely RDD materials (Harper 2007)RDD Types and Effects (10kCi Devices)

Nuclide	Primary Radiation Type (Half Life)	Primary Form	Size of Source for calculation in GBq(Ci)	Application that forms the basis for size of source
<sup>90</sup> Sr	Beta (28.6y)	Ceramic (SrTiO <sub>3</sub> )	1.11x10 <sup>7</sup> GBq (300,000 Ci)	Large radioisotopic thermal generator (RTG) (Russian IEhU-1)
<sup>137</sup> Cs	Beta + Ba -137 m Gamma (30.17y)	Salt (CsCl)	7.4x10 <sup>6</sup> GBq (200,000 Ci)	Irradiator
<sup>60</sup> Co	Beta, gamma (5.27y)	Metal	1.11x10 <sup>7</sup> GBq (300,000 Ci)	Irradiator
<sup>238</sup> Pu	Alpha (87.75y)	Ceramic (PuO <sub>2</sub> )	4.92x10 <sup>6</sup> GBq (300,000 Ci)	RTG used for the Cassini Saturn space probe
<sup>241</sup> Am	Alpha (432.2y)	Pressed ceramic	7.4x10 <sup>2</sup> GBq	Single well logging source

	Table A4: Analysis of likely RDD materials (Harper 2007)           RDD Types and Effects (10kCi Devices)					
		powder (AmO <sup>2</sup> )	(20 Ci)			
<sup>252</sup> Cf	Alpha (2.64y)	Ceramic (Cf <sub>2</sub> O <sub>4</sub> )	7.4x10 <sup>2</sup> GBq (20 Ci)	Several neutron radiography or well-logging sources		
<sup>192</sup> lr	Beta, gamma (74.02d)	Metal	3.7x10 <sup>4</sup> GBq (1,000 Ci)	Multiple industrial radiography units		
<sup>226</sup> Ra	Alpha (1600y)	Salt (RaSO <sub>4</sub> )	3.7x10 <sup>3</sup> GBq (100 Ci)	Old medical therapy sources		

 Table A5: Types of RDD's and their general impact

 (Armed Forces Radiobiology Research Institute)

Туре	Isotope	Physical Form	Dispersal Method	Construct Difficulty	Early Deaths	Psychological Effect	Economic Effect
Radiological Exposure Device	Co-60 Cs-137	Metal, Salt	None	L	Maybe	M	L
Food or Water	Cs-137 Pu-238 Sr-90	Salt Solution	Dissolve	L	Food- Yes Water - No	H	M
Fragment RDD	Co-60 Sr-90 Pu-238	Metal Ceramic	HE.	Μ	No	М/Н	M
Non-respirable Aerosol RDD	Cs-137 Co-60 Sr-90 Pu-238	Salt, Metal, Ceramic, Solution	HE Sprayer	M	No	H	н
Respirable Aerosol RDD	Sr-90 Cs-137 Co-60	Sat, Metal, Solution	HE Sprayer	M/H	Maybe	н	н
H,M,L- High, Med	ium, Low,	not otherwise of	defined	2015-0			

## Triage System-Organizing the Medical Response

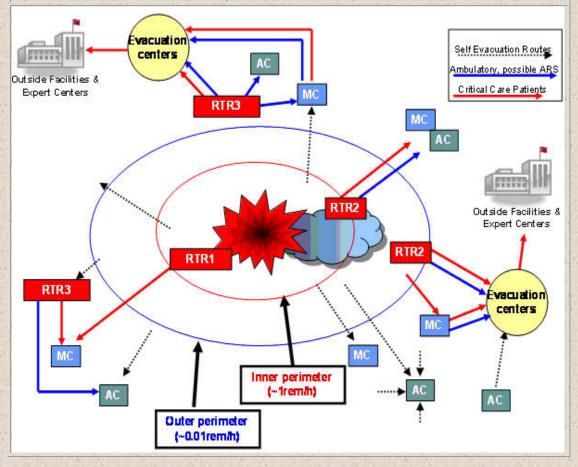
- Conceptual triage approach (see Figure A2-A3) is similar in concept to that of an IND in that the functions at the RTR, MC and AC sites are similar- described below) (Hrdina publication).
- The size of an RDD is such that it is likely the local/regional responders and medical facilities will be able to take care of the most if not all of the victims. However, large events may require substantial support from regional partners and possibly federal resources.
- Multiple simultaneous or closely spaced events may lead to a situation in which regional Emergency Medical Assistance Compacts (EMAC) may not be honored due to concern for additional events. This would accelerate the need for federal resources
- Nonetheless, whatever the size of a radiological event, a national response will likely be initiated immediately, with resources allocated as needed. (they can stand down if not needed)
- Assets of ESF#8 will be alerted and mobilized, including NDMS and other assets
- Radiation Injury Treatment Network (RITN) will be alerted
- HHS SOC will use GIS system (note: MEDMAP project) to identify medical facilities in the area and region



## Figure A2 Conceptual Triage System - RTR Sites

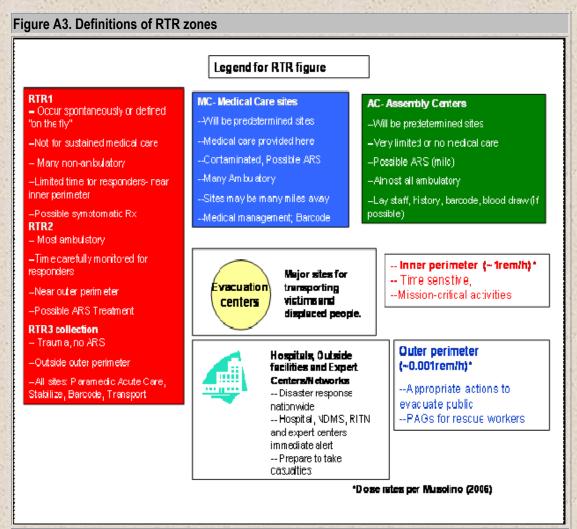
(See Figure A3 for definitions)

Figure A2 is a diagram of a conceptual triage system near the affected area. Close to the blast site, around the perimeter of the High Radiation zone or "inner radiation boundary" RTR1 site(s) will be set up for victims from the immediate blast site with major contamination, injuries, and/or trauma. Responders may only dwell for a limited time. RTR2 site(s) will be set up near the "outer radiation zone" where responders' time will still be carefully monitored. Most ambulatory victims will be assessed, and those with ARS (Acute Radiation Syndrome) may receive immediate care, and others will be directed as appropriate to Evacuation Centers and predetermined Medical care sites (MC) for treatment or Assembly Centers (AC) limited care and transport to nearby facilities and victim tracking. RTR3 sites will be set up outside the outer perimeter and act as collection sites for affected persons leaving the blast area; RTR3 sites will provide paramedic acute care, stabilize victims and direct them as appropriate to MCs, ACs, Evacuation Centers, or transport them to outside facilities.



- The zones will be determined by externally measured dose rates.
- In this Playbook, 1 rem/hour (1000 mrem/hr) is used as the "inner boundary" and 0.01 rem/hr (10 mrem/hr) as the "outer boundary". This is for illustration purposes and is consistent with NCRP (Commentary 19) guidelines. There will likely be intermediate zones established so that time spent and dose received by responders will be limited.
- Relocation guidelines will also be established by local/regional/state/tribal authorities in consultation with federal experts.
- Due to wind currents and other factors, there may be irregular shaped zones and the zones will change over time.





RTR sites are functional sites that define TRiage, TReatment, and TRansport functions. Time in zone may be limited by radiation.

**RTR sites** form spontaneously: Victims immediately in the blast site may have injury from the blast, fairly heavy contamination from radiation or combined injury (physical trauma and burn plus radiation). The radiation dose is likely to be limited as there is no detonation effect as with an IND but rather the radiation is being accumulated over time. RTR sites will be identified "on the fly" by responders and coordinated with the Emergency Operations Center (EOC). Health physicists and other radiation protection specialists will provide subject matter expertise to help interpret the readings obtained by emergency responders.

- RTR1 will have limited time for emergency workers but the high dose zone will be small and most likely a few hundred meters in diameter.
- **RTR2 sites**. These will be near the plume/footprint zone, recognizing that the plume will be very short-lived. While there may be some re-suspension of radioactive material most of the residual radiation will be a footprint on the ground and not a plume.
- RTR3 sites. Collection points with radioactivity screening (using survey meters) to identify those victims requiring decontamination and/or medical management.

**MC** (Medical Care) sites will be the focus of medical management. It is likely that the local hospital network will have adequate resources although regional facilities may be needed. Some hospitals may be off line due to the location of the RDD and plume. Expert centers for trauma or burn care may be needed beyond the region. Acute Radiation syndrome may occur depending on the size of the device.

## Figure A3. Definitions of RTR zones

Management and decorporation treatments will be managed locally or possibly through the National Disaster Medical System, the Radiation Injury Treatment Network and/or other expert centers.

- AC (Assembly Centers) will be used for displaced persons and for those with minor injury. This
  will be coordinate with ESF #6.
- **Population monitoring** (Plans for this are in progress- see Briefing Paper #16)
- Victim tracking is important. There are various systems in place with work ongoing to establish national standards or at least to try to establish compatibility among systems. The CDC will be called on for this.

## Decontamination

## Decontamination is a local responsibility.

ESF#8 will assist local authorities with coordination of decontamination of victims, responders, and persons exposed to contamination by an RDD.

Procedures used for decontamination are incident specific and may vary considerably. These procedures will be influenced by various factors including the following:

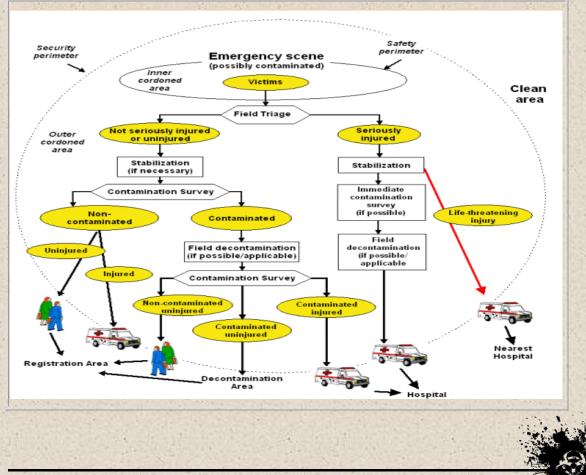
- Size and type of event
- Location of the event
- Weather conditions
- Availability of local decontamination resources and personnel to carry it out
- Whether or not "time zero" is known (as with a non-explosive RDD)
- Extent of civilian chaos
- Numbers of people self-evacuating before safe zones and decontamination areas can be established
- Concerns of the many people who may be far from the blast but who later worry about having been contaminated and who need reassurance
- Special concerns need to be paid to the following groups and issues:
  - Victims injured on the scene potentially requiring life-saving medical intervention prior to decontamination.
  - o At-risk individuals.
  - The need to avoid contaminating transportation vehicles of any kind.
  - The need to avoid contaminating Emergency Departments and other receiving areas including Red Cross shelters.
  - o Concerned citizens who are not exposed or contaminated but who need assurance.
- Personal external decontamination could take place in a number of places:
  - At entry points to medical facilities, to avoid contaminating the facility. Those needing life-saving care will require careful handling to minimize impact on care-givers and on the facility.
  - At exit points from control zones, for those who are ambulatory.
  - At entry points to collection sites
  - At home or remote sites for self-decontamination of those who leave the scene before decontamination sites are established or who flee the scene.
- Monitoring/assessment for victim contamination will occur at:
  - o Medical facility entry point.
  - Exit points from control zones, as needed.
  - Entry points to shelters such as American Red Cross and other AC collection sites.
     This is required for ESF #6 care.

- 218
- o Various remote sites for concerned citizens (so-called "worried well").
- Transportations sites for DOD transportation (no contamination is allowable) or other transportation hubs.
- Referral for surgical or medical internal decontamination may be needed for any victim with the following conditions:
  - Adequate external decontamination does not result in removal of radiation levels to below about 2 times background, thus indicating possible significant internal contamination.
  - Obvious shrapnel wounds containing radioactive materials. Surgical debridement with radiation precautions will be required.
- By history/location during an event, a victim may be at risk for having inhalation or ingestion. In lieu of a complex flow diagram illustrating these many possibilities, Figure A4 is a schematic as to how victim flow may occur at an RDD event, particularly one in which the event is obvious.

## Figure A4 Victim Handling Flow at Emergency Scene

Figure A4 illustrates the victim handling flow at the emergency scene. Life-Field triage will separate out the seriously injured, ensuring that life-threatening injuries are treated first and such patients are transported to the hospital immediately, even if contamination survey has not been done. Other seriously injured victims are also stabilized first before addressing contamination.

While still within the "outer cordoned area" (or "Outer Zone") contaminated patients are isolated among the non-critically injured victims. Decontamination protocols are administered before treating for minor injuries and before entering the "clean area" to transport them to other facilities. This will reduce the possibility of spreading contamination beyond the initial perimeter of potential contamination.



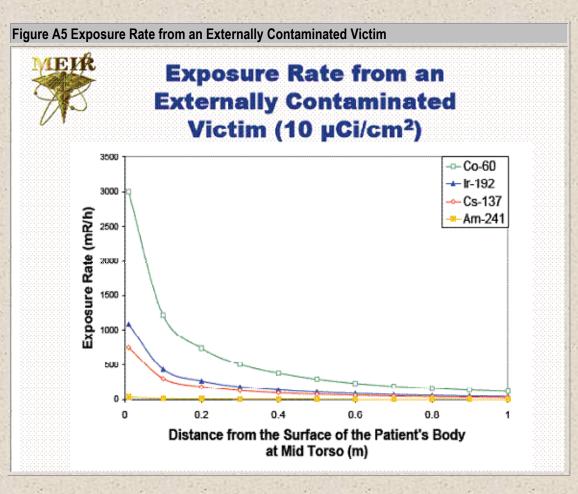
Evacuation / Transportation

- Transportation out of the event and transportation towards the event will be needed.
- Medical resources may need to be imported. While this is event dependent, major medical
  packs from the SNS will not likely be necessary for modest sized RDD events. However,
  resources and supplies may be needed to support local hospitals over time, possibly including
  FMS and decorporation agents.
- Emergency personnel: various HHS medical personnel and materiel assets will likely be deployed, at least on a stand-by basis.
- Evacuation may be needed for displaced persons based on the situation at the site. This could be from the explosive damage to infrastructure or to radiation contamination. In a large scale event, medical evacuation will be needed.
- Keeping transport vehicles free from internal contamination is a high priority so that they can remain "on line." This may not be entirely possible when transporting the critically injured.
- DOD and ESF #1 assets will not transport contaminated individuals. There are no exceptions to this for the DOD. Local governments may operate in the same way.
- Medical Responders May Be At Risk for Significant Dose
  - Life-threatening injuries must be managed before dealing with decontamination (Smith, 2005). Nevertheless, there are settings in which medical personnel might be exposed to a relatively high dose of radiation, as with cobalt radioactive shrapnel embedded in a victim.
  - Removal of outer garments and washing of exposed skin and hair from the victims and showering will usually remove about 90% of the victims' contamination,.
  - Health physicists/safety officers will provide guidance to medical and other responders. The use of personal dosimeters during work tours will be important. This is a local responsibility. HHS must not give reassurance until data have become available. Information recorded by the dosimeters must be carefully stored during and after the event.
  - First responders should use appropriate Personal Protective Equipment (PPE) to minimize contamination and have appropriate personal radiation dosimeters to guide the time they can be exposed to radiation.

#### Figure A5 Exposure Rate from an Externally Contaminated Victim

Figure A5 illustrates how medical personnel might be exposed to radiation from shrapnel embedded in a victim. The closer to the source (the victim's body surface), the more likely doses resulting in ARS could be produced over an hour or so. Exposure rates depend on the radionuclides. For example, Cobalt produces more dose than Iridium, Cesium and Americium at close proximity: Working directly on the victim's body (i.e., at zero distance), the exposure rate for Cobalt-60 is 3,000 mR/hr, about 1,100 mR/hr for Iridium-192, 750mR/hr for Cesium-137, and under 50mR/hr for Americium. Beyond one meter distance, however, even for Cobalt-60, external contamination produces very little exposure to personnel.





- Exposure rate versus distance for various radionuclides considered likely for an RDD.
- Even for Cobalt-60, external contamination produces very little exposure beyond 1 meter.
- The closer to the source, the more likely doses resulting in ARS could be produced over an hour or so.
- Cobalt produces more dose than Iridium, Cesium and Americium.

## Dose limits

- Draft Protective Action Guidelines to guide responses to radiological and nuclear events were published in the Federal Register, January 6, 2006 (Table A6)
- 5 rem total dose is the annual limit for occupational radiation workers doing their normal jobs. This is cumulative dose over time (up to a year). If actual dosimeters are not used, cumulative dose can be estimated based on physical measurements of dose rate by environmental survey meters.
- Higher dose limits are permissible for Emergency Response Workers in certain specific circumstances (Table A6) 25 rem is the guideline limit with only a few exceptions. Above that dose, informed consent is required.
- Local governmental entities and unions may have established different guidelines.
- Pregnant women must avoid exposure. Special counseling will be needed for pregnant victims including efforts to estimate their fetus' exposure.
- In general, the risk of a radiation-induced cancer is 8% for 100 rem (5 rem is less than 1% and 25 rem is about 2%). This is in addition to the background lifetime risk of 30-40%. Radiationinduced cancer has long latency (10-30+ years) so that younger people are at greater risk.



Table A6- Protective Action Guides (PAGs)
(Federal Register, January 2006)

(Federal Reg	(Federal Register, January 2006)				
Phase	Protective Action	Protective Action Guide	Reference		
Early	Limit Emergency Worker Exposure. Sheltering of Public Evacuation of Public Administration of Prophylactic Drugs.	5 rem (or under exceptional circumstances <sup>1</sup> 1 to 5 rems projected dose <sup>2</sup> o 5 rems projected dose <sup>3</sup> For potassium iodide, FDA Guidance dose values <sup>4 5</sup>	EPA PAG Manual EPA PAG Manual EPA PAG Manual FDA Guidance <sup>6</sup>		
Intermediate	Limit Worker Exposure. Relocation of General Public	5 rem/yr 2rems, projected dose first year Subsequent years: 500 mrem/yr projected dose.	EPA PAG Manual		
Late	Food Interdiction Drinking Water Interdiction Final Cleanup Actions	500 mrem/yr projected dose Late-phase PAG based on optimization.	EPA PAG Manual FDA Guidance <sup>7</sup>		

<sup>1</sup> In cases when radiation control options are not available or, due to the magnitude of the incident, are not sufficient, doses above 5 rems may be unavoidable.

<sup>2</sup> Should normally begin at 1 rem; however, shelter may begin at lower level if advantageous.

<sup>3</sup> Should normally begin at 1 rem.

<sup>4</sup> Provides protection from radioactive iodine only.

<sup>5</sup> For other information on medical prophylactics and treatment please refer to http://www.fda.gov/Radiation-EmittingProducts/default.htm, http://www.bt.cdc.gov/radiation/ http://www.orau.gov/reacts. or 6 Potassium lodide As-Α Thyroid Blocking Agency in Radiation mergencies, http://www.fda.gov/ForIndustry/FDAeSubmitter/ucm107871.htm, December 2001, Center or Drug Evaluation and Research, FDA, HHS.

<sup>7</sup> "Accidental Radioactive Contamination of Human Food and Animal Feeds: Recommendations for State and Local Agencies, "August 13, 1998, Office of Health and Industry Programs, Center For Devices and Radiological Health, FDA, HHS.

Table A7 - Protective Action Guides (PAGs)           Response Worker Guidelines					
Total Effective Date Equivalent (TEDE) guideline		Condition			
5 rems	All occupational exposures	All reasonably achievable actions have been taken to minimize dose.			
10 rems*	Protecting valuable property necessary for public welfare (e.g. a power plant)	appropriate actions taken to reduce doep			
25 rems**	Lifesaving or protection of large populations	Exceeding 5 rems unavoidable and all appropriate actions taken to reduce dose. Monitoring available to project or measure dose			



#### Personal Protective Equipment

Avoiding inhalation of radionuclides is critical.

 Appropriate Personal Protective Equipment, including respiratory protection, is necessary for responders who may be exposed to any radionuclides. Improvisation may be necessary for people in the affected zones who do not have appropriate PPE. Even victims in the area should use improvised respiratory protection.

#### Fatality Management

Fatality management and management of radioactive remains will be coordinated through HHS using established guidelines (CDC).

#### Medical Countermeasures

- Detailed medical management guidelines are included on the web portal Radiation Event
  Medical Management
- Local responders should be encouraged to use REMM for medical guidelines.
- Diagnostic assessment of victims potentially exposed to and internally contaminated by radiation is essential. This includes but is not limited to:
  - History, physical examination, hematology (blood counts) and blood chemistry evaluation.
  - The CDC Laboratory Response Network may be needed to supplement local/state/regional/tribal resources.
  - Special analysis may be required (e.g. nasal swabs, skin or hair swabs urine or feces) to determine presence of radiation and possibly the identification of the specific radionuclide. Internal contamination requires accurate analysis and usually repeated sampling for appropriate clinical management. The size of the event and potential number of victims will be used to determine how to utilize the limited laboratory assay capabilities. For example, nasal swabs, skin or hair swabs might be done for a small-sized event, but not a large one.
  - These analyses will be coordinated through the Centers for Disease Control (CDC) Radio-bioassay laboratory.
  - Low levels of contamination will not need treatment. Therefore, bioassay (to measure the type of radionuclide) and dose calculation (with biodosimetry) are important in knowing which patients need therapy. If empirical treatment is started before measurements are available, as might be done with DTPA (plutonium, americium) or Prussian Blue (Cesium), the treatment course may be discontinued if unnecessary.
  - Currently, CDC has limited capacity to provide bioassay results. If the number of casualties is large, the laboratory capacity may be insufficient, and patients will be managed clinically.
  - Annual limit on intake (ALI) is the derived limit for the amount of radioactive material taken into the body by inhalation or ingestion in a year. ALI is the value of intake of a given radionuclide in a year that would result in a committed effective dose equivalent of 5 rem (0.05 Sievert) or a committed dose equivalent of 50 rem (0.5 Sievert) to any individual organ or tissue (adapted from Nuclear Regulatory Commission). In general, treatment for internal contamination is given is 10 times the ALI is calculated.
  - Most authorities do not recommend treatment of internal contamination when the body burden is less than one annual limit of intake (ALI). Treatment is strongly recommended when the body burden exceeds 10 ALI. For internal contamination levels greater than 1 ALI and less than 10 ALI, clinical judgment dictates treatment of internal contamination.



- If there is concern about a possible diagnosis and need for treatment of Acute Radiation Syndrome, monitoring of blood counts and possibly special biodosimetry analysis (if available) may be needed.
- Specific treatments are available for particular radionuclides as listed below. The identification of the radionuclide is important so that unnecessary toxicity is avoided.

Table A8. Examples of radionuclides and medical countermeasures           (See REMM.nlm.gov for details, also in Briefing papers)				
Radionuclide Medical countermeasure Procured through				
Cesium	Prussian Blue	Local institutions and commercial vendors SNS		
Plutonium, Americium	DTPA	Local institutions for Ca-DTPA and some Zn-DTPA SNS can provide Zn-DTPA and restocking		
Strontium	Calcium, ammonium chloride, other	Commercial vendors		
lodine	Potassium iodide	Commercial vendors		

- **Not all victims with internal contamination require treatment.** Many countermeasures have an unfavorable risk-to-benefit ratio when used to treat persons having low levels of internal contamination.
- An event with radioactive iodine would require appropriate identification (by determination through, survey or interview of likely proximity or ingestion or inhalation) of exposed children and young adults so KI could be provided to prevent later development of thyroid cancer. Administration must be started promptly, ideally by 4-5 hours. Most of the efficacy is lost if more than 12 hours have transpired. KI is not indicated for other radionuclides.
- The development of Acute Radiation Syndrome severe enough to require countermeasures for treatment is unlikely for those receiving whole body doses below 2 Gy. Individuals who receive a cumulative whole body dose of >2 Gy and < 3Gy need to be monitored very closely, as they may need treatment for ARS. Those suspected of having received a dose above 3 Gy probably need prompt medical intervention with "mitigating agents" such as hematological growth factors for granulocytes. Other ARS agents are in development. Management details are in REMM.

#### Managing Potential Long-Term Medical Consequences: Fear of Cancer

- The disruptive aspect of an RDD will quickly become the major aspect of this event including health fears, economic loss, and infrastructure disruption. The major health fear is likely to be the "perceived risk" of the inevitability of developing a radiation-induced cancer.
- Fear of damage to fetuses and concerns about genetic mutations that could be passed along to future generations will likely arise as well. These fears are best addressed by education including public media presentations and also by regional face-to-face meetings with medical and epidemiological experts.
- It is possible that there will be suspicion of any comments from government officials who are
  not medical experts, so HHS will try to use academic and medical radiation experts. These
  include staff from the National Cancer Institute, CDC, NIH, epidemiologists involved in the
  Japanese atomic bomb studies including the Japanese Radiation Effects Research Foundation
  (REFR) and from the Chernobyl studies. Other international experts may be called upon.
- For those victims who had potential for low dose exposure, cytogenetic biodosimetry studies
  may be conducted. Radiation produces characteristic chromosome changes in white blood
  cells (called dicentrics) that are stable for many years so that the Radiation Laboratory
  Response Network (Rad-LRN which is still being established) could study potential victims and
  correlate the number of dicentrics with estimated dose (see REMM).



- Given the time and expense of these tests, only those who were clearly within a zone in which exposure may have been relatively high and those who had suspected contamination determined by a health physicist will be subject to study. While the exact cut-off would be determined at the time of the event, a suspected dose of less than 50 75 cGy (rem) would not require study as this would raise the lifetime risk by about 4% at most. Age would also be a factor in deciding whom to study. Emphasis on studying young people is important because the latency for radiation-induced cancer is usually at least one decade, often 3 or more. Other medical factors would be considered regarding biodosimetry study and the need and type of long-term screening.
- As has been learned with genetic testing for cancer risk, many people do not want to know if they are at increased risk for developing a disease or illness. It may be that lifestyle changes (no smoking) and routine recommended medical screening test (colonoscopy, mammograms) may be the mainstay of medical follow up. There may be insurance coverage issues should a victim be determined to be at higher risk so that legal protection and privacy must be considered.
- **Recovery:** Decisions about reoccupation of the involved area, clean-up and even transient entry to remove valuables and personal items will be made by the local/regional government, expert consultants and citizens. The relative risks, expense, time, and possibility for site clean up should be determined as clearly and as quickly as possible to expedite the community's recovery. Agencies involved in these discussions would be EPA, DHS, HHS and others.
- ESF #14 will assume a lead role as the recovery phase ramps up. Interagency PAGs should be consulted as in Table A6 (Draft PAGs from Federal Register).

## Population Monitoring

## What is the Role Specified in the National Response Framework for HHS?

- The text directly addressing this topic is found in the Nuclear/Radiological Incident Annex (June '08), page NUC-22, under "Population Monitoring" and "Population Decontamination" (emphasis added):
- "The Department of Health and Human Services (HHS), through ESF #8 Public Health and Medical Services and in consultation with the coordinating agency, coordinates Federal support for external monitoring of people.
- HHS, through ESF #8 and in consultation with the coordinating agency, coordinates Federal support for population decontamination.
- HHS assists and supports State, tribal, and local governments in performing monitoring for internal contamination and administering available pharmaceuticals for internal decontamination, as deemed necessary by State health officials.
- HHS assists local and State health departments in establishing a registry of potentially exposed individuals, performing dose reconstruction, and conducting long-term monitoring of this population for potential long-term health effects."

## What the Centers for Disease Control and Prevention (CDC) have done to date.

- CDC hosted a roundtable in Atlanta on population monitoring with participants from Federal agencies, state and local health departments, academia and many professional organizations.
- CDC chairs a small interagency working group of technical experts to discuss practical aspects
  of population monitoring. The working group has provided CDC with significant input on the
  topic.
- CDC has prepared a planning guide for state and local public health planners highlighting the many challenges in a mass casualty radiation incident and suggesting ways to address those challenges.
- CDC is preparing a public health toolkit with a video segment on population monitoring.



• CDC is planning on developing a planning decision tool (software) for optimizing the design and operation of community reception centers used to screen population in mass casualty radiation emergencies. This is based on the concept of PODs (points of dispensing) and will use field data on radiation screening.

## What needs to be done next?

- Identify, and solidify Interagency Agreements with, Federal resources that can be made available to assist with population monitoring, i.e., clarify what constitutes the "Federal support" that HHS is responsible to coordinate.
- Remain proactive in coordinating with all identified resources. This includes the Commissioned Corps, Medical Reserve Corps, or other assets that can be used to assist with population monitoring. Coordination with all these resourced needs to be done proactively in the specific context of population monitoring.
- Conduct a national radiation exercise with an ESF #8 focus on Population Monitoring issues. To date, many radiation exercises conducted locally or nationally lack such emphasis. Population monitoring issues are especially overlooked and challenges underestimated.

## Common response phase terminology

- **Phases of Response** (from Federal Register PAGs, January 2006). These are verbatim definitions. Note: our response plans are tied to hours/days after the event so that these terms are useful but not used specifically in our CONOPS.
  - The early phase (or emergency phase) is the period at the beginning of the incident when immediate decisions for effective use of protective actions are required and actual field measurement data is generally not available.
  - **The intermediate phase** of the response may follow the early phase response within as little as a few hours. The intermediate phase of the response is usually assumed to begin after the source and releases have been brought under control and protective action decisions can be made based on measurement of exposure and radioactive materials that have been deposited as a result of the incident.
  - **The late phase** is the period when recovery and cleanup actions designed to reduce radiation levels in the environment to acceptable level area commenced, and it ends when all the recovery actions have been completed.

Casualties	180 fatalities 270 injuries 20,000 detectible contaminations (at each site)				
Infrastructure Damage	Near the explosion				
Evacuations/Displaced Persons	<ul> <li>10,000 evacuated to shelters in safe areas (decontamination required prior to entering shelters)</li> <li>25,000 in each city are given shelter-in-place instructions</li> <li>Hundreds of thousands self-evacuate from major urban areas in anticipation of future attacks</li> </ul>				
Contamination	36 city blocks (at each site)				
Economic Impact	Up to billions of dollars				
Potential for Multiple Events	Yes				

## National Planning Scenario #11

Casualties	180 fatalities 270 injuries 20,000 detectible contaminations (at each site)
Recovery Timeline	Months to years

Scenario Overview

## **General Description**

In this scenario, the Universal Adversary (UA) purchases stolen cesium chloride (CsCl) to make a radiological dispersal device (RDD), or "dirty bomb." The explosive and the shielded cesium-137 (<sup>137</sup>Cs) sources are smuggled into the Country. Detonator cord is stolen from a mining operation, and all other materials are obtained legally in the United States. Devices are detonated in three separate, but regionally close, moderate-to-large cities.

<sup>137</sup>Cs is mostly used in the form of CsCl because it is easy to precipitate. CsCl is a fairly fine, light powder with typical particle size median at about 300 microns. Fractions below 10 microns are typically less than 1%. In an RDD, most will fall out within approximately 1,000 to 2,000 feet (although many variables exist), but a small amount may be carried great distances, even hundreds of miles.

## **Detailed Attack Scenario**

The UA, having learned from press and scientific reports how to make an RDD, activates a U.S.-based cell to carry out attacks on U.S. cities. The UA chooses <sup>137</sup>Cs because of its availability, high radioactivity, high dispersability, and the difficult nature of cleanup and remediation. The UA's goal is to conduct a highly visible attack creating fatalities, fear, and social and economic disruption.

The U.S. cell spends several years slowly acquiring a large quantity of prilled ammonium nitrate (NH<sub>4</sub>NO<sub>3</sub>). UA members plan attacks on three significant cities in regional proximity. Via black-market contacts, the foreign cell purchases three stolen seed irradiators that each contains approximately 2,300 curies of CsCl and several kilograms of highly explosive Pentaerythritol Tetranitrate (PETN). The CsCl powder is removed from its containment, transferred to plastic zip-lock bags, and placed in heavy lead-shielding containers. The explosive and the shielded <sup>137</sup>Cs sources are smuggled into the country in sea-land containers shipped separately to a U.S. port under assumed business names. Detonator cord is stolen from a mining operation without raising concern, and all other materials are obtained legally in the United States.

The sea-land containers are picked up and transferred to safe houses near the target cities, where rented vans await containing the ammonium nitrate and containers of fuel oil. The vans have been painted to appear as commercial delivery vehicles. At the safe houses, terrorists assemble the devices by carefully mixing the Ammonium Nitrate with Fuel Oil (ANFO; 95:5 by weight) inside the truck and fixing the detonator with a 0.5-kilogram highly explosive core as a booster. The total explosive yield in each device will be approximately 3,000 pounds. Because each radiation source gives off 760 rad per hour (at 1 meter), the sources are left in their lead containers until the final minutes—at that time, they are transferred to the van and inserted down into the explosive mixture. The vans arrive at the target downtown locations in the U.S. cities. Three to five individuals are involved in executing each attack.

At 11:15 a.m. during the school year, UA members detonate the 3,000-pound truck bomb containing the 2,300 curies of <sup>137</sup>Cs in the downtown business district of City One. The explosion collapses the front of one building and causes severe damage to three others. Windows are blown out of five other buildings. The area is contaminated with <sup>137</sup>Cs, and the contaminated detonation aerosol is lifted more than 100 feet into the air.

A similar scene plays out in two other moderate-to-large cities. The second and third explosions are timed to go off simultaneously in City Two and City Three, at approximately 12:30 p.m. on the same day. The time lag is intended to maximize press coverage and spread fear and uncertainty. Local firstresponse capacity, however, is depleted in City Two and City Three, because many responder assets have been dispatched to assist nearby City One with the response.

## Planning Considerations:

## **Geographical Considerations/Description**

The three cities are regionally close. They are physically similar (for the sake of this assessment), with similar building environments and geographic topography that is essentially flat. The results in each city are essentially the same. The contaminated region covers approximately 36 blocks in each city and includes the business district (high-rise street canyons), residential row houses, crowded shopping areas, and a high school. Buildings in the affected areas are principally made of concrete and brick; some are stone faced. Building heights in the entire affected area range from 2 to 20 stories, and buildings in the immediate vicinity of the blast are 8 to 16 stories. The area within a radius of five blocks of the blast is a narrow urban canyon of medium-to-tall buildings abutting sidewalks, and streets are approximately 40 feet wide.

The entire scene is contaminated with <sup>137</sup>Cs, though not at levels causing immediate concern to first responders. Due to the size of the explosion, the radioactive contamination is blown widely such that the ground zero area is not as radioactive as might have been expected. The detonation aerosol contains 90% of the original <sup>137</sup>Cs source with radioactive particles whose sizes range from 1 to 150 microns the size of most of the particles is approximately 100 microns. Larger particles either penetrate building materials in the blast zone or drop quickly to the ground as fallout within about 500 feet.

Variable winds of 3 to 8 miles per hour carry the radioactively contaminated aerosol throughout an area of approximately 36 blocks (the primary deposition zone). Complex urban wind patterns carry the contamination in unpredictable directions, leaving highly variable contamination deposition with numerous hot spots created by wind eddies and vortices. Radioactivity concentrations in this zone are on the order of 5 to 50 microcuries/m2, with hot spots measuring 100 to 500 microcuries/m2; however, traces of the <sup>137</sup>Cs plume carry more than 3.5 kilometers (~ 2.2 miles) on prevailing winds. Negative indoor building pressure draws radioactive aerosols into buildings via cracks around windows and doors. Exterior air intakes increase the contamination in the interior of larger buildings. In City One, the subway system is contaminated by radioactive aerosols entering through subway ventilation system air intakes.

In all cities, foot and vehicular traffic after deposition re-suspend and transfer contamination for hours afterward until the entire scene has been effectively controlled and cordoned, contributing to contamination spread beyond the 36-block primary deposition zone. People who were in the deposition zone also take contamination home with them in hair and clothing.

#### **Timeline/Event Dynamics**

The attacks have no advance notice or intelligence that indicates their possibility. The explosions are instantaneous, but plume dispersion continues for 20 minutes while breezes navigate the complex environments before particles have fully settled. First responders do not recognize radioactive contamination for 15 minutes in City One. The explosions in City Two and City Three are promptly identified as "dirty bombs"-this provides some advantage to first responders and government officials in managing contamination on-scene, and in communicating with the public concerning topical contamination and spread of contamination.



227

## Assumptions

- As a result of the explosions, 90% of the 2,300-curies <sup>137</sup>Cs source is aerosolized and carried by winds, with radioactive particles ranging in size from 1 to 150 microns. The remaining fallout creates debris and contaminates surrounding structures.
- There is no precipitation. There are light, variable winds of 3 to 8 mph. The temperature is 65° F.
- The port of entry through which the smuggled materials enter is not equipped with radiation detection equipment that can detect the shielded <sup>137</sup>Cs source. The target and surrounding access routes are not equipped with radiation sensors that can detect the shielded source. The acquisition of bomb-making materials does not draw the attention of law enforcement.
- First responders from City Two and City Three assist City One.
- A disposal facility is available for cleaning up waste.

## **Mission Areas Activated**

#### Prevention/Deterrence:

Prevention efforts should include such law enforcement goals as prevention of trafficking and importation of CsCl and weapon components, reconnaissance of the site, protection, and deterrence measures taken at the site before and during the attack. Target and surrounding access routes are not equipped with radiation sensors that can detect the shielded source. DHS would be involved in detection of the shielded <sup>137</sup>Cs radiation sources.

## Emergency Assessment/Diagnosis:

The explosion in City One is not recognized as a "dirty bomb" until responding units arrive with gamma detection equipment. This leads to contamination of first responders and inadvertent contamination spread that might have otherwise been avoidable. The downwind aerosol dispersion will be a significant component of the hazard and will cause extended local and regional disruption. Actions of incident-site and EOC/Joint Field Office (JFO) personnel tested during and after the attack include providing personnel dispatch; assessing the extent of physical damage, including engineering assessments of buildings; assessing medical response needs; detecting and identifying the radiation source; establishing and preserving the site for crime scene analysis; collecting site data and information; making hazard assessments and predictions for responders and the public; and coordinating preliminary radiation monitoring, surveying, and sampling operations.

## Emergency Management/Response:

Incidents result in 180 fatalities, 270 injuries, extensive environmental contamination, evacuation of thousands of individuals, and thousands of potentially exposed individuals in the downwind zone. Actions of EOC/JFO personnel required after the attack include mobilizing and operating incident command; overseeing victim triage; stabilizing the site; cordoning the site and managing and controlling the perimeter; providing notification and activation of special teams; providing traffic and access control; providing protection of at-risk and special populations; providing resource support and requests for assistance; providing public works coordination; providing direction and control of critical infrastructure mitigation; and providing public information, outreach, and communication activities.

Because first-responder assets (e.g., medical evacuation, fire, rescue, and EMS personnel) were promptly dispatched from nearby City Two and City Three to assist City One, City Two and City Three are low on response capacity, and officials find themselves unprepared when attacks strike their cities.

#### Hazard Mitigation:

Required actions of incident-site personnel include isolating the incident scene and defining the hazard areas, building stabilization, providing fire suppression, conducting debris management, conducting radioactive and hazardous contamination mitigation, decontaminating responders and equipment, conducting local-site contamination control, and decontaminating local citizens.

#### Evacuation/Shelter:

Evacuation and/or sheltering of downwind populations will be required. This must occur promptly and in an orderly fashion, but will likely not occur before the plume has passed and settled, given the lack of warning. Actions taken by Federal, State, and local EOC/JFO personnel performed after the attack include developing protective action recommendations and communicating them to the public (e.g., to evacuate the affected area and/or shelter-in-place, as appropriate, and self-decontamination); providing management of evacuation, whether ordered or spontaneous; protecting special populations, schools, and day care centers; establishing temporary sheltering alternatives and provision of food for evacuees; and offering veterinary services for pets.

#### Victim Care:

Injured people will require some decontamination in the course of medical treatment and, if possible, prior to hospital admission. Thousands more will likely need superficial decontamination and both short-term and long-term medical follow-ups. Actions of incident-site, local-area, hospital, and EOC/JFO personnel tested after the attack include conducting search and rescue; providing triage, emergency aid, treatment, and stabilization; decontaminating victims (ambulatory and non-ambulatory); establishing relief stations, impromptu decontamination centers, and site access portals; screening, monitoring, and decontaminating evacuees (numbers are expected to be up to 100,000 at each site); conducting victim/evacuee data and information collection and management; making radio-protective pharmaceutical decisions and efficiently providing protective and/or therapeutic drug administration; conducting patient status tracking and reporting; providing patient transport; treating ER walk-in radiation victims; providing hospital care; providing collection, decontamination, and cataloging of human remains and personal effects; and providing next-of-kin notification.

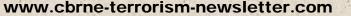
#### Investigation/Apprehension:

Actions of law enforcement personnel tested after the attacks include dispatching personnel, conducting site cordoning and control, collecting field data, conducting witness interviews, and performing tactical deployment and apprehension of suspects. Reconstruction of the attack will occur and will include information about the occurrence of importation of illicit materials, acquisition of materials within the United States, planning, movements, financial backing, communications, suppliers/accomplices tracking, and suspect apprehension.

#### Recovery/Remediation:

**Decontamination/Cleanup:** The extent of contamination will be a major challenge, because <sup>137</sup>Cs is highly water soluble and is chemically reactive with a wide variety of materials, including common building materials such as concrete and stone. Approximately 36 city blocks will be contaminated to varying degrees. Contamination will settle on streets, sidewalks, and building surfaces, and will be found in several kilometers of the subway system (City One). Building interiors will become contaminated due to ventilation systems, doors, windows (because negative building pressure can draw aerosols in through very small openings), and foot traffic. Personal property—including vehicles and items inside buildings—will also become contaminated, but many items can be adequately decontaminated for free release.





A summary of decontamination and cleanup activities is as follows:

- Some demolition will likely be required, but most surfaces may be systematically decontaminated to low levels (a lengthy, costly process).
- Officials may focus decontamination work first on critical infrastructure—such as major thoroughfares, the subway, and the water treatment plant—in order to restore basic functions as quickly as possible.
- Streets with cracks are cut, refilled, and resurfaced; some must be completely removed and repaved.
- Most sidewalks must be surface cleaned.
- Roofing materials are mostly removed, and roofs are resurfaced.
- Surface soil and vegetation are removed for disposal and replaced with fresh material.
- Exterior surfaces are decontaminated with an assortment of chemical treatments (e.g., stripping, vacuum blasting, scabbling), and collected wastes are hauled off for disposal.
- Contaminated building interiors are mostly stripped of surface coatings, carpet, drapery, furniture, etc., and are refurbished.
- Workers try to capture decontamination wastes for disposal, but much will escape into storm drains with each spring rain. Sewers become contaminated. Some are cleaned of hot spots, but others may be left fairly contained if cleaning them is not justified.
- Though concentrations are low, river sediment remediation will likely become a big issue with the public.

**Site Restoration:** Several buildings (those most damaged) will be torn down and eventually rebuilt. Decontamination activities are undertaken for building exteriors and interiors, streets, sidewalks, and other areas. Federal, State, and local officials and stakeholders hold numerous public meetings to evaluate current and future land use goals, dose/risk goals for the site, and the possible use of institutional controls if decontamination is unsatisfactory. Economic and tax incentives may need to be instituted, and Federal, State, and local governments might start a "save our city" campaign to build community support to reclaim and revitalize the area. (A heated debate is likely to ensue in public meetings and the press over the adequacy of site restoration goals and the resultant risks to the public, presenting major communication and negotiation challenges to local, State, and Federal officials.)

#### Implications

#### Secondary Hazards/Events

Small fires from ruptured gas lines occur in the vicinity of the blasts. Unstable building facades, rubble, and broken glass create physical hazards for rescue workers. Small amounts of lead, asbestos, and Polychlorinated Biphenyls (PCBs) are present in the air and on surfaces. Human remains present a biohazard, and some of these may be radioactive.

#### Fatalities/Injuries

At each site, the blast results in 180 fatalities and about 270 injured requiring medical care. In addition, up to 20,000 individuals in each primary deposition zone potentially have detectable superficial radioactive contamination. Most of them also have internal contamination via inhalation and secondary ingestion. Most cases are seen in City One. In each city, tens of thousands of people located downwind have minor external and internal contamination and will require monitoring and medical surveillance.

#### Property Damage

In each blast, one building and 20 vehicles are destroyed (i.e., not salvageable), and eight other buildings suffer varying degrees of damage, such as minor structural damage and broken windows. Radioactive contamination is found inside buildings as well as on building exteriors, streets, sidewalks,

people, and personal property over an area of approximately 36 blocks in each city. Minor contamination may be an issue further downwind as investigators perform more thorough surveys. Most of the subway system in City One is contaminated.

Over the long term, decontamination efforts are expected to be effective, but some property owners choose demolition and rebuilding. Many square blocks will be unavailable to businesses and residents for several years until remediation is completed.

## Service Disruption

Transportation is severely hampered in each city. Bus, rail, and air transportation routes are altered, and officials build highway checkpoints to monitor incoming traffic for contamination. The subway system in City One, which carries 500,000 passengers a day, is completely or partially closed for an extended period. In each city, the entire contaminated zone is closed to all traffic for an extended period (though peripheral areas and some thoroughfares are opened within several weeks for limited use). Hospitals in each region, already at maximum capacity with injuries from the blasts, are inundated with up to 50,000 "worried well," most of whom were not in the blast or plume zone but are concerned about health issues (despite special relief stations established by the incident command for contamination monitoring and public outreach).

The sewage treatment plant is quickly contaminated as a result of people showering and decontaminating personal effects. In each city, 75 businesses are closed for an extended duration while radioactive contamination is remediated. Local tax revenues plummet, and people discover that insurance claims are rejected. The schools in the contamination zones are closed, and students meet in alternate locations. Nearby towns and cities close their doors to residents of the impacted cities for fear of contamination spread. Bus, rail, and air transportation routes are altered, and officials build highway checkpoints to monitor incoming traffic for contamination.

If one of the events occurred near a border, there would be a need for intense communication and cooperation between the two border governments that would engage their respective foreign affairs organizations and the full range of other Federal, State, and local agencies. In addition, the RDD attacks may warrant limiting access to or closing U.S. borders, which would have an immediate effect on Mexico and Canada.

## Economic Impact

Although technologies exist to decontaminate areas, these technologies were designed for smaller, isolated areas, and the process may take several years. Decontamination, destruction, disposal, and replacement of lost infrastructure will be costly (i.e., hundreds of millions of dollars per site). Economic losses in the area due to lost business productivity, tax revenue, and property will be significant. The entire contaminated area may be economically depressed for years.

Additionally, an overall national economic downturn may occur in the wake of the attack due to a loss of consumer confidence. Virtually all commercial insurance policies exclude radioactive contamination, so the Federal Government will be left with a massive bailout. Total economic impacts would almost certainly be in the billions of dollars. Some residents will show no signs of willingness to resettle their former domiciles. Schools may permanently relocate. Some businesses may relocate to an unaffected zone or another city altogether. However, depending on the city; its size; and its historical, economic, and political significance, the will to recover and repopulate would vary widely from long-term decline to complete revitalization.

## Long-Term Health Issues

The following is a summary of human health issues likely to occur over the long term:



- No one will suffer acute radiation syndrome.
- Approximately 20,000 individuals are likely to become externally contaminated at each site. A
  high percentage of these (perhaps 40% to 60%) will have measurable internal contamination
  via inhalation and primary and secondary ingestions that require treatment. Low-level
  contamination may enter food and water supplies and may be consumed at projected doses
  below EPA Protective Action Recommendations. The sum of the cumulative exposures results
  in an increased lifetime cancer risk proportionate to the dose.
- All exposed individuals will need to be monitored for health outcomes over their lifetimes, especially those that suffer internal contamination.
- Many individuals, including those close to but not within the affected area, will require mental health counseling for an extended period of time. First responders make up a unique group often in need of mental health services. The total number in need of mental health services may be on the order of 5,000 to 20,000 per site.

**NOTE:** Read or download the rest of these guidelines from the "Terror Medicine" section at Newsletter's website. Look for the banner of US Public Health Emergency.

## Molecules could help solve radioactive waste concerns

Source:http://www.homelandsecuritynewswire.com/molecules-could-help-solve-radioactive-waste-concerns

One component of nuclear waste -- called "minor actinides" -- present an extreme hazard as they are intensely radioactive and long-lived nuclides; they must be safely stored for at least 100,000 years; researchers have discovered a class of molecules that can selectively extract minor actinides, making the eventual waste far less radiotoxic.

The problem of storing some of the most radioactive elements of nuclear waste could be close to being solved thanks to experts from the University of Reading.

Researchers in the Department of Chemistry have discovered a class of molecules that can selectively extract extremely radioactive components – "minor actinides" — that remain after spent fuel has been reprocessed, making the eventual waste far less radiotoxic. The minor actinides can potentially be fed back into nuclear reactors, providing extra energy and, in turn, be converted to non-radioactive products.

A University of Reading release reports that the U.K. nuclear power industry produces about 10,000 megawatts of power each year. Although the vast bulk of the spent fuel from a reactor can be reprocessed and fed back into the fuel cycle, a residue, consisting of corrosion

products, lanthanides, and minor actinides, must be sent to storage.

For every 500 kg of spent fuel, there is 15 kg of waste, of which the minor actinides, such as americium, curium, and neptunium, constitute less than 1 kg. These, however, present an extreme hazard as they are intensely radioactive and long-lived nuclides that cause serious concern when it comes to storing them for more than 100,000 years.

Professor Laurence Harwood, who led the research at Reading, said: "The minor actinides are highly radioactive and have half lives up to millions of years. If these can be removed they could be used as fuel in the new generation of nuclear reactors that will come on-stream around 2025 and converted to non-radioactive material. Being able to separate out the minor actinides even now already makes storage simpler and reduces the security risk as well.

"Our research has produced molecules capable of removing 99.9 percent of the minor actinides left after reprocessing spent fuel, ensuring much smaller levels of radioactive waste would accrue and remain hazardous for a much shorter period of time; a few hundred years, rather than effectively forever."

- Read more in F. W. Lewis et al., "Highly efficient separation of actinides from lanthanides by a phenanthroline-derived bis-triazine ligand" (a paper at the Central Archive at the University of Reading, 2011)



# Iran runs nuclear missile payload tests, moves onto 60 pc fuel enrichment

Source: http://www.debka.com/article/21271/

The UN International Atomic Energy Agency Friday, Sept. 2 stressed its increasing concern



"about the possible existence in Iran of past or current undisclosed nuclear-related activities involving military-related organizations, including activities related to the development of a nuclear payload for a missile, about which the Agency continues to receive new information."

The nuclear watchdog was also alarmed by three disclosures made by Fereydoon Abbas, head of Iran's atomic energy agency, Monday, Aug. 29, attesting to the speeding-up of its military nuclear program and preparations for a possible attack on its installations.

1. Abbasi boasted that Iran's nuclear fuel production already far exceeded its needs. debkafile's military sources report that this first public announcement meant that Tehran was about to move on from 20 percent enriched uranium to 60 percent – the last step before the 90 percent enrichment for weapons-grade fuel. According to several sources, Iran has already stocked 4,500 kilograms of low-enriched uranium, which would be enough for four nuclear weapons after further enrichment.

2. Abbas pronounced "dead" the 2009 proposal for the West to supply Iran with new fuel for its small research reactor in return for

an end to Iranian production of the fuel. "We will no longer negotiate a fuel swap and a halt to our production of fuel," he said.

3. The head of Iran's atomic agency also revealed the imminent transfer of its critical enrichment facilities from Natanz to a heavily fortified subterranean facility near the holy city of Qom to keep it safe from air, missile and cyber attack.

#### Advanced IR-2m centrifuge

Tehran has made it clear that the facility will not be open to international oversight and will use the most advanced centrifuges – IR-4 and IR-2m - for speeding up the production of highly-enriched uranium.

Western intelligence sources estimated Sunday, Sept. 4, that Iran's advances had brought forward to the spring of 2012 the potential completion of between two and four bombs and the ability to conduct a nuclear test.

At the White House, Tommy Vietor, a spokesman for the National Security Council said that the Iranian plan "to install and operate centrifuges at Qom is a violation of their United Nations security obligations and another provocative act."

While demonstrating the arrogance of a wouldbe global nuclear power, Iran suffered an unexpected diplomatic snub Sunday, Sept. 4, when parliamentary speaker Ali Larijani was informed at the last minute that he would not get to meet the Chinese and North Korean heads of state when he visited Beijing and Pyongyang - only low-ranking officials. He thereupon cancelled his trips. China and North Korea appear to have decided to keep their distance from the nuclear miscreant in Tehran. Last Wednesday, Aug. 31, French President Nicolas Sarkozy warned, "Iran's attempts to build long-range missiles and nuclear weapons could lead unnamed countries to launch a preemptive attack."



# New materials hold promise for better detection of nuclear weapons

Source:http://www.homelandsecuritynewswire.com/new-materials-hold-promise-better-detection-nuclear-weapons

Researchers have developed new materials that can detect hard radiation, a very difficult thing to do; the method could lead to a handheld device for detecting nuclear weapons and materials, such as a "nuclear bomb in a suitcase" scenario

Northwestern University



scientists have developed new materials that can detect hard radiation, a very difficult thing to do. The method could lead to a hand-held device for detecting nuclear and weapons materials. such as a "nuclear

bomb in a suitcase" scenario.

"The terrorist attacks of 9/11 heightened interest in this area of security, but the problem remains a real challenge," said **Mercouri G. Kanatzidis** (photo, left), who led the research. "We have designed promising semiconductor materials that, once optimized, could be a fast, effective and inexpensive method for detecting dangerous materials such as plutonium and uranium."

Kanatzidis is a Charles E. and Emma H. Morrison Professor of Chemistry in the Weinberg College of Arts and Sciences. He also holds a joint appointment at Argonne National Laboratory.

The Northwestern materials perform as well as materials that have emerged from five decades of research and development, Kanatzidis said.

A Northwestern University release reports that to design an effective detector, Kanatzidis and his team turned to the heavy element part of the periodic table.

The researchers developed a design concept to make new semiconductor materials of heavy elements in which most of the compound's electrons are bound up and not mobile. When gamma rays enter the compound, they excite the electrons, making them mobile and thus detectable. And, because every element has a particular spectrum, the signal identifies the detected material.

The method, called dimensional reduction, will be published in the 22 September issue of the journal *Advanced Materials*.

In most materials, gamma rays emitted by nuclear materials would just pass right through, making them undetectable. Dense and heavy materials, such as mercury, thallium, selenium, and cesium, absorb the gamma rays very well, however.

The problem the researchers faced was that the heavy elements have a lot of mobile electrons. This means when the gamma rays hit the material and excite electrons the change is not detectable.

"It's like having a bucket of water and adding one drop — the change is negligible," Kanatzidis explained. "We needed a heavy element material without a lot of electrons. This doesn't exist naturally so we had to design a new material."

Kanatzidis and his colleagues designed their semiconductor materials to be crystalline in structure, which immobilized their electrons.

The materials they developed and successfully demonstrated as effective gamma ray detectors are cesium-mercury-sulfide and cesium-mercury-selenide. Both semiconductors operate at room temperature, and the process is scaleable.

"Our materials are very promising and

competitive," Kanatzidis said. "With further development, they should outperform existing hard radiation detector materials. They also might be useful in biomedicine, such as diagnostic imaging."



The work was a Northwestern team effort, involving three professors and their research groups. Kanatzidis made the materials; Bruce W. Wessels, the Walter P. Murphy Professor of Materials Science and Engineering in the McCormick School of Engineering and Applied.

Science, measured and evaluated the materials; and Arthur J. Freeman, a Charles E. and Emma H. Morrison Professor of Physics and Astronomy in Weinberg, provided

theoretical predictions of the materials' performance.

DHS and the Defense Threat Reduction Agency supported the research.

— Read more in John Androulakis et al., "Dimensional Reduction: A Design Tool for New Radiation Detection Materials," Advanced Materials 922 September 2011)

## **Detecting contraband radioactive material**

Source: http://www.homelandsecuritynewswire.com/detecting-contraband-radioactive-material

Researchers at the University of New Hampshire's Space Science Center (SSC), in partnership with Michigan Aerospace Corporation, have been contracted by the federal Defense Threat Reduction Agency (DTRA) to build a highly sensitive instrument that will detect illicit radioactive materials with pinpoint accuracy from a safe distance. Such materials, located in shipping ports, train stations, truck stops, or warehouses, potentially could be used to make dirty bombs or associated with a nuclear device itself.



James Ryan beside the Portable Neutron Spectroscope (NSPECT). The instrument was conceived, designed, and tested to image and measure sources of neutron radiation. Photo by Kristi Donahue, UNH-EOS

The one-year contract of \$303,000 will include a realistic field test of the device's capabilities in 2012.

A University of New Hampshire release reports that the Portable Neutron Spectroscope, or NSPECT for short, is a next-generation instrument based on those originally designed and built at the SSC for space-based missions studying high-energy neutrons and gamma rays emanating from the sun and distant astronomical objects. NSPECT will have the capability to detect, make an image of, and identify hazardous and dangerous nuclear materials because such sources emit radiation similar to that in space. The device will be useful for security and proliferation deterrence, as well as for nuclear waste characterization and monitoring.

"This type of capability doesn't exist at the moment," says lead scientist James Ryan of the UNH Institute for the Study of Earth, Oceans, and Space and the department of physics. Ryan adds, "There are several designs in development in the United States but, basically, what people have to do now is go into a building or a container and fish around in hopes of finding the source. The expertise that has been acquired over many years in the space program can now be brought to bear on this problem to better find and locate nuclear bomb-making material."

DTRA is the U.S. Department of Defense's official combat support agency for countering weapons of mass destruction, and its programs include basic science research and development.

"The funding from DTRA enables us to significantly advance the NSPECT technology and accelerate its deployment," says Dominique Fourguette, chief technology officer at Michigan Aerospace. "One of our primary goals is to produce a robust instrument that can be put to use as quickly as possible," she adds.

To build the instrument, UNH says it is leveraging forty years of experience conducting space-based neutron and gamma-ray detection, with university scientists and engineers developing all the related instrument hardware and software.

Michigan Aerospace is responsible for the support engineering that will turn the bench-top instrument into a rugged field-deployable device equipped with a nimble graphical user interface and live video imaging capability.

NSPECT will have the capability to detect both gamma rays and neutrons but it is the neutron detection that is of greatest interest to DTRA

Unlike other forms of radiation, such as gamma rays, penetrating neutron emission is very uncommon and neutrons are by their nature resistant to detection and defy easy imaging. Indeed, for every one neutron that can be detected 10,000 hurtle past unseen. And when detection is achieved, extracting any meaningful information about the particle is challenging. And therein lies the key to the neutron detector.

While a Geiger counter simply clicks at a higher rate the closer it is to a source of radiation and cannot filter out the ever-present background radiation, the neutron camera discreetly records every neutron that interacts with the instrument and puts each one in a specific "bucket" based on what direction that neutron came from. The buckets are then emptied and, using software developed at SSC, the instrument "focuses" the neutrons

into a coherent picture, emerging just like an image in a Polaroid snapshot.

"You need a complicated instrument that allows you to follow the neutron and give you information about its velocity and the direction it's coming from," says Ryan. "Our instrument will be very sensitive, and when it detects these neutrons it will be able to construct images of the emission pattern and report the neutron spectrum, which in turn will allow us to nail down what type of nuclear material we're dealing with."

He adds that, unlike gamma rays, which if detected would alert authorities to something like radioactive medical waste that could be used to construct a **dirty bomb**, "If you were to get a neutron signal at some port, for example, you'd bring everything to a halt because what you're potentially dealing with there is someone trying to smuggle in material for a nuclear device, or a nuke itself."

## A Nightmare That Could Be Worse than 9/11

#### By Michaela Bendikova

Source: http://blog.heritage.org/2011/09/12/a-nightmare-that-could-be-worse-than-911/

After 9/11, an event that Americans and their allies will never forget, the United States focused on a war on terrorism. There is, however, a threat that has been largely ignored—the threat of an electromagnetic pulse (EMP), noted by *Investor's Business Daily*. In 2004 and 2008, the Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack (also known as the EMP Commission) released its reports on how to protect the United States from an EMP. Despite its recommendations, little progress has been made in protecting the country from an EMP attack and its catastrophic consequences.

An EMP is a high-intensity burst of electromagnetic energy caused by the rapid acceleration of charged particles. Nuclear and non-nuclear weapons or geomagnetic storms can cause an EMP. An EMP would disrupt electronics, transmission distribution centers, fuses, and power lines, sending the United States back to the 19th century. While an EMP does not kill people, millions would die as the distribution of food, transportation, and delivery of a basic health care would collapse.

Manmade causes of an EMP include a nuclear weapon detonated at a high altitude.

Intercontinental-range ballistic missiles are one of the possible means of delivery for such a scenario. Short-range, less technologically challenging, nuclear-tipped ballistic missiles launched off U.S. shores would deliver a similarly devastating attack. North Korea currently possesses nuclear weapons, and its missiles can reach Hawaii and Alaska. Iran continues to improve the range of its ballistic missiles and work towards obtaining nuclear weapons capability. A robust missile defense is essential for protection from this type of attack. Such a missile defense system, composed of Aegis ballistic missile defense capable ships: Aegis Ashore, a land-based missile defense component; and Unmanned Aerial Vehicle capabilities, can deprive the opponent of the opportunity to deliver a nuclear warhead on a ballistic missile and cause an EMP in the first place.

But an EMP could be inflicted without an organized group behind it. With the right equipment, a lone terrorist could cause a blackout of a city—with commercially available equipment. Time is running short. For about \$200 million, the United States can harden the major transformers associated with large metropolitan areas. This would allow, more

people to survive the consequences of an EMP. If the electrical power grid were destroyed, it would take years to replace critical transformers, since only a few countries build

them; it takes more than a year to make one transformer. The United States can and has the obligation to prevent another "failure of imagination." The time to act is now.



23,300 nuclear weapons are stored at an estimated 111 locations in 14 countries



Source: http://www.fas.org/programs/ssp/nukes/images/globaled.jpg



# Explosive News

#### Bomb-proof bag for planes' luggage compartment developed

Source:http://www.homelandsecuritynewswire.com/bomb-proof-bag-planes-luggage-compartment-developed

The blast-absorbing bag, named the Fly-Bag, features multiple layers of novel fabrics, composites, and coatings and is designed to be filled with passenger luggage and then



placed in the hold of a plane; if one of the pieces of luggage inside the Fly-Bag

had a bomb in it and the bomb exploded during the flight, the resulting blast would be absorbed by the bag owing to its complex fabric structure. preventing damage to the plane; fundamental to the design of the bag is the internal elastomeric coating and impregnation of fabric with Shear Thickening Fluids (STF); STFs work by increasing in viscosity in response to impact.

Richard Palmer and his d3O non-newtonian fluid // Source: blogspot.com

A bag which can protect planes from bombs in passenger luggage has been developed by an international team of scientists, among them academics from the University of Sheffield working within University spinout company



Blastech Ltd. The bag, named the Fly-Bag, features multiple layers of novel fabrics, composites, and coatings and is designed to be filled with passenger luggage and then placed in the hold of a plane. If there were a bomb in the luggage in the bag which exploded during the flight, the resulting blast would be absorbed by the bag due to its complex fabric structure, preventing damage to the plane.

A university of Sheffield release reports that fundamental to the design of the bag is the internal elastomeric coating and impregnation of fabric with Shear Thickening Fluids (STF).

Elastomers are very low stiffness, high failure



strain materials, often used as adhesives, sealants, or in structures where high strains are expected. An elastomer was developed to provide a gas seal in the bag at very high strain rates and very high deformations, while resisting flame and heat.

STFs work by increasing in viscosity in response to impact. A simple STF can be made from mixing corn flour with water. Providing quantities are correct, it would be possible to roll this simple STF into a ball that will bounce on hard surfaces but return to a fluid once it is left alone.

The release notes that under normal circumstances, the particles in STFs repel each other slightly, but following sudden impact, the extra energy in the system proves stronger than the repulsive forces, causing the particles

to clump together in structures called hydroclusters, which bump into each other, consequently thickening the fluid.

This unusual behavior of STFs has already generated significant commercial interest and STFs are being considered to improve body armor designed to protect the wearer from weapons such as knives and bullets.

In the case of the Fly-Bag, the STF is coated onto the yarn of the fabric and as the fabric comes under strain, shearing forces between the yarns cause the STF to thicken, temporarily increasing the stiffness of the fabric, reducing the total deformation.

Hardened luggage containers (HULD) have been developed to deal with bombs hidden in passenger luggage, but these containers are heavier and more costly than conventional equivalents and are only suitable for wide body aircraft.

It is expected that the Fly-Bag will be on the market in one to two years, although cost would depend on a range of variables, such as the structure of the plane. Team member Dr. Jim Warren from the University of Sheffield's Department of Civil and Structural Engineering, said: "The use of explosives on aircrafts has had a renaissance in recent years, with recent attempted attacks coming not just from passengers, but also as loaded freight. Since weight and operational flexibility is key for aircraft operators, this low weight, removable solution would seem to be a paradigm shift in the hardening of aircraft structures."

#### Militants may try bomb implants to attack

Source: http://www.reuters.com/article/2011/07/06/us-usa-security-implants-idUSTRE7652QX20110706

Militants are showing renewed interest in using a bomb surgically implanted inside a passenger's body to blow up a commercial flight, though there is no indication an attack is



#### UNDERWEAR WITH EXPLOSIVE PACKET

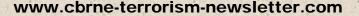
imminent, a U.S. security official said on Wednesday.

U.S. authorities have warned their counterparts abroad as well as air carriers about new intelligence on this method and were taking steps to boost security. "The Department of Homeland Security has identified a potential threat from terrorists who may be considering surgically implanting explosives or explosive components in humans to conduct terrorist

attacks," the advisory to foreign counterparts said, according to the U.S. security official.

Such a threat is likely to come from overseas rather than domestically, but precautions were being taken on both sides, the official said on condition of anonymity. The new intelligence did not indicate an attack was imminent, the official said. U.S. authorities have been on high alert after American forces killed al Qaeda leader Osama bin Laden in May, ramping up security at airports, government

buildings and other facilities in case of a retaliatory strike. The official declined to say whether the new intelligence came from documents collected at the compound in Pakistan where bin Laden was found and killed.



The possibility of a suicide bomber attacking with explosives implanted in the person's body has long been a concern for authorities -- and a difficult threat to detect. Attacks in the past have involved explosives packed in luggage. shoes, clothing or other items. A U.S. national security official told Reuters the U.S. had recently received credible intelligence that al Qaeda's Yemeni affiliate, known as Al Qaeda in the Arabian Peninsula, is working on methods to plant bombs inside its operatives. The official indicated the body-bomb research was part of AQAP's broader effort to develop weapons not detectable by standard security methods. In the best-known AQAP plot, a Nigerian man was arrested in December 2009

and has been accused of trying to ignite a

bomb hidden in his underwear aboard a flight

from Amsterdam to Detroit. In October, toner cartridges packed with explosives were sent aboard U.S.-bound cargo planes but were intercepted and defused overseas before they exploded.

In the wake of such attacks, U.S. aviation security authorities have steadily ramped up passenger and cargo screening, requiring travelers to have their shoes X-rayed, go through full-body scanners and restricting liquids allowed in the passenger cabin of planes.

Transportation Security Administration spokesman Nicholas Kimball said passengers flying into the United States may notice enhanced security measures, including talks with them as well as pat-downs and "enhanced tools and technologies."

#### Similar threat in 2010:

#### Terrorists planning breast implant bombs

Source: http://www1.whdh.com/news/articles/local/boston/BO135406/#ixzz1RQoY001B

Reports say terrorists could begin hiding explosives in breast implants. British spy satellites have apparently intercepted terrorist communications from Pakistan and Yemen, talking about women suicide bombers getting explosives put inside breast implants. Former Houston FBI Director Don Clark said he believes U.S. Homeland Security is taking this threat very seriously. "Sometimes as ridiculous as it may sound, it can probably be pulled off...Terrorists and terrorist attack are a reality," Clark said. The British Intel service reports several plastic surgeons who were trained in many of London's hospitals have returned to their countries to perform the surgeries. "I'm sure we are gathering all the information, intelligence that the government can," he said. "They are also securing all the ports, airports and main attractions as much as possible. The government takes these types of threats seriously and not relaxed."

Houston plastic surgeon Dr. Franklin Rose said that the industry's technology makes the

bombs possible and easy. "To have a plastic surgeon put in liquid explosion in an implant and teaching somebody how to detect it, it's unfathomable," Rose said.

Travelers at Boston Logan International Airport reacted with outrage and anxiety. "I guess it's surprising, but I guess it's not surprising that they're gonna go to any lengths," one traveler said. Another person at Logan said increased security might measures need to be taken. "I think that we need to invest.



in full-body scan equipment at the airports. I think that would be the only helpful and the right thing to do," one man said.

No full body scanners are at Logan, but they could be in place in a few months. The Transportation Security Administration says its scanners do detect explosive materials and residue. However, it's unknown how well fullbody scanners would detect explosives inside implants. TSA officials at Logan said they have been informed of the possible threat and are on the lookout.

#### TSA could begin searching for explosives hidden inside you

Source:http://www.homelandsecuritynewswire.com/tsa-could-begin-searching-explosives-hidden-inside-you

Government intelligence officials are now warning airlines that terrorists could be using surgically implanted explosives to bypass security measures.

There is no information regarding a specific plot or threat, but airlines could begin to implement additional screening procedures as the current body scanners cannot effectively detect bombs hidden inside an individual.

According to the Los Angeles Times, U.S. officials have received new information that suggest terrorists may be seriously considering surgically implanting explosive devices to circumvent existing screening procedures.

(TSA), said airline passengers flying into the United States will likely face additional screening measures.

"These measures are designed to be unpredictable, so passengers should not expect to see the same activity at every international airport," Kimball said. "Measures may include interaction with passengers, in addition to the use of other screening methods such as pat-downs and the use of enhanced tools and technologies."

Current body scanners cannot detect explosive materials hidden in body cavities or below the skin, so airport screeners will rely on explosive trace detection swabs.

In 2009, in a failed suicide bomb attack aimed at assassinating Prince Mohammed Bin Navef, the of Saudi Arabia's head counterterrorism operations, an al Qaeda operative hid a pound of high explosives and a detonator in his rectum. Using this technique, the suicide bomber was able to avoid two sets of airport security screening systems, palace security, and more than thirty hours of close observation by the prince's secret service agents. The bomber attended a

meeting with the prince where he detonated the bomb killing himself and lightly injuring the prince.

In response, Nicholas Kimball, a spokesman for the Transportation Security Administration

Swabbing hands for explosive residue //

Source: consumer traveler.com

## Anti-Terror Sensor That Scans Crowds for Bombers Tested in U.K.

Source: http://www.foxnews.com/scitech/2011/07/07/anti-terror-sensor-that-scans-crowds-for-bombers-tested-in-uk/



A sensor that can scan huge crowds and pick out a lone suicide bomber by homing in on hidden explosives has undergone official tests, The Sun reported Thursday.

The revolutionary gadget -- similar to airport scanners but top secret -- is believed to silently analyze materials using the unique "terahertz" waves emitted by different substances.

British government scientists began testing it a year ago on mock crowds where one person in every 75 carried a "Person-Borne Improvised Explosive Device."

Heavily-censored reports obtained by the newspaper in a freedom of information request reveal other trials saw the guinea pigs armed with "handguns and knives."

Real terrorists would have no idea they had been scanned from a distance -- and could be intercepted before causing mayhem.

The futuristic device -- officially known as a "stand-off imaging system" -- could be used to protect Al Qaeda targets such as rail stations, shopping malls and sporting events.

The device is thought to be sophisticated enough to differentiate between plastic explosive and plasticine.

British government sources have not ruled out the system being in place at the London Olympics.

The Home Office said, "Protecting the public is our number one priority. We regularly test new technologies to help us face the ongoing terrorist threat."

#### Stand-Off Detection of Suicide Bombers and Mobile Subjects

(NATO Security Through Science Series / NATO Security Through) Source: http://www.powells.com/biblio?isbn=9781402051586

The book contains lectures of an international NATO-Russian Advanced Research Workshop



#### Stand-Off Detection of Suicide Bombers and Mobile Subjects



TO The pathware The NATO Programme An approximate for Security through Science

② Springer

121 180 8

about the Stand-off-Detection of concealed explosives or explosive charges carried by Suicide-Bombers or in mobile objects (vehicles). The explosives or explosive charges should be detected by harmless methods from a distance and unnoticed by persons under inspection. The ARW was one of a series of workshops before, dealing with the detection of explosives used by terrorists and was initiated by the "Explosive Detection Working Group" of NATO to create projects of applied research. The aim of the workshop was to present suitable projects, to exchange knowledge and to discuss the feasibility and realization of methods.

Projects aim at improvements in sensing techniques that will allow the shortest developing time and are suitable for commercial production. Potential short time availability was a prioritizing isssue.

#### **Table of Contents**

Preface.- Acknowledgement.- Problem of Explosive Detection on Human Subjects.- MS-SRIP - Microwave System for Secret Standoff Inspection of People.- Secret Microwave "Door" for Inspection of People and Luggage.-MIP-based Low-cost Sensor for Short-range Detection of Explosives.- Scanned Multiple (Electro-) Chemical Sensors Located at Critical Infrastructures.- Real-Time Detection of IED Explosives with Laser Ionization Mass Spectrometry.- High Speed Mid Infrared Detection of Explosives Using Laser Spectroscopy.-Detection Remote of Explosives by Enhanced Pulsed Laser Photodissociation 1 Laser Ind

Fluorescence Method.- Gas Analytical System of Explosives Detection for the Manual Check of Objects and Use in Walk-through Portals.-Threat Detection DC to Daylight.- Stand-off Detection of Concealed Improvised Explosive Devices (IEDS).- Stand-off Detection of Surface Contaminations with Explosives Residues Using Laser-Spectroscopic Methods.- Distributed Trace Level Explosives Sensor Network.- Time-resolved Excitation-Emission Matrices Spectroscopic Approach to Explosives Detection.- MID-Infrared Lidar for Remote Detection of Explosives.- Stand-off Detection of Explosives of Suicide Bombers by Means of Open-Path FTIR Spectroscopy.- 14N NQR Detection of Explosives.- Stand-off Explosives Detection Using Terahertz Technology.

#### Terrorists in Drag: Bombs Beneath the Burqa

#### **By Phyllis Chesler**

Source: http://frontpagemag.com/2011/07/06/terrorists-in-drag-bombs-beneath-the-burga/

These photographs conclusively validate the concern that Dr. Daniel Pipes has had about the security risk that burqas represent. For the last six years, Dr. Pipes has been detailing the number of common criminals and Islamist terrorists who have robbed jewelry stories and peeped into women's bathrooms while wearing

burqas, or who have blown themselves and others up from under the protective cover of a mere woman's shroud.

These photographs conclusively validate the concern that Dr. Daniel Pipes has had about the security risk that burgas represent. For the last six years, Dr. Pipes has been detailing the



There they all stand, guilty as sin, Afghan Taliban terrorists disguised in women's burgas—but exposed when they were captured by the Afghan Border Police. Their photo (or rather photos) were taken by an Afghan photographer somewhere near Jalalabad and have just been seen worldwide.



One of these charmers was wearing an explosive vest; six had AK-47s. Clearly they were up to no good. One wonders how long they will remain in jail and what they will do when they emerge.

number of common criminals and Islamist terrorists who have robbed jewelry stories and peeped into women's bathrooms while wearing burqas, or who have blown themselves and others up from under the protective cover of a mere woman's shroud.

In December, 2009, a suicide bomber dressed in a full veil and abaya gained access to a ceremony attended by Somali government officials in Mogadishu and killed 19 people, including three cabinet ministers. In February, 2010, a female suicide bomber killed 54 Shia pilgrims in Baghdad. She was dressed in an abaya, which police said allowed her to hide an explosive device. In December, 2010 in Pakistan, a woman wearing a burqa threw a grenade and detonated an explosive vest at a U.N. security checkpoint, killing 41 people.

This is not just happening in Muslim-majority countries or in war zones.

In August, 2010, a man wearing a burga



robbed a bank in Silver Spring, Maryland. In January, 2011, a man wearing niqab (a face veil) attempted to rob a bank in Philadelphia. Three years earlier, also in Philadelphia, three men dressed as Muslim women stuck up a Bank of America branch. One of the men shot and killed a police officer during their getaway.

Why are burgas allowed in public? Or rather, why don't we view them as potentially suspicious as opposed to a religious custom which we infidels are obligated to honor and revere?

For reasons of safety, the West, and for that matter the entire Muslim world, should immediately ban the burqa as a security risk.

However, I have also gone on record calling for a ban on the burqa, at least in the West, on the grounds that it violates a woman's human rights.

A burqa wearer may feel that she cannot breathe, that she might slowly be suffocating.

She may feel buried alive and may become anxious or claustrophobic. She is trapped in a sensory deprivation isolation chamber. It is a form of permanent torture. Just imagine the consequences of getting used to this as a way of life. But perhaps one never gets used to it. They merely continue to suffer. For example, an unnamed Saudi princess described her experience of the Saudi abaya (to Jean Sasson) as follows:

When we walked out of the cool souq area into the blazing hot sun, I gasped for breath and sucked furiously through the sheer black fabric. The air tasted stale and dry as it filtered through the thin gauzy cloth. I had purchased the sheerest veil available, yet I felt I was seeing life through a thick screen. How could women see through veils made of a thicker fabric? The sky was no longer blue, the glow of the sun had dimmed; my heart plunged to my stomach when I realized that from that moment, outside my own home I would not experience life as it really is in all its color. The world suddenly seemed a dull place. And dangerous, too! I groped and stumbled along the pitted, cracked sidewalk, fearful of breaking an ankle or leg.

Qanta Ahmed, a Pakistani-British-American religious Muslim physician worked in Saudi Arabia for a few years. Board certified in four areas, immediately upon arrival, she nevertheless became invisible, demeaned, shrouded, akin to chattel property in the airport where no man and no porter helped her (or other women) with their luggage. She writes:

The veiling was anathema to me. Even with a deep understanding of Islam, I could not imagine mummification what is an enlightened, merciful God would ever have wished for half of all His creation. These shrouded, gagged silences rise into a shrieking register of muted laments for stillborn freedoms. Such enforced incarceration of womanhood is a form of female infanticide.

I must repeat, as I always do, that I am not opposed to the hijab (the headscarf). I am only addressing the face-obscuring garments that are cumbersome, dangerous, and exclude a woman from normal social interaction.

And, as I have said before, wherever burqas, chadris or the extreme Saudi or Iranian versions of female head, face, and body covering exist, you will probably find fundamentalist Islam and potentially infidel-hating, Jew-hating terrorists. Burqas and jihad go hand-in-hand.

There is another reason to ban the burqa in the West. Muslim girls and women are being beaten and even honor killed for refusing to wear this costume of utter subordination. Many (certainly not all) Muslim girls must toe the line in terms of how they dress or they will be threatened, beaten, acid-attacked, or even honor killed. If their families or roving self-appointed Vice and Virtue squads decide that they are looking too "Western," or dressing in too modern a fashion, they will be punished.

Young, including educated, Muslim women in the West are increasingly wearing oppressive Muslim garb in a show of resistance to infidel culture. Just yesterday in New York City, I saw, in ninety-degree heat, a casually dressed man followed by a woman in a severe and heavy hijab.

I have found that Muslim girls and women are at risk in the West when they attempt to assimilate. When they begin to want "Western" things, beginning with casual clothing, makeup, an education, non-Muslim friends, perhaps a non-Muslim boyfriend, perhaps a divorce from an illiterate and violent first cousin—that is when their fundamentalist families view them as "prostitutes" and kill them.

We in the West must strategize ways to protect those Muslims and ex-Muslims who choose to assimilate and to prosecute those who are violent towards them.

#### Roving robot can rescue people, detonate bombs

Source: http://www.northeastern.edu/news/stories/2011/06/wifi\_robot.html

Northeastern University student-researchers have created a roving robot named WiLU that may be able to locate and rescue victims of

natural disasters or participate in military missions that are too dangerous for soldiers. The innovative technology was developed for a senior capstone project under the direction of electrical and computer enaineerina professor Charles DiMarzio and associate professor in the College of Computer and Information Science. Guevara Noubir. The team

members included electrical and computer engineering students Tom Bottiglieri, Spiros Mantzavinos, Travis Taylor, Ryan Whelan, and Eric Williams.

WiLU — which looks like a Tonka truck — could help save the lives of victims of catastrophic disasters, such as the massive 9.0 earthquake that rocked Japan in March, said Whelan.

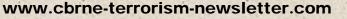
As he put it, "You could send this robot into a search and rescue scenario where you don't want humans to go."

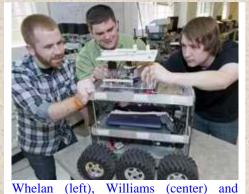
A Northeastern University release reports that Noubir sponsored the students and funded the project with a portion of the National Science Foundation (NSF) Major Research Instrumentation grant awarded

to him and an interdisciplinary team of professors from Northeastern to develop wireless sensor networks that support key

applications such as search and rescue by swarms of robots.

He praised the student's innovative robot. "It's a great example of an effective research platform that integrates multi-disciplinary expertise spanning mechanical engineering, RF communications, embedded software development, and algorithms designs."





Bottiglieri (right) created a robot that can

find disaster victims through their mobile

phones Photo by Mary Knox Merrill

Students created a complex algorithm that would enable the robot to locate people — or even bombs that are detonated through mobile phones.

Here is how it works: a smart antenna mounted atop WiLU measures the signal strength of a mobile phone that is connected to a wireless network. Then, the robot autonomously determines the location of the object by adaptively forming beams to pinpoint the direction and location of the wireless signal source.

Students, who say humans could also control the robot from remote locations, hope to create a subscription service whereby mobile phone



users could automatically join the WiFi network.

"Incorporating so many different creative and technical skills on a single project is the goal of our Capstone Design course," DiMarzio said.

#### Colombia rebels kill 2 police, set off "horse bomb"

Source:http://www.publicbroadcasting.net/kial/news.newsmain/article/0/0/1825936/World/Colombia.rebe ls.kill.2.police..set.off.%27horse.bomb%27

Colombian rebels shot dead two policemen in one attack and wounded two soldiers with a horse packed with explosives in another Sunday as Bogota vowed to beef up security in a violence-hit south- western

state.

Colombia has been battling leftist rebels for nearly five decades and while security has improved drastically

over the last few years, illegal armed groups continue to stage bombings, hit-and-run attacks and other bloodshed.

Police said two officers were shot dead in the southwest state of Cauca Sunday -- the same province where a day before rebels detonated a car bomb, a bus bomb and another explosive device.

Colombian President Juan Manuel Santos said that he was sending reinforcements of police, army and special forces to Cauca, an area plagued by drug and guerrilla violence. Santos also said that Colombia would create

another mountain battalion for the area. "We've taken the measure that from now on,

security personnel will destroy any house that

is used by terrorists to attack government forces or civilians. No more utilizing houses to shoot at government forces or at civilians," he said.

Local media also reported Sunday that suspected FARC rebels had detonated a horse packed with explosives, injuring two soldiers, in the southern province of Caqueta.

> The security situation has worsened this year in the departments of Cauca, Caqueta, Norte de Santander. Arauca and Antioquia, according to the Colombian thinktank Corporacion Nuevo Arco Iris. The attacks came a week after the leader of the

FARC, Colombia's largest guerrilla group, narrowly eluded capture by security forces. The FARC has stepped up violence recently in the world's No. 1 cocaine producer. Santos, who took office last August, has vowed to keep up former President Alvaro

Uribe's tough stance against left-wing rebels, paramilitary gangs and cocaine traffickers.



#### In June 2009:

#### Israelis 'thwarted Gaza horse bomb attack'

Source: http://news.bbc.co.uk/2/hi/8089535.stm



Four Palestinian militants have been killed on Gaza's border as Israeli forces fired at what they said were men and horses carrying explosives. The Israeli military said its forces returned fire at a group including a few men wearing explosive vests and five horses loaded with explosives. Israel said the Palestinians opened fire and tried to plant bombs near a crossing on the Gaza-Israel border. Palestinian officials said about 10 gunmen were involved in the incident. The Palestinian health ministry, which is run by the Hamas movement that controls Gaza, confirmed that four fighters were killed in the shooting. Israeli forces fired on the militants with machine guns and tanks backed up with combat helicopters, the military

said. There were no Israeli casualties in the incident, which took place north of Nahal Oz, the main terminal for transferring fuel into Gaza. Nahal Oz and the nearby Karni crossing, used for transferring grain and animal feed, were closed in the wake of the incident. It is one of the worst clashes since Israel's three-week operation in Gaza in December and January. Both Israel and the Hamas movement, which controls the Gaza Strip, declared unilateral ceasefires in the wake of the fighting. Senior Hamas leader, Ismail Haniya, said the incident was confirmation that Israel's "aggressive intentions" continued, and accused Israel of not respecting the cease fire. Although Gaza has been relatively quiet since Israel's three-week offensive against Hamas ended on 18 January, the border is a flashpoint for sporadic violence.

#### Beware of Dr. Jihad

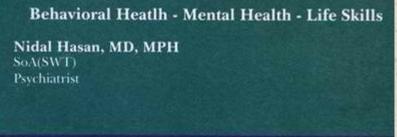
#### By Michelle Malkin

Source: http://michellemalkin.com/2011/07/08/beware-of-dr-jihad/

Splendid news: Our homeland security officials have sent fresh warnings to foreign governments that "human bombs" may try to

board planes with surgically implanted explosives. The ticking terrorists are reportedly getting help from murderminded Arab Muslim physicians trained in the West, Infidels beware: Dr. Jihad's version of the health care oath omits the "no" in "Do no harm."

detection equipment cannot penetrate. At least one Saudi operative has been nabbed with explosives in his bum, and British intel picked



Contact Number: 301-547-1599 E-mail: NidalHasan@aol.com

up on Arab website chatter last year about possible breast-bomb inserts. Officials are now said to be on the lookout for physicians' notes requesting that passengers be allowed to carry

### Doctor of medicine, soldier of Allah

The death docs may be using their expertise to play "Hide the IED" in body cavities that bomb-

syringes — which could carry detonation chemicals.

Lest you shrug off reports of these literal booby-traps as empty fear-mongering, listen up:

"It's more than aspirational," one U.S. official told The Wall Street Journal. "They're trying to make this happen."

There should be no shock at the role of purported healers in these and other hellish plots to destroy masses of innocent lives in the name of Allah. Anyone who still clings to the bleeding-heart belief that poverty breeds terrorism — including, alas, our commander in chief — is willfully blind to past history and present reality.

Medical charities have long served as front groups for jihad. Palestinian jihadists used ambulances owned and operated by the United Nations Relief and Works Agency for Palestine Refugees (UNRWA) — subsidized with billions in American tax dollars — to ferry explosives and gunmen from attacks. Hezbollah terrorists used ambulances as props in Lebanon to stage anti-Israel propaganda and elicit sympathy from Western media.

And radical Islam's bloody perversion of the medical profession traces back to the Egyptbased Muslim Brotherhood, the global terror operation that wooed wealthy young docs and other intellectual elites with cushy union benefits.

- Ayman al-Zawahiri, a surgeon from a family of doctors, was raised in the Muslim Brotherhood; helmed the murderous Islamic Jihad; and masterminded myriad al-Qaida plots before succeeding Osama bin Laden this summer.
- Former Hamas leader Abdel Rantissi, bent on wiping out the children of Israel, was a pediatrician.
- Convicted al-Qaida scientist Aafia Siddiqui studied microbiology at MIT and did graduate work in neurology at Brandeis.
- Rafiq Abdus Sabir was a Columbia University grad who served as an emergency room physician in Boca Raton, Fla., before his terrorism conviction in 2007 for agreeing to provide medical aid and treatment to

wounded al-Qaida fighters so they could return to Iraq to kill American soldiers.

- Rafil Dhafir, an Iraqi-born oncologist, practiced in New York before being convicted in 2004 on 59 criminal counts related to violating Iraqi sanctions and committing large-scale medical charity fraud.
- A den of well-heeled jihadi doctors from around the world was implicated in the 2007 London/Glasgow bombings. At least one of the convicted terror MDs worked for Britain's National Health Service.
- Mahmoud al-Zahar. another Hamas bloodthirsty biggie and doctor. medical described his specialty to a New York Times reporter in 2006 this way: "Thyroids: I'm very good at cutting throats,' Dr. Zahar said, drawing his forefinger across his neck as a rare smile spread across his face."

Evil zealots who'll use children as human shields won't hesitate to employ revered caregivers as human explosive-enablers. They've warned us for years. Days after the 2007 terror doc conspiracy unraveled in London, a Church of England clergyman, Andrew White, recounted to National Public Radio a warning he received from a Sunni fanatic in Amman, Jordan:

"I listened to him for 40 minutes, and he went on about how they were going to destroy Britons and Americans and how they were going to be doing more in the U.K. and U.S., and he finished by saying 'those who cure you will kill you.""

Closer to home, Army psychiatrist Nidal Hasan starkly diagnosed the ideological fanaticism of every soldier of Allah in a Koranic-inspired PowerPoint presentation that concluded: "We love death more than (sic) you love life!"

Military officials plagued by political correctness ignored Hasan. Thirteen Fort Hood soldiers and civilian personnel, and one unborn child, paid with their lives.

How many more Dr. Jihads are operating in the open, exploiting our borders and tolerance, wielding medical licenses to kill?







### The New MagShoe<sup>™</sup> 3G Series

MagShoe "3G series - The latest metal detectors from the MagShoe" family of Shoes-On Metal Detectors from IDO Security.

MagShoe" metal detectors are employed all over the world wherever a strict control over entry of weapons and other metal objects is required.

Our detectors employ state-of-the-art sensors and algorithms to detect weapons and other controlled metal articles going in or out of secure environments such as government

facilities, stadiums, airports, prisons, coin-production mints etc. By providing accurate measurements MagShoe" solutions keep the false alarm rate low, while detecting guns, parts of guns, knives and metal objects concealed in shoes and the lower



part of the body, and at the same time ignoring metal normally found in footwear, like heels, zippers, ornaments etc. This keeps the number of manual inspections required at minimum focusing on the real threat.

> The latest models of the MagShoe"3G series - features improved sensors and detection algorithms, higher detection range, on-board LED displays for scan results and user information together with the ability to connect to a MagShoe" centralized Network Management and Control System - the NMC-3.

Usage of the NMC-3 software system allows realtime monitoring and control of all the deployed MagShoe<sup>\*\*</sup> units from a central remote location.

### MagShoe<sup>™</sup>3G/2

The 3G/2 model is actually the predecessor of the fieldproven and widely used MagShoe<sup>™</sup> model 2.72, already installed in numerous locations worldwide and used in various applications, both in the Home Land Security and Loss Prevention markets.

MagShoe<sup>™</sup> systems are installed in Parliaments and other Governmental buildings, Prisons, Cruise Ships, Sport Stadiums, Residential compounds, Coin production mints, Jewellery factories and more

The 3G/2 model features improved detection and sensitivity settings to comply with the unique detection requirements of the HLS market (i.e. detection of a blasting-cup or other detonation apparatus, small ammunition, electrical wires etc.) and the Loss Prevention market (i.e. theft-prevention of small metallic items like coins, electronically parts and other valuable metallic items). An optional fixed safety Rails system ensures a safe and simple use.

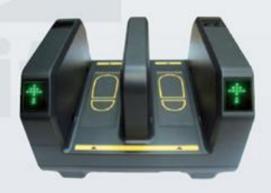


#### The MagShoe<sup>™</sup>3G Series

- Fully automatic and fail-proof operation requiring minimal training and supervision
- Discrimination of the metal components found in shoes
- Significantly reduces the number of manually examined or X-Rayed footwear
- Scanning only takes a number of seconds increasing the passenger flow rate
- Two levels of password-protected user-permissions reduce the probability of human error or malicious disruption
- On-board statistic data collection and analysis with download options
- Ability to connect to the remote Network Management & Control system (NMC-3) via a local Ethernet Network
- Magnetic interference resistance for flexible placement among the existing equipment and infrastructure
- Certified as fully safe for wearers of pacemakers and pregnant women; uses non-ionizing and harmless low-frequency electromagnetic fields

#### MagShoe<sup>™</sup>3G/2 Features:

- Detection height of 20 cm (7.9") from sole
- Improved algorithm for sensitive detection of small items
- Rapid scan time about 2 seconds per check
- Low false alarm rate
- Preconfigured threshold levels according to needs and demand
- Manual threshold settings option to conform to local regulations and for training purposes
- Back-up Battery with audio/visual indication of emergency use, i.e. during main power failure or use in a temporary location
- No special training required, simple and easy to use
- Light weight and portable, easily moved and re-installed in a matter of minutes
- Small foot print, easily integrated into existing check point operations
- Low maintenance required





#### IDO Security Ltd.

20 Freiman Street, 4<sup>th</sup> ent. Rishon LeZion 75358, Israel Tel. 972-3-952 3599 Fax: 972-3-952 3604 inquiries@idosgroup.com www.magshoe.net IDO Security Inc. 17 State Street, 22<sup>nd</sup> Fl. New York, NY 10004. USA Tel. 646-214 1234 Fax. 646-285 0026 inquiries@idosecurityinc.com www.idosecurityinc.com

The company reserves the right to change subjects and contents without any notice.

#### New software to improve explosive detection

Source: http://www.homelandsecuritynewswire.com/new-software-improve-explosive-detection

New software developed by Peaklet Analysis with the aid of a Western Kentucky University



(WKU) math professor could help existing explosives detectors improve their detection abilities.

Using a mathematical algorithm developed by Bruce Kessler, a math professor at WKU, Peaklet Analysis hopes to improve its ability to detect explosives. Programmers and software developers at Hitcents.com are currently working on translating Kessler's algorithm into multiple programming languages to make software that can function in any computer environment.

Gordon Baylis, the vice president for research at Peaklet, said the algorithm "has the potential to be a very important breakthrough in security screening and explosives detection."

Kessler added, "My hope is that our product would come into play to help explosives detection in airports, in detection of drugs and contraband and even help protect our military from explosive devices."

Peaklet's software detects explosives by analyzing low-level radiation when an item is

scanned. Different elements give off different energy levels, so a graph of the spectrum rays of an individual item will indicate the presence of explosives if it contains peaks in certain locations.

Baylis applauded Kessler's involvement as well as WKU, which is helping to support the research through its Office of Research and its Research Foundation. "We all dream of creating the next big thing," Dr. Baylis said, "but I'm more concerned with getting ideas out there and solving problems. It would be nice to hit a home run with a product or an idea but I want our people out in the ballpark playing the game. Putting smart ideas to work is what WKU can do for the community and is what universities need to be doing for this country."

Peaklet plans on selling its software to detection companies to help them locate explosives, drugs, and other contraband items in luggage or cargo containers. In addition Peaklet's technology can be used by petroleum and coal companies to detect impurities in their product.

Baylis hopes that the technology will eventually be used to help DHS screen cargo ships in a more efficient manner.

The technology could even be used to help U.S. troops detect improvised explosive devices. "If we can get this developed into one of those machines they test in Afghanistan to help the troops, it would be huge," said Ed Mills, the chief financial officer of Hitcents.com. "To save one life would make a difference."

#### Animal kingdom's alternatives to full-body scanners

Source: http://www.homelandsecuritynewswire.com/animal-kingdoms-alternatives-full-body-scanners

A typical full-body scanner costs upward of \$150,000, and some argue that this to high a price for a piece of machinery which is not always accurate — and, what is more, the health effects of which are still being studied. Lawmakers on the Hill, for example, are currently debating whether explosive-sniffing dogs would do a better job than scanners at U.S. airports and other transportation hubs. The pro-dog camp argue that dogs have at least two distinct advantages over scanners:

first, they pose no radiation health risk to those

being scanned. Second, they are much cheaper (on average, the cost of a dog plus its training in bomb detection is about \$8,500).The pro-dog camp also argues that dogs are equal or better than scanners when it comes to detecting explosives.

Explosives-detection dogs were used successfully in Iraq by U.S. and coalition forces. Reporting on the success of dogs in sniffing IEDs in Iraq and Afghanistan, NPR reported that "Sniffer dogs are universally

recognized as the most effective means of detecting explosives."

Other countries have reached similar conclusions. The BBC reports that in Russia, the military is using dogs in the fight against Chechen terrorists. "Dogs can detect the kind of deadly material and explosives that a human being, a robot or a mine detector often struggle to find," a Russian military official told the BBC.

Care2 reports that the Russians have been using Sulimov dogs for sniffing bombs since 2002.

Bomb-sniffing dogs, however, may be no match for two other animals. Israeli researchers report that they found that mice are better than dogs in the bomb sniffing department, while a group of researchers in Hertfordshire reported that bees are superior to both dogs and mice in bomb sniffing

The Sulimov Dog (Russian: Собака Сулимова) is a Russian Jackal-Dog Hybrid originating from an



initial hybrid between a Lapponian Herder and a Turkmen golden jackal. The breed was introduced by Klim Sulimov, the chief breeder for Aeroflot airline security. The primary use of this breed has been to aid airport security as sniffer dogs. Quoting Sulimov, "My dogs combine the qualities of Arctic reindeer herding dogs, which can work in temperatures as low as -70C, and jackals which enjoy the heat up to +40C. They're perfect for our country."

During the breeding process male jackal

pups had to be fostered on a Lapponian Herder bitch in order to imprint the Jackals on dogs. Female Jackals accepted male Huskies more easily. The half-bred Jackal-Dogs were hard to train and were bred back to Huskies to produce quarter-bred hybrids (quadroons). These hybrids were small, agile, trainable and had excellent noses. They were then called Sulimov Dogs after their creator and may one day be registered as a working breed of dog. Twenty-five Sulimov dogs are used by Aeroflot at Sheremetyevo Airport in Moscow, for functions which include bomb-sniffing. Their breeding program dates back to 1975, but was not applied to bomb detection until 2002

#### Specialized Search Dog Add New Weapon to Fight

Source:http://www.military.com/news/article/marine-corps-news/specialized-search-dog-add-new-weapon-to-fight.html

Specialized search dogs have become a new weapon in the war on improvised explosive devices, roving more than 100 meters in front of their handlers to find the deadly devices



before they can be triggered.

SSD handlers with Military Police Support Company, III Marine Expeditionary Force Headquarters Group, III MEF worked with their

dogs to perfect their detection abilities at Oura Wan beach at Camp Schwab July 26, clearing designated lanes of travel of explosive devices planted for training purposes, much as they would do on a combat deployment.

"We set up scenarios such as a possible IED lane that friendly forces need passage through. The SSD handlers needed to clear the passage-way prior to the friendly forces going through," said Cpl. Anthony J. Manfredini, combat tracking dog handler, MP Support Co. "We set up what we call 'aids'. They are live explosives without the

initiating system and I can either bury them or hide them under something."

SSDs and their handlers also train to be able to identify other threats and bomb-making materials along with IEDS:

"Our dogs are trained to find different types ammunition,

explosives, IEDs, weapons caches, whether they be freshly dug or hidden for a long time. They are also trained to find homemade explosives," said Lar



explosives," said Lance Cpl. Joel Juarez, specialized search dog handler, MP Support Co.

It is the ability of the dogs to be released from the leashes to move freely in front of their handlers that makes them unique.

"Most dogs in the military working dog program work on-leash, and there is always a limitation there. Even though they have leashes military working dog program to extend those limitations," said Juarez. "That provides a safety barrier for the handler. When the handler is working on-leash, he is always in greater danger because he is right up there with the dog finding the IEDs."

SSDs are only one of the tools in the fight against IEDs, but their ability to remotely detect explosives saves lives.



U.S. Army Capt. Stephen Johnson shakes the paw of Sgt. 1st Class Freida, a specialized search dog, after a re-enlistment ceremony on Forward Operating Base Hammer, Iraq, June 9, 2008. Johnson is commander of the 1st Armored Division's Headquarters Company, 2nd Brigade Combat Team. U.S. Army photo by Pfc. Michael Schuch



"SSDs are not the answers to everything even though they are very effective. They are just one of the tools we have, and they, along with military working dogs in general, save lives," said Juarez.

To achieve this level of effectiveness, extreme care must be taken in the dogs' training, according to the handlers.

"We always take notes (on the dogs' training), The handlers post records everyday of exactly what kind of training they did and the proficiency and

deficiencies they have with their dog," said Manfredini. "The records let them know what their dogs need to work at and what they are good at."

The bond between an SSD handler and their dog is unlike that of other military working dogs and their handlers.

"One of the unique things about SSD handlers is that they usually stay with their dogs for the course of their careers," said Juarez. "Almost from day one, a handler is assigned two dogs, and throughout the training the handler take cares of his dogs and trains his dogs as best as possible."

> The IED-detection training here served to make the bond stronger, helping prepare the dogs and their handlers for potential service in Afghanistan.

The specialized search dogs did very well locating the bomb-making materials that were planted, according

to Manfredini. He went on to say that the dogs demonstrated a good ability to determine their own search patterns and focus on highprobability areas for improvised explosive devices.

#### Blast gauge gives medics, doctors critical information

Source:http://www.homelandsecuritynewswire.com/blast-gauge-gives-medics-doctors-critical-information

CPECIALIZE

SE

TEAM

Researchers are working to enhance the safety of soldiers in the field through the development of a device that monitors the physical impacts of exposure to an explosive blast; 188,270 service members have suffered a traumatic brain injury in the last decade; the extent of injury is often difficult to discern, making diagnosis and selection of appropriate medical treatment challenging.

Traumatic brain injury is emerging as a significant challenge for veterans. The Rochester Institute of



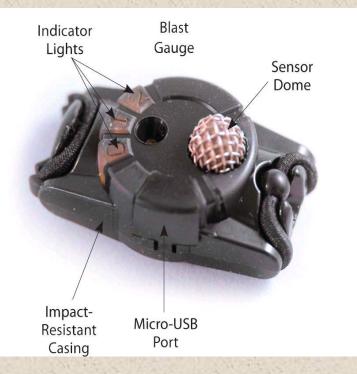
13.

254

Technology assembled a response team that engineered a dosimeter device to monitor blast exposure, which in the future could assist with field triage to identify injury long before physical and cognitive symptoms arise.

According to the Defense and Veterans Brain Injury Center established by Congress, 188,270 service members have suffered a traumatic brain injury in the last decade. The extent of injury is often difficult to discern, making diagnosis and selection of appropriate medical treatment challenging.

When a solider is exposed to a blast, shockwaves can cause a series of complex mechanical and physical reactions in the brain. These blast waves can induce tissue strains and stress, which may result in brain damage. Currently, no experimental data for humans exists to correlate pressure and stress on the brain with an actual explosive event that could assist with predicting brain injury. A



Rochester Institute of Technology release reports that through an effort funded by the Defense Advance Research Projects Agency (DARPA), a team of RIT engineers has responded to this urgent need by designing, engineering, and testing a blast measurement device that in the near future could be used to assist with field triage.

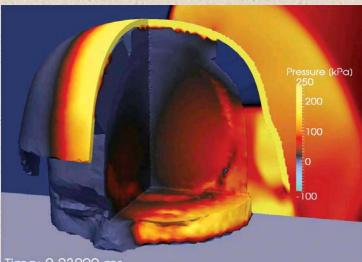
Blast Gauge: The data-logging device measures pressure, resulting head acceleration, and time to help correlate blast events with injuries. The compact device weighs less than one ounce, making it easy for soldiers to wear.

Dr. David Borkholder, associate professor of electrical and microelectronic engineering,

assembled a project team consisting of Dr. Lynn Fuller, professor of electrical and microelectronic engineering; two senior engineers, Gary Parrett and Werner Fassler; a recent RIT engineering graduate, Matthew Waldron; and staff assistant JoEllyn Tufano.

Blast Exposure: When a solider is exposed to a blast, a compression wave propagates through the cranial cavity, causing strain and stress to the brain.

Andrew Blair, an Army ROTC cadet; Stefan Wojick, a former U.S. Marine; Aalyia Shaukat; and Sigitas Rimkus, all undergraduate engineering students, are also involved in the project, participating in design work as well as system testing. "While the core technology



Time: 0.23200 ms

exists, the challenge is customizing the capabilities through creative engineering and integrating the components into a single system that provides a practical solution for the military," Borkholder told the Engineer.



The device was recently tested in the field using propane and oxygen explosions and weighted crashtest dummies to simulate a soldier.

The research has resulted in the formation of a company, BlackBox Biometric, which plans to commercialize the device this year.

#### DHS slow to crack down on ammonium nitrate sales

Source: http://www.homelandsecuritynewswire.com/dhs-slow-crack-down-ammonium-nitrate-sales

U.S. lawmakers are becoming frustrated with DHS for its slow implementation of regulations on ammonium nitrate fertilizer, a key ingredient in dangerous homemade explosives like the one used in the deadly 1995 Oklahoma City bombing; Congress initially passed legislation tightening control on the sale of the fertilizer in 2008, but DHS has yet to implement such regulations and three years later is only now publishing a set of "proposed" rule.



Pallets of Ukranian-made ammonium nitrate fertilizer // Source: allianz,com

Congress initially passed legislation tightening control on the sale of the fertilizer in 2008, but DHS has yet to implement such regulations and three years later is only now publishing a set of "proposed" rules. Representative Bennie Thompson (D – Mississippi), the ranking member on the House Homeland Security Committee who

authored the 2008 bill, said, "I am disappointed that more progress has not been made to put reasonable protections in place ... since we acted to fix this in 2007."

DHS officials say they are still in the process of creating rules as well as a reporting mechanism for more than 100,000 individuals working in agriculture, construction, and mining who use ammonium nitrate for legitimate purposes.

On Tuesday, DHS announced that it will publish a set of proposed rules that will be subject to a fourmonth review period during which industry representatives and the public can comment on any



concerns they have. As of now, no date has been set for when the final regulations will be issued.

Ammonium nitrate fertilizer was the main component in the 1995 bombing of the Alfred Murrah Federal Building in Oklahoma City.

"In today's ever-evolving threat environment, we must continually reinforce the security of substances, such as ammonium nitrate, which can be used for

legitimate purposes or exploited by terrorists," DHS Secretary Janet Napolitano said. Thompson noted that the release of the proposed rules is "a positive development, especially given the events in Norway." It is believed that in the recent bombing in Norway, Anders Behring Breivik used an ammonium nitrate based explosive.

Meanwhile Senator Bob Casey (D – Pennsylvania) echoed Thompson's frustrating saying that the "delay was unacceptable." Senator Casey is currently working to stop supplies of ammonium nitrate from flowing into Afghanistan from Pakistan, where it is used to construct improvised explosive devices that are endangering U.S. troops.

Efforts to restrict access to the dangerous fertilizer began after the Oklahoma City bombing where Timothy McVeigh used two tons of ammonium nitrate mixed with fuel to build a truck bomb that killed 168 people, in one of the deadliest attacks on U.S. soil in years. "I think most Americans would be outraged to know that we haven't made much progress on ammonium nitrate since Timothy McVeigh," Senator Casey said.

Under the proposed regulations, individuals who purchase large quantities of ammonium nitrate must first register in advance and can only purchase the substance after the government has approved their application. Officials will screen applicants to make sure they are not on any government watch lists.

Upon approval individuals will receive a federal use number and a photo ID which they must present at the time of purchase. In addition, dealers are prohibited from selling more than twenty-five pounds of the fertilizer to individual who are not registered. Dealers will also be required to keep records on all sales and to report any loss or theft within twenty-four hours.

#### New device identifies unknown liquids instantly

Source: http://www.homelandsecuritynewswire.com/new-device-identifies-unknown-liquids-instantly

Materials scientists and applied physicists have invented a new device that can instantly identify an unknown liquid; the 3Dnanostructured chip offers a litmus test for surface tension (and doubles as a carrier for secret messages); the researchers are



currently developing more precisely calibrated chips and conducting field tests with government partners for applications in quality assurance and contaminant identification Materials scientists and applied physicists collaborating at Harvard's School of Engineering and Applied Sciences (SEAS) have invented a new device that can instantly identify an unknown liguid.

The device, which fits in the palm of a hand and requires no power source, exploits the chemical and optical properties of precisely nanostructured materials to distinguish liquids by their surface tension.

The finding, published in the Journal of the American Chemical Society (JACS), offers a cheap, fast, and portable way to perform quality control tests and diagnose liquid contaminants in the field.

When dipped in varying concentrations of ethanol, the 3D-nanostructured device reveals different parts of a secret message. A customdesigned "W-Ink" can detect and identify many different types of liquids on a single chip.

"Digital encryption and sensors have become extremely sophisticated these days, but this is a tool that will work anywhere, without extra equipment, and with a very wide range of potential applications," says co-principal investigator Marko Lončar, Associate Professor of Electrical Engineering at SEAS.

A Harvard School of Engineering and Applied Sciences release reports that the new device, akin to the litmus paper used in chemistry labs around the world to detect the pH of a liquid, changes color when it encounters a liquid with a particular surface tension. A single chip can react differently to a wide range of substances; it is also sensitive enough to distinguish between two very closely related liquids. The "W-Ink" technology has only become possible due to a seamless fusion and interaction between chemistry, optics. condensed matter, and fluidics. In the prototype device discussed in JACS, the chip appears blank in the air. When dipped in varying concentrations of ethanol, however, it reveals new markings. Because all liquids exhibit a surface tension, this indicator has the potential to be used to differentiate between liquids of any type.

A hidden message can actually be "written" on a chip, revealing itself only when exposed to exactly the right substance. Dipped in another substance, the chip can display a different message altogether.

"This highly selective wetting would be very difficult to achieve on a two-dimensional surface," explains lead author Ian B. Burgess, a doctoral candidate in Lončar's lab and in the Aizenberg Biomineralization and Biomimetics Lab. "The optical and fluidic properties we exploit here are unique to the 3D nanostructure of the material."

The Watermark Ink, or W-Ink, concept relies on a precisely fabricated material called an inverse opal. The inverse opal is a layered glass structure with an internal network of ordered, interconnected air pores.

Co-authors Lidiya Mishchenko (a graduate student at SEAS) and Benjamin D. Hatton (a research appointee at SEAS and a technology development fellow at the Wyss Institute for Biologically Inspired Engineering at Harvard), recently perfected the production process of large-scale, highly ordered inverse opals. "Two factors determine whether the color changes upon the introduction of a liquid: the surface chemistry and the degree of order in the pore structure," says Mishchenko, who works in the Aizenberg lab. "The more ordered the structure, the more control you can have over whether or not the liquid enters certain pores by just changing their surface chemistry."

Burgess and his colleagues discovered that selectively treating parts of the inverse opal

with vaporized chemicals and oxygen plasma creates variations in the reactive properties of the pores and channels, letting certain liquids pass through while excluding others.

Allowing liquid into a pore changes the material's optical properties, so the natural color of the inverse opal shows up only in the dry regions.

Each chip is calibrated to recognize only certain liquids, but it can be used over and over (provided the liquid evaporates between tests).

With the hope of commercializing the W-Ink technology, the researchers are currently developing more precisely calibrated chips and conducting field tests with government partners for applications in quality assurance and contaminant identification. "If you want to detect forgeries," says Burgess, "you can tune your sensor to be acutely sensitive to one specific formulation, and then anything that's different stands out, regardless of the composition."

One immediate application would allow authorities to verify the fuel grade of gasoline right at the pump. Burgess also envisions creating a chip that tests bootleg liquor for toxic levels of methanol.

The release notes that the W-Ink technology would additionally be useful for identifying chemical spills very quickly. A W-lnk chip that was calibrated to recognize a range of toxic substances could be used to determine, on the whether spot. the spill required special treatment. "A device like this is not going to rival the selectivity of GC-MS [gas chromatography-mass spectrometry]," remarks co-principal investigator Joanna Aizenberg, the Amy Smith Berylson Professor of Materials Science at SEAS and a core faculty member of the Wyss Institute. "But the point is that if you want something in the field that requires no power, is easy to use, and gives you an instant result, then the W-Ink may be what you need."

## New material dramatically increases explosive force of weapons

Source:http://www.homelandsecuritynewswire.com/new-material-dramatically-increases-explosive-force-weapons

A revolutionary material that will replace steel in warhead casings will bring added lethality and increase the likelihood of a hit on an enemy target, the Office of Naval Research (ONR) said. By combining several metals with standard manufacturing techniques, **High-Density Reactive Material** (HDRM) has the potential dramatically to increase the explosive impact of most weapons with little or no compromise in strength or design.

An Office of Naval Research release reports



that unlike conventional munitions, the innovative materials approach integrates the casing with approved warhead explosives for increased lethality. In addition, the unique design for fragmenting warheads allows release of chemical energy after impact, increasing the probability of a catastrophic kill.

"Recent testing and demonstrations have consistently shown that the new casings can be integrated into naval missiles and are durable enough to withstand both high acceleration of missile launch and the forces

exposed to during the detonation event," said Dr. Clifford Bedford, ONR's energy conversion program officer. "The HDRM fragments can penetrate a target's skin, followed by a rapid and sustained combustion/explosion." The last test shots were fired at the Army's Blossom Point Field Test Facility in Maryland at the end of June.

> HDRM has the strength of common aluminium alloys yet the density of mild steel, making it an ideal replacement for steel components. This is important because, in order for existing weapon systems to maintain probability of a hit, they must have a density similar to that of steel.

> ONR is planning additional test shots in mid-August at Blossom Point. A large-



scale demonstration against multiple stationary targets is tentatively planned for September. The reactive materials team at Naval Surface Warfare Center, Indian Head Division, a partner with ONR, was recently honored with a Top Scientists and Engineers of the Year award for developing the material.

#### Sacramento Plastic Surgeon on the Possibility of Breast Implant Bombs

Source:http://www.sfgate.com/cgi-bin/article.cgi?f=/g/a/2011/08/11/prweb8709998.DTL#ixzz1Upebyp Ms

The Transportation Security Administration (TSA) was recently briefed by the federal government on new intelligence that shows terrorists could be using breast implants as surgically implanted bombs. At his Sacramento plastic surgery practice, Dr. Charles Perry discusses the likelihood of such an event, and how a terrorist could turn a procedure like breast augmentation into a potentially destructive threat.

The federal government recently briefed the Transportation Security Administration (TSA) on the potential threat of breast implant bombs [1]. While the information does not constitute an immediate threat, Sacramento plastic surgeon Dr. Charles Perry says the ability to turn breast implants into bombs is a real possibility. "Conceivably, a sterile device could be manufactured that would detonate inside a breast implant. All it would need is a propellant, an igniter, and a detonating receiver."

However, Dr. Perry says he finds it extremely difficult to believe any doctor would so blatantly ignore their Hippocratic oath to do no harm. He adds that even if a doctor were to cast aside his extensive training and commitment to helping people, the breast implants turned

explosive devices would have a different appearance and feel.

Despite the ability to conceal a device from the naked eye, Dr. Perry believes the advanced body imaging devices used by the TSA would be able to detect a breast implant bomb. However, he adds that while a device someone had swallowed or implanted elsewhere on the body would look suspicious, a device within a breast implant may not warrant a red flag.

Regardless of the potential that exists for using cosmetic enhancement procedures such as

#### Source:

[1] Straw, Joseph. "Beware new breast implant bomb, feds warn: Terrorists may try to sneak in explosives in implants" New York Daily News, retrieved on 08/10/2011 from articles.nydailynews.com/2011-07-06/news/20766606\_1\_bemb implant threat

06/news/29766606\_1\_bomb-implant-threat

Dr. Charles Perry earned his medical degree from the University of Washington. He then completed his general surgery residency at the University of Arizona, and his plastic surgery residency at the University of Massachusetts. Dr. Perry is certified by the American Board of Plastic Surgery, is a fellow of the American College of Surgeons, and is a member of the American Society of Plastic Surgeons. Dr. Perry specializes in an expansive spectrum of cosmetic enhancement procedures, ranging from laser skin resurfacing to liposuction, to the mommy makeover in Sacramento. breast augmentation to carry out a terrorist plot, Dr. Perry says he remains doubtful. While this may be a viable option conceptually, now that the TSA and federal government are aware of the threat, he says the ability to successfully implant and detonate a breast implant bomb seems unlikely.



#### Aussies to clone explosives sniffer dogs

Source: http://www.homelandsecuritynewswire.com/aussies-clone-explosives-sniffer-dogs

Two Aussie dog-breeding companies will collaborate with South Korean scientists on cloning explosives and drug sniffer dogs; the first batch of ten dogs will go into service in 2013; the Australians cloned dogs would be made from tissue samples taken from a German shepherd called Hassan von Gruntal, who



died in 2001; cloned sniffer dogs have already been used in South Korea and the United States.

## Trackr, cloned in 2008 // Source: thedogfiles.com

Australian law enforcement and military agencies have come up with a new way to make sure they have the best explosives sniffing dogs on service: clone currently serving sniffing dogs.



The Herald Sun reports that the first batch of ten cloned explosives and drugs sniffer dogs would be made available to Aussie government agencies and companies in the private sector by 2013. Two Australian companies — <u>Detector Dogs Australia</u> and <u>Von Forell International</u> – already breed and train



dogs for different tasks, including bomb detection at Port of Melbourne. The two companies will now collaborate with a South Korean company on the dog cloning project.

The Herald Sun notes that the cloned dogs would be made from tissue samples taken from a German shepherd called Hassan von Gruntal, who died in 2001. Hassan came "from an East German bloodline known for courage and commitment," the paper notes.

## VON FORELL Global leader in working canine genetics

Sniffer dogs cloning is not new. The world's first cloned sniffer dogs was employed in South Korea in July 2009. An American police dog called Trakr, who sniffed out survivors in the rubble of the World Trade Center after the 9/11 attacks, was privately cloned in 2008.



#### Marines deploy bomb-sniffing dog alternative

Source: http://www.homelandsecuritynewswire.com/marines-deploy-bomb-sniffing-dog-alternative

When bomb-sniffing dogs at Camp Lejeune, the Marine base in North Carolina, are unavailable, military police turn to Fido; the Fido XT Explosives Detector is a handheld device that is capable of sniffing out explosives or residuals in vehicles When bomb-sniffing dogs at Camp Lejeune, the Marine base in North Carolina, are unavailable, military police turn to Fido. The Fido XT Explosives Detector is a handheld device that is capable of sniffing out explosives or residuals in vehicles. The device, developed by ICx Technologies, can take air samples, analyze a swab from an individual's clothing, of

oils from a suspect's hands to determine if explosives are present. Eric Raduenz, the head of the regional chemical, biological, radiological, nuclear and high-yield explosive equipment and training team for Marine Corps Compared to other similar detection devices, Raduenz said Fido is superior as it is "many times more" sensitive. "It's very difficult to get a false positive on this," he added.

Fido can even out-perform dogs. In its



Installations East, said the devices would be used at base gates to intercept any potential threats.

For instance, if a low-riding van approaches a gate without proper identification, security personnel can use Fido to scan for any explosives and get an instant report, he said. "It could stop something small from turning into

something really big," said Lance Corporal Joseph Pall, a Military Policeman at Camp Lejeune who has trained with the device.

The technology used in Fido stems from a Defense Advanced Research Projects Agency (DARPA) project that sought to "mimic the capabilities of a dog," specifically when it came to sniffing out landmines, Raduenz said.

detection capabilities it is "comparable to the dogs in side-by-side tests," but the devices never get tired, Raduenz said.

"At Camp Lejeune ... [it's] 97 degrees, with humidity. It's very hot," he said. "Working dogs can get overheated." The device also emits no radiation making it safer to use. Marines at Camp Lejeune are currently training with the devices and they are expected to be deployed this month. The base has purchased five devices, which cost roughly \$21,000 each. Fido is already in use at other Marine Corps bases on the East Coast including Marine Corps Logistics Base Albany, Georgia and Marine Corps Support Facility Blount Island, Florida as and Afghanistan. well as in Irag

#### Nanotechnologists Are Targets of Unabomber Copycat, Alarming Universities

Source: http://chronicle.com/article/Nanotechnologists-Are-Targets/128764/ By Marion Lloyd and Jeffrey R. Young

A package bomb that injured two professors at a university here this month is the latest in a string of attacks by a new terror group inspired by the Unabomber. Its violent actions have put campuses across Mexico on alert and caused

nanotechnology researchers worldwide to take precautions with their mail.



A police officer stands guard after a mail bomb injured two professors at the Monterrey Institute of Technology and Higher Education, near Mexico City.

Nanotechnology was singled out as a target for the attacks in manifestos posted on the Web by the group behind the bombs, which calls itself "Individualities Tending Toward Savagery." It has been linked to attacks in France, Spain, and Chile, and to a bomb sent earlier this year to a scientist at another Mexican university who specializes in nanotech. An analyst who helped identify the Unabomber-who turned out to be a former professor-says the posts show signs of someone well-educated who could be affiliated with a college. The online rants credit the Unabomber as an inspiration. The Unabomber, a former professor of mathematics at the University of California at Berkeley named Theodore Kaczynski, spread fear in academe for nearly 20 years with his mail-bombing campaign, which killed three professors and wounded 23 others until he was arrested, in 1996. Today he sits in a federal prison in Colorado with no chance of parole, but he continues to write articles calling for a revolution to achieve his dream of an end of technology and a return to hunter-gatherer societies.

The new group's latest package exploded in an office on the campus of the Monterrey Institute of Technology and Higher Education, outside of Mexico City, in early August. The blast wounded its intended target, Armando Herrera Corral, director of a technology-transfer center, which the group's manifesto said is key to the university's plan to promote research projects that "are relevant for the progress of nanobioindustry within the country." The explosion also wounded a nearby colleague, Alejandro Aceves López, director of the university's graduate school of engineering and science. Both men are expected to recover from their injuries. Officials closed the campus for a day and have added new security procedures, which include the use of metal detectors at all campus entrances, random sweeps of campus areas with metal detectors, and searching the cars of some students, according to a statement.

The university also sent e-mails to parents of its students (in English translation to the parents of its approximately 100 foreign students) explaining the new security measures, according to a university publicrelations official who asked not to be named, because he was not authorized to discuss the incident. The official said all of the foreign students decided to remain on campus.

#### Nanotechnologists as Targets

In the group's online post (written in Spanish) claiming credit for the latest bombing, the terrorists complained about the growing number of nanotechnology experts in Mexico,



which it estimated at 650. "The ever more rapid acceleration of this technology will lead to the creation of nanocyborgs that can self-replicate automatically without the help of a human," it said. Such a scenario was popularized in Michael Crichton's 2002 novel, Prey (though the post did not cite the work), in which microscopic robots escape from a lab and take over people's bodies. The manifesto argues that nanoscientists "have given their lives for years in the name of human self-destruction."

The same group sent a parcel bomb to a nanotechnology researcher at the Polytechnic University of the Valley of Mexico in April. That package was addressed to "Oscar Camacho" but apparently was intended for the head of the nanotech department, Carlos Alberto Camacho Olguín. The bomb detonated and wounded a security guard; the professor was unharmed. In early May the group sent another bomb to the same university, but the package was intercepted, and no one was injured. In an online manifesto published soon after those attacks, the group threatened more violence. "Last month we made an attempt against Oscar Camacho, today against the institution, tomorrow who knows?" it said. "Fire to the development of nanotechnology, together with those who support it." Mexican lawenforcement officials have called on universities around the country to beef up their security.

The University of the Americas-Puebla, said to be the first institution in the country to set up a nanotechnology major, sent an e-mail message to all students, professors, and staff members alerting them not to open suspicious packages, and held a meeting to discuss other security measures.

"When I heard the news about what happened at Monterrey Tech, I was very worried, because of the large number of students that we have in the program here," says Miguel Ángel Méndez Rojas, coordinator of the university's nanotechnology program, in an email message. "Because we were the first undergraduate program in Mexico, we felt we could be a target." It was "devastating" to read the group's online manifestos, he says. "I'm convinced that the group's phobia of science (and nanotechnology and its risks) comes mostly from ignorance and misinformation." Many people in the region are skeptical of science, he adds. "In our country, and in the whole Latin American region, we put more faith in the supernatural than in reason. This poses fatal consequences, making people view researchers in science and technology with suspicion and hate, as inhuman individuals, who work against society and as the exploiters and destroyers of natural resources." Alfredo Castillo, attorney general in the State of Mexico, where Monterrey Tech is located, said in a news conference that the terrorist group has ties to acts of violence in other countries, although he did not provide details and did not

respond to requests for an interview. Last month members of a group called the ELF Switzerland Earth Liberation Front were sentenced to prison for plotting to bomb an IBM laboratory that does nanotechnology research in Switzerland. It is not clear whether that group has any ties to the Mexican terror group.

#### Watching Their Mailboxes

Though most nanotechnology researchers in the United States are not as nervous as their Mexican colleagues, some are watching the situation-and their mailboxes-closely. "We've warned our faculty and staff and students to be wary of packages, but we're not too concerned at this moment," says Wade Adams, director of Rice University's Richard E. Smalley Institute for Nanoscale Science and Technology. Some U.S. nanotechnology researchers have not yet heard of the bombings, though, or say they feel that risks to their own labs are minuscule. Among the latter is Ian T. Ferguson, chairman of the department of electrical and computer engineering at the University of North Carolina at Charlotte, who works on nanotech projects. "Driving on the road is problematic," he says, putting the risk in perspective. "Today I was driving behind a truck and its tire blew out," which almost caused a crash. "Do I stop driving? No way." Jack Levin, a professor of sociology and criminology at Northeastern University, says he is not surprised to see others follow the Unabomber's pattern of mail bombings followed by anti-technology screeds. "I don't think we should be surprised that killers are inspired by other killers," he says. For such criminals, the main goal of producing manifestos is to justify their violent actions and portray themselves as heroes rather than villains, he argues. "The terrorists are motivated as much from personal pathology as they are from politics or science or antiscience." Some experts wonder whether the bombs in Mexico are the work of a group or the actions of a lone attacker presenting himself as a group in his writings. "Much of it is written in the plural possessive pronoun 'we,' but there are occasions where the singular personal pronoun was used by the author." says Randall G. Rogan, a professor of communication at Wake Forest University. He is an expert on author identification and served on the team of analysts that helped identify the Unabomber, who signed his own manifesto as the work of a group, which he called the

Freedom Club. Based on initial readings of two of the manifestos, Mr. Rogan guesses that the writer has some sort of college education and could even be affiliated with a college. "The author is drawing on data and drawing on references and quoting a variety of scientists"all of which suggests academic training, he says. Mr. Méndez, at the University of the Americas, agrees. He notes that the manifestos are full of references to American texts and suggest that the author, or authors, have a solid command of English. They also know how to use computer networks and technology, and how to build and handle explosives. Such skills suggest a key contradiction in the group's antitechnology position, says Mauricio Terrones, a leading Mexican researcher in nanotechnology, who has worked outside the country since 2010. "They don't want technology, but they use it to

make bombs with gunpowder, a battery, et cetera, and they also use the Internet to make themselves known," wrote Mr. Terrones, who is now a professor of physics at Pennsylvania State University, in an e-mail interview with The Chronicle. "If it weren't for science and technological development, they could never have gone public." In the "endnotes" to its May manifesto, the group anticipates such criticisms. But it denies that its use of the Internet undermines its antiscience stance. "Only in this way can we disseminate our ideas," the manifesto says. "Are you really stupid enough to think that we who criticize the Techno-industrial System would carve this manifesto stone?" in For now, the bomber or bombers who struck Mexican campuses remain at large, acting, as they put it, "without compassion and without mercy."

#### INNOVATION

## Bomb attack on beach in Antalya, Turkey: ten wounded in explosion

Source: http://www.foxcrawl.com/2011/08/28/bomb-attack-on-beach-in-antalya-turkey-ten-wounded-in-explosion/

An explosion occurred Sunday on a beach from Antalya, – a Turkish resort area crammed with tourists during this busy period of the year, agency Dogan revealed. According to the first information the bomb was apparently **buried in the sand** and blew up before noon at about 10 a.m. when vacationers arrived on the seashore. Ten people were reportedly injured by fragments and little stones blasted away by the blow.

Most of the wounded tourists were from Norway and two of them from Romania, the



authorities announced. The rescue teams rushed to the deflagration place and those hit by explosion received medical assistance on site and at Yaşam hospital. The authorities opened an investigation to find out the cause of the blast.

#### Suicide Bombs In Iraq Caused 200 Coalition Soldier And 12,000 Civilian Casualties From 2003-10

#### Written by Grace Rattue

Source: http://www.medicalnewstoday.com/articles/233782.php

In *The Lancet's* special 9/11 issue, a report details the devastating impact of suicide bombs on both Iraqi civilians and coalition troops. The editorial is by Dr Madelyn Hsiao-Rei Hicks,

Institute of Psychiatry, King's College London, UK, and Iraq Body Count, London, UK, and colleagues. In Iraq, two data sets recorded suicide bomb casualties from March 20, 2003 to December 31, 2010, and examined and

compared by investigators. One set documented coalition-soldier deaths from suicide bombs and the other documented deaths and injuries of Iraqi civilians caused by armed violence. 19% (42,928 of 225,789) of overall civilian casualties were caused by documented suicide bomb events, 26% (30,644 of 117,165) of injured civilians, and 11% (12,284 of 108,624) deaths.

For civilians the injured-to-killed ratio was 2-5 individuals injured to one person killed from suicide bombs. 43% of recorded suicide bomb deaths were caused by suicide bombers on foot, suicide bombers using cars cause 36% of documented deaths and 40% of civilian injuries. 75% of the 3,963 identifiable suicide bomb fatalities were men, 11% women, and 14% children. Children made up for a higher ratio of demographically identifiable deaths caused by suicide bombings compared to general armed violence (9%). For women the injured-to-killed ratio for all suicide bombings was a little higher than for men, however, for children the ratio was lower than for both women and men, revealing lower survival of children from suicide bombings.

In at least 159 (16%) of 1,003 suicide bombing events documented, an Iraqi child died, and at least 211 (21%) women or children died of the 1,003 bombings documents. 14% of civilian deaths recorded were police officers, an occupational category overlapping with the demographic category of men and to some degree women. During 2003 to 2010, 200 coalition soldiers were killed in 79 suicide bomb attacks. Compared to coalition soldiers, more Iragi civilians were killed per suicide bombings. These were documented as follows: 175 US soldiers killed in 76 suicide bombs, 16 Italian soldiers killed in one event, three British killed in one event, and four Bulgarian and two Thai soldiers killed in one event. The researchers explain:

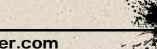
"Rapid access to adequate hospital treatment is crucial for survival of blast injuries, but such access can be difficult for civilians in Iraq. Survival and recovery of Iraqis injured by suicide bombs could possibly have been worsened by Iraq's severe shortage of adequate emergency rooms, diagnostic equipment, trained paramedics and doctors, senior and specialty surgeons needed for complex blast injuries, intensive care units, rehabilitation, and supplies."

They conclude:

"Our findings suggest that the Iraqi civilian population suffers a substantial public health burden because it is a primary chosen target of suicide bombers and those who deploy them. Our findings about the likelihood of surviving injuries, which was particularly low for children recorded in our dataset, need further study and draw attention to the need for improved monitoring. prevention, and interventions to reduce mortality from suicide bombs in Iraq."

In a joint comment, Dr Gilbert Burnham, Johns Hopkins School of Public Health, Baltimore, MD, USA (and co-author on the 2006 Lancet report on deaths in Iraq) states:

"Prevention of suicide attacks is difficult because of their complex origins. The military's approach of controlling access and attacking suspicious targets has protected coalition forces in Iraq, but the resulting deaths of innocent civilians have alienated many Iraqis. This action has played a part in shifting suicide attacks towards civilian targets. Attempts to stop bombers are often futile. Most effective is the elimination of conditions that cause popular support for terrorist groups. Interruption of jihadist networks and their financial support is also a successful approach. The changing habits of populations exposed to terror attacks (eg, the avoidance of high-risk locations) build resilience and individual coping capacities. Eventually, suicide attacks lose their strategic and psychological effect on a population, and insurgent groups shift to other method".



#### Suicide attacks—the rationale and consequences

#### By Gilbert Burnham a

Source:http://www.thelancet.com/journals/lancet/article/PIIS0140-6736%2811%2961258-0/fulltext

The use of suicide bombers as a military and political strategy has a long history. At present, most suicide attacks happen in Iraq, Afghanistan, and Pakistan. In *The Lancet*, Madelyn Hicks and colleagues1 present findings from their study of military and civilian suicide bomb casualties in Iraq, drawing on the extensive but incomplete Iraq Body Count database. For the period between March, 2003, and December, 2010, their database contained information for 1003 suicide attacks on Iraqi targets, which resulted in an estimated 12 284 deaths—79 suicide attacks on coalition forces caused about 200 deaths.

Understanding of the motivations for suicide attacks can help in the development of responses to lessen the chance of suicide attacks, the number of casualties, and the psychological consequences of such attacks. attacks contributed to Israeli withdrawal from Lebanon in 2000, and helped build popular support for Hezbollah. $\underline{2}$ ,  $\underline{3}$ 

Suicide bombing is a misnomer because little evidence exists for the perpetrators having psychopathology or suicidal thinking.4 A common motivation for suicide attacks is retribution, especially for individuals with personal losses, or communal losses with which bombers identify. A sense of humiliation, dishonour, injustice, or deprivation of expected rights and privileges are powerful motivators.5 Palestinian suicide bombers during the second intifada grew up as children during the first intifada, and many shared a sense of defeat and humiliation.6 Conflict over territorial or national control has been a traditional driver for suicide attacks. Examples include the Liberation Tigers of Tamil Eelam's 22-year



As a method of bringing parity in a conflict between unequal forces, suicide attacks have often proved effective. During World War 2, Kamikaze pilots inflicted heavy damage on the US fleet, bringing about a reassessment of the USA's plans to invade Japan. In 1983, suicide attacks on American and French forces in Beirut led to the withdrawal of the international peace-keeping mission from Lebanon. Suicide bombing campaign in Sri Lanka, and attacks by the Kurdistan Workers' Party in Turkey.

Suicide attacks are effective because they show great commitment to a cause. Where there is widespread suffering and anger, attacks can further inflame and radicalise popular opinion, draw financial support, and help to recruit new individuals to terrorist groups.<u>3</u> Groups organising suicide attacks

hope for a strong reaction from authorities to further strengthen their image. Suicide attacks can arise from competition between insurgent groups attempting to build their public stature. Fear, anxiety, and demoralisation of civilian populations and a perceived loss of protection and legitimacy from government are important goals of suicide campaigns. Although religious motivation has played a part in many individual acts and bombing campaigns, religion has had a primary role in suicide attacks only in the past two decades.<u>7</u>

Although suicide attacks are largely politically motivated, criminal elements can take advantage of the chaotic environment they create for extortion and exploitation. In Iraq, suicide attacks are done by three main groups that all seek destruction of the state, but for different reasons.8 The first group are former Baathists and former members of Saddam Hussein's regime who lost positions in 2003. Their resentment has led them to promote state collapse, with suicide bombing as one tactic. A second group that supports suicide attacks are those closely identified with Sunni or other groups whose anger comes from the political ascendancy of Shia and Kurdish Sunnis in Iraq. Both groups draw on popular resentment towards the presence of an occupying power, and capitalise on a historical sense of injustice dating back to the creation of Iraq as a British colony.9 Although superficially Islamist, both groups are essentially secular.

The third and most vigorous users of suicide attacks are the Jihadi Salafis. Their goal is the destruction of the secular state and elimination of roles for non-Sunnis. They seek an Islamic state that is based on the practices of early Islam, sweeping away later traditions of Islamic jurisprudence and elements of democracy. Taliban-controlled Afghanistan was previously a haven for these organisations. Jihadi Salafis are connected with other jihadist organisations in Jordan, Indonesia, Yemen, north Africa, Europe, and elsewhere, not only to share skills and techniques but to enable effective channelling of motivated and educated recruits to Iraq. The killing of Muslim civilians, viewed as apostates and collaborators, is accepted as unfortunate but unavoidable by Jihadi Salafis in their bid to destroy the secular state.

In Afghanistan, the presence of foreign forces and the collateral damage caused by military raids are a potent source of popular anger, as is dissatisfaction with the government. The Taliban's vision of returning to a primitive theocracy resonates with some Afghans, but is not universally shared. Suicide attackers tend to be poor, uneducated, and often with chronic disease or disabilities.10, 11

In Afghanistan, suicide vests or turbans are often used, whereas in Iraq vehicles laden with explosive are the preferred method of bombing, which, along with the lower education level of Afghan bombers, has meant that the number of deaths per event has been less in Afghanistan<u>10</u> than in Iraq.<u>1</u> From 2007 onwards, vehicles were often used in Pakistani suicide attacks, resulting in a death rate per attack much the same as in Iraq.<u>1</u>, <u>12</u>

Prevention of suicide attacks is difficult because of their complex origins. The military's approach of controlling access and attacking suspicious targets has protected coalition forces in Iraq, but the resulting deaths of innocent civilians have alienated many Iragis. This action has played a part in shifting suicide attacks towards civilian targets. Attempts to stop bombers are often futile. Most effective is the elimination of conditions that cause popular support for terrorist groups. Interruption of jihadist networks and their financial support is also a successful approach.2 The changing habits of populations exposed to terror attacks (eq, the avoidance of high-risk locations) build resilience and individual coping capacities.13 Eventually, suicide attacks lose their strategic and psychological effect on a population, and insurgent groups shift to other methods. Witnessing a recent suicide attack at a distance, an Afghan colleague sighed, "Ah, that's just life in Kabul".

#### References

<u>1</u> Hicks MH-R, Dardagan H, Bagnall PM, Spagat M, Sloboda JA. Casualties in civilians and coalition soldiers from suicide bombings in Iraq, 2003—10: a descriptive study. Lancet 2011; 378: 906-914.

2 McBride M, Richard G. Stopping suicide bombing: optimal strategies and unintended consequences. http://www.religionomics.com/asrec/ASREC10\_Papers/McBride\_Richardson-suiciderecruit.pdf. (accessed July 20, 2011).

3 Atran S. Genesis of suicide terrorism. Science 2003; 299: 1534-1539.

4 Post J, Ali F, Henderson SW, Shanfield S, Victoroff J, Weine S. The psychology of suicide terrorism. Psychiatry 2009; 72: 13-31.

6 Sarraj EL. Suicide bombers: dignity, despair, and the need for hope. J Palestine Studies 2002; 31: 71-76.

7 Ginges J, Hansen I, Norenzayan A. Religion and support for suicide attacks. Psychol Sci 2009; 20: 224-230.

8 Hafez MH. Suicide bombers in Iraq: the strategy and ideology of martyrdom. Washington, DC: United States Institute of Peace, 2007.

9 Rosen N. In the belly of the green bird, the triumph of martyrs in Iraq. New York: Free Press, 2006.

10 Fair CC. Suicide attacks in Afghanistan (2001-2007). Kabul: United Nations Assistance Mission in Afghanistan, 2007.

11 Nelson SS. Disabled often carry out Afghan suicide missions. National Public Radio. http://www.npr.org/templates/story/story.php?storyId=15276485. (accessed July 22, 2011).

12 Bhatti JA, Mehmood A, Muhammad S, Bhatti SA, Umbreen A, Razzak JA. Epidemiological patterns of suicide terrorism in the civilian Pakistani population. Int J Inj Contr Saf Promot 2011; 30: 1-7.

13 Strous RD, Mishaeli N, Ranen Y, Benatov J, Green D, Zivotofsky AZ. Confronting the bomber: coping at the site of previous terror attacks. J Nerv Ment Dis 2007; 195: 233-239.

<u>a</u> Center for Refugee and Disaster Response, Johns Hopkins Bloomberg School of Public Health, Baltimore MD 21205, USA

#### Taliban issue statement on use of child suicide bombers

Source: http://www.jamestown.org

Afghanistan's Taliban movement is seeking to deflect a wave of criticism surrounding its alleged use of children as suicide bombers following a public appearance by President Hamid Karzai with eight children the president said were recruited by the Taliban for "martyrdom operations." The eight children were being sent back to their families after being rescued by national security services, while another 12 juveniles were being sent for education and reintegration programs before they are similarly returned home (Reuters, August 30). In the latest incident, a 16-year-old was detained on August 27 in the Baharak district of Badakhshan while wearing a suicide vest. The teenager was stopped while on his way to bomb a local mosque (Frontier Post [Peshawar], August 28).

A report released only days later by Human Rights Watch described "an alarming increase in recent months of suicide bombings and attempted suicide bombings by children." According to the group's Asia director, "The Taliban's use of children as suicide-bombers is not only sickening, but it makes a mockery of Mullah Omar's claim to protect children and civilians." [1]

In response the Taliban issued a statement describing the charges as a "ploy against the mujahideen" by an enemy that is reeling from suicide bombings that the Taliban refer to as "effective tactical enterprises." [2]. To malign this tactic, the "invaders and their internal puppets" have presented the children of employees of their spy agencies as would-be martyrdom-seekers. The movement reminds observers that the Islamic Emirate of Afghanistan has already issued a ban on the recruitment of children in the ranks of the mujahideen. The ban is contained in Article 69 of the Taliban Code of Conduct (or *Layha*), an effort to impose a unified disciplinary code on Taliban fighters. [3]

The movement insists it has not faced any shortage of manpower, suggesting that there are so many volunteers for martyrdom operations that would-be suicide bombers must wait months for an opportunity to carry out "their jihadist task."

According to the Taliban statement, there are three Shari'a-based preconditions for recruits willing to carry out martyrdom operations:

- The volunteer's intention "should be for the sake of Allah".
- The volunteer should have the capability of inflicting heavy losses on the enemy.
- The volunteer should be armed with full military training and capacity.

The Taliban use the statement to reject the concept of using children as mujahideen or as martyrdom-seekers, pointing out that such use would only inhibit the success of martyrdom operations as an effective military tactic as they lack the "physical and mental capacities" and "deep Islamic knowledge and motive" necessary to bring the task to completion.

#### Notes:

Human Rights Watch, Afghanistan: "Taliban Should Stop Using Children as Suicide Bombers," August 31, 2011, http://www.hrw.org/news/2011/08/31/afghanistan-taliban-should-stop-using-children-suicide-bombers.
 "Statement of the Islamic Emirate in Response to the Propaganda about Recruitment of Children in Martyrdom-seeking Attacks," September 5, 2011.

3. Muhammad Munir, "The Layha for the Mujahideen: an analysis of the code of conduct for the Taliban fighters under Islamic law," *International Review of the Red Cross*, No. 881, March 31, 2011, http://www.icrc.org/eng/resources/documents/article/review-2011/irrc-881-munir.htm.

#### An amazing story

Source: http://www.militarytimes.com/multimedia/video/rpg\_surgery/

You all know that a "RPG" is a rocket propelled grenade.



This video story is about Channing Moss, who was impaled by a live RPG during a Taliban ambush while on patrol.

Army protocol says that medivac choppers are never to carry anyone with a live round in him.

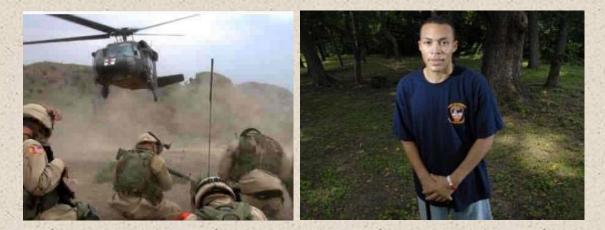
Even though they feared it

could explode, the flight crew flew him to the nearest aid station.

Again, surgical unit protocol says that in such a case the patient is to be put in a sandbagged area away from the surgical unit, given a shot of morphine and left to wait (and die) until others are treated. The whole medical team voluntarily performed the emergency surgery to remove the RPG.

Here's a short video put together by the Military Times, which includes actual footage of the surgery where Dr. John Oh, a Korean immigrant who became a naturalized citizen and went to West Point, removed the live round with the help of volunteers and a member of the EOD (explosive ordinance disposal) team.

Moss has undergone six operations but is doing well at home in Gainesville, GA.







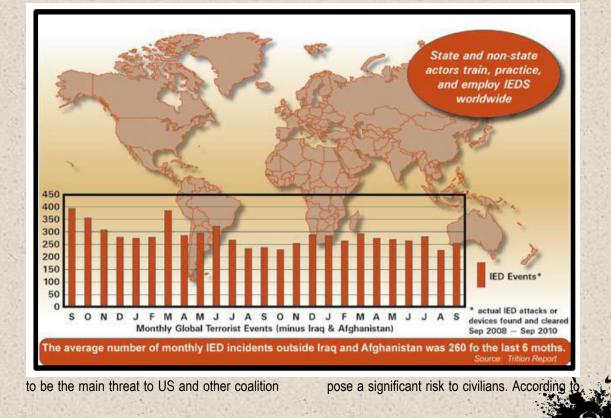
Watch the video at: <a href="http://www.militarytimes.com/multimedia/video/rpg\_surgery/">http://www.militarytimes.com/multimedia/video/rpg\_surgery/</a>

#### **Understanding the basics of IEDs**

By John Caldwell C-IED Knowledge Manager

Improvised explosive devices (IEDs) continue

forces in both Afghanistan and Iraq. They also



the United Nations Annual Report on Protection of Civilians in Armed Conflict, IEDs were the primary cause of violent civilian death in Afghanistan in 2010. In Iraq, an average of nearly two explosions per day by violent extremists in 2010 resulted in 685 explosions, killing 2,649 civilians.

Nor are the risks from IEDs solely in Afghanistan and Iraq. The US military command known as the Joint IED-Defeat Organization, or JIEDDO, stated in their 2010 annual report that IEDs continue to be the weapon of choice for global insurgents, with approximately 260 IED incidents per month occurring outside of Afghanistan and Iraq.

In the most basic terms, IEDs are homemade bombs. According to U.S. Army Field Manual 3-34.119, they can be made with explosives alone, or combined with other materials, such as projectiles or toxic chemicals, to create an expedient, effective, and dangerous weapon

Main Charge Explosive Filler Initiating System Switch Initiator In

vehicle, or be loaded in a car or truck and driven into markets or buildings. In the past few years, as military and commercial grade explosives become more difficult to acquire, bomb-makers have become increasingly creative by making IEDs from home-made characteristics, explosives (HME). The composition, and method for initiating IEDs are constantly changing, and the degree of complexity and sophistication of an IED is limited only by the ingenuity and the materials available to the bomb-maker. Although the difference may seem slight, and even though the effect of the explosions may be quite similar, a mine is not considered an IED unless it has been modified (improvised) in some fashion.

#### **Basic Components of an IED**

The basic elements of an IED consist of a main explosive charge, a power source, an initiating

system, and a casing or container. The IED is triggered by the initiating system, which could be a pressure plate, mobile phone, radio, timer or wire physically connected to the device. A battery is used as the power source. When the firing mechanism is triggered and the circuit is completed, a signal is sent to the initiator - a blasting cap or detonating cord - which then detonates the main charge. Common explosive charges could include mortar, artillery or tank ammunition rounds, since they are the easiest to handle and provide a ready-made means of fragmentation. However, when military munitions are not available, main charges can be made from plastic explosive, trinitrotoluene (TNT), ammonium nitrate fertilizer, fuel oil, or other types of explosive ingredients and placed in a container. In some cases, ball bearings, nuts, bolts, nails or other hardware can be added to the IED

that can cause death or serious injury to large numbers of people. IEDs can vary widely in shape and form – ranging from small pipe bombs to multiple artillery shells linked together to create a device with greater explosive weight. They can be planted alongside a road, magnetically attached to a target, placed in a to enhance the fragmentation.

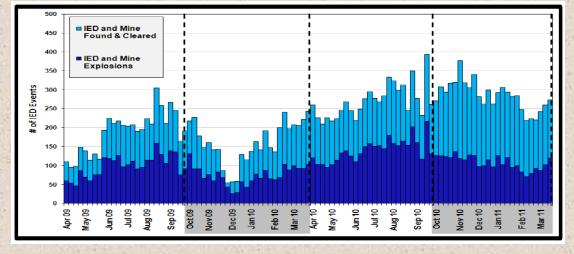
#### Types of IEDs

In generic terms, IEDs can be broken into several different types – depending on the method of detonation or the method of delivery.

There are three basic methods to initiate detonation of the IED. It can be detonated by command, by time, or it could be initiated through actions by the victim. In command detonation, someone observing the target area could trigger the IED by either a wire directly connected to the device or by remote control through wireless devices such as cell phones, pagers, remote car door openers, or garage door openers. IEDs triggered by wire are sometimes referred to as CWIEDs (commandwired) while those that are remotely detonated are known as RCIEDs (radio-controlled). A timed IED is designed to detonate at a specified time after the device is planted, thus providing the emplacer sufficient time to get away from the scene of the explosion. Finally,

explosion. While the most common VBIED is a car or truck, that doesn't have to be the case. The 2000 attack on the USS Cole in Yemen was carried out by terrorists on a boat loaded with explosives.

Suicide bombers constitute another category of IEDs. Suicide bombers may opt to attack using a vehicle laden with explosives, or the attacker could choose to wear an explosive belt or vest. Suicide bombers who use an explosive vest or belt to conduct the attack are referred by the military as person-borne IEDs (PBIED). The IED could be triggered by the bomber or by another person located nearby. In recent years, suicide bombers have targeted crowded markets, funerals, wedding celebrations, local police and government facilities, and military



a victim-operated IED (VOIED) detonates when a person or vehicle triggers the initiator – which could be a trip wire, a pressure plate or pressure release mechanism, a light sensitive apparatus or other similar devices – resulting in the explosion.

Another type of IED is the vehicle-borne IED (VBIED), commonly referred to as a car bomb. The vehicle may be as small as a bicycle, motorcycle or as large as a car, van, or truck. It could be parked along a road or a target building, or could be driven by a suicide bomber. In many cases, VBIEDs are frequently used near crowded areas in order to maximize their destructive power and instill terror within the population. As insurgents have become more adaptive in their efforts, many VBIEDs may have a second person ready to initiate the attack in case the primary triggerman hesitates or is unable to conduct the attack. It is also not uncommon for terrorists to place other IEDs in the vicinity of the attack to target emergency personnel who may respond to the initial

recruitment centers. In some cases, female suicide bombers and unsuspecting children have been used to conduct attacks.

#### **IED Trends in Afghanistan**

According to JIEDDO, the volume of IED use in Afghanistan in fiscal year 2010 increased significantly over 2009. That trend has continued into 2011. The US Department of Defense Semiannual Report on the Progress toward Security and Stability in Afghanistan stated that overall IED activity from October 2010 - March 2011 remained 'elevated'. As seen in the chart from the DoD semiannual report below, the number of weekly IED events during the winter of 2010 - 2011 is noticeably higher than 2009 - 2010. Similarly, the UK newspaper, The Telegraph, reported on 2 September 2011 that the use of IEDs rose 14% year-on-year in the 2nd guarter of 2011. Citing JIEDDO sources, the article went on to say that from April to June, 2011, 3,845 IEDs exploded or were found. Coalition killed and wounder

from IEDs rose 15% yearly to 1,248 soldiers over the same period. Citing a United Nations report released in August, *The Telegraph* reported that 60% of coalition casualties and 30% of civilian casualties were caused by IEDs.

In general, IEDs in Afghanistan tend to be of simple, but effective, design. They tend to be primarily victim-operated or command wire IEDs. Despite a ban enacted in February 2010 to prevent the import, sale, manufacture, and use of ammonium nitrate fertilizer, many IEDs are prepared using home-made explosives (HMEs). Increasingly, many IED attacks are targeting military personnel on foot patrols.

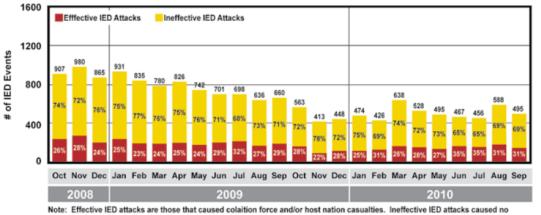
#### IED Trends in Iraq

In Iraq, the overall number of IED attacks has been drastically reduced, and according to 42 apparently coordinated attacks against Iraqi security forces and civilians killed 89 people, including 3 suicide bombers, and injured 315 others. The most lethal attack occurred in Kut, when two car bombs exploded, killing 35 and wounding 71 Iraqis.

#### **Individual Protective Measures**

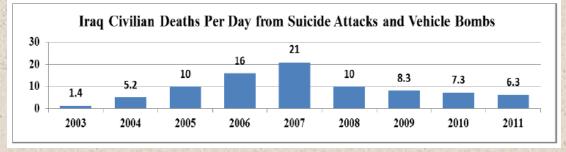
Military forces have invested vast amounts of resources over the past decade in an effort to detect and defeat IEDs. However, a Homeland Security Newswire report in October 2010 indicates bomb-detecting dogs are more effective in detecting IEDs than the most sophisticated detection technologies.

For civilians working in high threat environments that likely will not have access to intelligence information or IED detection technology that military forces possess, host



Note: Effective IED attacks are those that caused colaition force and/or host nation casualities. Ineffective IED attacks caused no casualities and include detonations with no casualities, early detection, pre-detonations, and turn-ins.

JIEDDO, is currently at levels that have not been seen since 2003. However, despite the decline in the number of IED attacks from its peak of 3500 events per month in 2006, JIEDDO's 2010 Annual Report shows that substantial numbers of IED attacks still occur each month (see chart below). Nor are the casualties insignificant. Data from nation civilians may sometimes be able to provide information on dangerous areas that should be avoided. However, the number one way to protect yourself and others from an IED attack is to be alert to your surroundings. Although not intended as an inclusive list, some examples of possible roadside IED indicators from FMI 3-34.119/MCIP 3-17.01



iraqbodycount.org shows that in 2011, an average of over six people are killed each day from IED attacks (see chart below). The New York Times reported that on 15 August 2011,

include:

 Unusual changes in community patterns, such as fewer people or



vehicles in a normally busy area, or the absence of women or children

- Personnel on overpasses
- People videotaping ordinary activities or military actions. Insurgents using IEDs will often tape their activities for use in recruiting, training, or planning
- Suspicious or metallic objects, such as cylinders or 5-gallon jugs / cans
- Colors that seem out of place, such as freshly disturbed dirt, concrete that does not match the adjacent / surrounding blocks, colored detonating cord or other parts of an IED that may be exposed
- Markers by the side of the road, such as tires, rock piles, that may identify an IED location to the local population or serve as an aiming reference

The US Department of Homeland Security issued some basic guidelines for actions in the event of an IED attack. While the guidelines are directed toward domestic threats, the principles appear equally useful for civilians working in high-threat environments overseas.

Steps to take if you see something suspicious

- Trust your instincts, if something feels wrong, don't ignore it. Contact the authorities.
- Keep your distance from suspicious packages or devices
- Make a personal plan for emergency response, to include:

- emergency procedures at your place of work or places you visit frequently
- ✓ know how to get out of the area
- ✓ routes to local hospitals
- ✓ take a first aid course

What to do if you encounter an IED attack

- If you are in a building, get under a sturdy table or desk if objects are falling around you.
- If you are outside, move away from the blast area to a safe location. Be aware that secondary explosions may occur at or near the original bombing site – either by accident or by design
- If you are near, but not at the immediate site of an IED attack, avoid being lured closer to see what is happening due to risks of secondary



#### attacks

The IED is not a new phenomenon on the battlefield. It is one of the main causes of casualties among military forces and exacts a heavy toll on local populations. With its proven lethality and effectiveness, it will likely continue to be a weapon of choice among poorly armed insurgents in the future. Nongovernment and international organization civilian employees working in high-threat areas to alleviate battlefield.

suffering and / or promote conflict resolution, health care, economic development, environmental protection, and other similar

#### Laser device detects IEDs

Source: http://news.msu.edu/story/9780/

A research team at Michigan State University has developed a laser that could detect roadside bombs — the deadliest enemy weapon U.S. and coalition soldiers encountered in Iraq and Afghanistan.

The laser, which has comparable output to a simple presentation pointer, potentially has the sensitivity and selectivity to canvas large areas and detect improvised explosive devices — weapons that account for around 60 percent of coalition soldiers' deaths. A Michigan State University release reports that Marcos Dantus, chemistry professor and founder of BioPhotonic Solutions, led the team and has published the results in the current issue of



*pplied Physics Letters*, The detection of IEDs in the field is extremely important and challenging because the efforts should be aware of the risks and exercise care as they conduct their daily activities.

environment introduces a large number of chemical compounds that mask the select few molecules that one is trying to detect, Dantus said.

"Having molecular structure sensitivity is critical for identifying explosives and avoiding unnecessary evacuation of buildings and closing roads due to false alarms," he said

Since IEDs can be found in populated areas, the methods to detect these weapons must be nondestructive. They also must be able to distinguish explosives from vast arrays of similar compounds that can be found in urban environments. Dantus's latest laser can make these distinctions even for quantities as small as a fraction of a billionth of a gram.

The laser beam combines short pulses that kick the molecules and make them vibrate, as well as long pulses that are used to "listen" and identify the different "chords." The chords include different vibrational frequencies that uniquely identify every molecule, much like a fingerprint. The high-sensitivity laser can work in tandem with cameras and allows users to scan questionable areas from a safe distance. "The laser and the method we've developed were originally intended for microscopes, but we were able to adapt and broaden its use to demonstrate its effectiveness for standoff detection of explosives," said Dantus, who hopes to net additional funding to take this laser from the lab and into the field.

This research is funded in part by DHS. BioPhotonic Solutions is a high-tech company Dantus launched in 2003 to commercialize technology invented in a spinoff from his research group at MSU.

— Read more in Marshall T. Bremer et al., "Highly selective standoff detection and imaging of trace chemicals in a complex background using single-beam coherent anti-Stokes Raman scattering," Applied Physics Letters, 99, no. 10 (9 September 2011) (DOI: 10.1063/1.3636436)



187 6

276

# Cyber News

# Study finds nearly 90 percent of businesses victim of cyber attacks

Source:http://www.channelinsider.com/c/a/Security/Cyber-Security-Breaches-Hit-90-Percent-of-Businesses-Report-410815/

A recent survey of information technology (IT) security professionals reveals that cyber attacks are on the rise and businesses have had difficulty defending their networks.

The survey, conducted by the Ponemon Institute and sponsored by Juniper Networks,

SSWORD

confidence in their organization's ability to protect their networks.

"Our survey research provides evidence that many organizations are ill-equipped to prevent cyber attacks against networks and enterprise systems," said Dr. Larry Ponemon, chairman

> and founder of the Ponemon Institute. "This study suggests conventional network security methods need to improve in order to curtail internal and external threats."

> Mark Bauhaus, the executive vice president and general manager of Juniper Networks' device and network services business group, added, "The size and complexity of today's security threats

found that of the more than 1,000 IT security professionals polled, 84 percent admitted to having been the victim of a cyber attack. In addition nearly 60 percent admitted that their organizations had experienced multiple network breaches in the past twelve months.

These cyber attacks have been costly causing a majority of companies an estimated \$500,000 or more in lost revenues, cash outlays, business disruptions, and other expenses.

The survey also indicated that attacks are on the rise with more than 43 percent revealing that they have experienced a sharp increase in the frequency of attacks in the last twelve months. In addition, 77 percent of respondents say the attacks have become more severe and difficult to detect and defend against which has led 34 percent to say that they had little continue to intensify, leaving organizations and governments vulnerable to cyber attacks."

He continued, "Business leaders need to consider a more aggressive, systemic security approach—implementing end-to-end comprehensive protection at all points in the network to help mitigate risk."

To help secure networks from attacks, 76 percent said that streamlining and simplifying network security operations would make them more secure and 75 percent said their effectiveness would increase by implementing end-to-end solutions.

In particular, mobile devices and laptops are the most likely entry points that hacker use to break into networks or unleash viruses. 34 percent of attacks originated from laptops and 29 percent from mobile devices.



# Google Ideas think tank gathering former extremists to battle radicalization

Source:http://www.linkedin.com/share?viewLink=&sid=s443489248&url=http%3A%2F%2Ft.co%2FVvO H1n6&urlhash=8BiD&uid=5490241967411429376&trk=NUS\_UNIU\_SHARE-lnk

Technology giant Google, having conquered the Internet and the world around it, is taking on a new challenge: violent extremism.

The company, through its eight-month-old think tank, Google Ideas, is paying for 80 former Muslim extremists, neo-Nazis, U.S. gang members and other former radicals to gather in Dublin this weekend to explore how technology can play a role in de-radicalization efforts around the globe.

The "formers," as they have been dubbed by Google, will be surrounded by 120 thinkers,

activists, philanthropists and business leaders. The qoal is to dissect the question of what draws some people, especially young people, extremist to movements and why some of them leave. "We are trying

to reframe issues like radicalization and see how we can apply technology to it," said Jared the 29-year-old former State Cohen, Department official who agreed to head Google Ideas with the understanding he would host such a conference. "Technology is part of every challenge in the world and a part of every solution."

In forming Google Ideas, company officials said, they were eager to move beyond the traditional think tank model of conducting studies and publishing books, saying their "think/do tank" would make action a central part of its mission.

But in its first venture, the decision to enter the space between thinking and doing is also drawing some criticism as Google steps enthusiastically into what many view as an intractable, enduring problem - and one that has traditionally been left to governments.

even Nye

Google Ideas may be setting its sights too high, said Christopher Boucek of the Carnegie Endowment for International Peace, and getting terrorists to give up violence may be a more attainable goal than getting them to change their sympathies.

"You'll never make a hard-core jihadi into a Jeffersonian democrat — it's just not going to happen," he said. He also noted that while there may be common threads to why people join extremists groups, the remedies to that problem are more likely to be "culturally, and

country, specific."

Harvard University professor Joseph S. Jr., who specializes in theories and application of power, agreed that the endeavor "could be problematic especially if it is perceived to be in conflict with the foreign policy of the United States." He added that the

ambition could "complicate things further since profit is ostensibly involved."

Officials at Google express little concern that their efforts are overly ambitious or will tread in others' territory.

Eric Schmidt, Google's executive chairman, said the company decided to get in the think tank business with the goal of tackling "some of the most intractable problems facing mankind by combining a new generation of leaders with technology. We're not looking for silver bullets but new approaches."

Up to now, efforts to reform extremists have largely been government-run and focused on distinct groups. Many of the programs have operated in Muslim countries, and their sponsors have struggled with whether it was enough to get radicals to disengage from extremist movements or whether they must reject extremism and embrace mainstream values.



Cohen said the approach at the conference will be to treat extremism as a universal problem that cuts across cultural, ideological, political, religious and geographic boundaries. Bringing together former extremists from a variety of backgrounds, he theorizes, could point to common factors that pull people into violence. "If we compartmentalize different radicalization

challenges, that also means we compartmentalize the de-radicalization solutions," and that could be a lost opportunity, he said.

Although he didn't want to prescribe an answer, he said a campaign in the coming months could harness the power of YouTube, employ advanced mapping techniques or create alternative Web spaces to compete with radicalizing voices.

Cohen, a former aide to Secretaries of State Condoleezza Rice and Hillary Rodham Clinton who had focused at the State Department on counterterrorism and radicalism, said he joined Google to escape some of the limitations on what can be done within a government agency to address extremism.

"You can't build things," said Cohen, noting that government often lacks the resources to create technologies aimed at complex social and political problems.

In his new job, heading a think tank supported by a company that earned \$30 billion in sales last year, the limitations are guite different.

"There's no sense in bothering with some of these challenges at a place like Google if we can't take risks," he said.

In the future, Cohen predicted, the think tank will take on the challenges of fragile states, democracy building, and questions about the Internet and society.

Google Ideas, with six full-time employees working out of the company's New York offices, is somewhat removed from the Washington environs where Cohen had operated for the past several years. He had become known at the State Department for bringing together unlikely participants, often in gatherings with a strong technology component.

In 2009, Cohen drew attention when he asked a friend, Twitter co-founder Jack Dorsey, to

delay a scheduled maintenance shutdown so protesters in Iran could coordinate during an uprising and reach international media.

The White House had wanted to fire Cohen after the incident, out of concern the United States would be seen as meddling in Iranian affairs, according to a report in the New Yorker, but he stayed in his job.

This weekend's conference, formally known as the Summit Against Violent Extremism, or SAVE, will run Sunday through Tuesday.

Among the speakers will be T.J. Leyden, a former skinhead leader from California and now executive director of Hate2Hope. Leyden has said he began to turn away from the white supremacist movement as he watched his young children take on his anger and bigotry.

Another participant, Maajid Nawaz, is a British citizen of Pakistani descent who resigned from Hizb ut-Tahrir, a pan-Islamist group whose goal is to establish a global Islamic state, and now leads an organization that counters Islamic extremism.

The conference will also include Carie Lemack, whose mother was killed in one of the planes that crashed into the World Trade Center. Lemack co-founded Global Survivors Network, an organization for victims of terrorism and produced the documentary "Killing in the Name."

"The hope from the conference is that we will figure out some of the 'best practices' of how you can break youth radicalization," said James M. Lindsay, a senior vice president at the Council on Foreign Relations, which is helping organize the summit.

Cohen also turned to the Tribeca Film Festival, which was founded to help bring people back to the lower Manhattan neighborhood after the Sept. 11 attacks.

Jane Rosenthal, co-founder of the festival, is making a film about de-radicalization that will draw on the work coming out of the conference. "You have to create deeper opportunities for involvement," she said.

Follow Allen McDuffee's reporting from the Google Ideas conference at Think Tanked and live updates on Twitter.



# Cybercrime statistics wildly inaccurate

Source:http://www.homelandsecuritynewswire.com/cybercrime-statistics-wildly-inaccurate-says-researcher

A cybersecurity researcher is questioning the various statistics that U.S. government officials and IT companies use as evidence of the rampant and deleterious effects of hackers.

Cormac Herley, a principal researcher at Microsoft Research, argues that the existing data on the estimated losses from cyberattacks is wildly inaccurate to the point that analysts have no idea what the problem's economic impacts are.

As evidence he cites the fact that in three

He added these numbers "just didn't make sense."

In addition to their wide range, some of them are illogically high. For example, he says the \$1 trillion figure would mean that every adult in the United States that was online lost \$5,000.

Herley says that the lack of accurate data has serious consequences.

"Without numbers, we can't make good policy or sound investment decisions," he said."Not only that, but we can't figure out where key



instances, corporate executives presented numbers that dramatically differed.

Patrick Peterson, the chief security researcher at Cisco, estimated that losses from cyberattacks totaled \$560 million in 2009, while Killian Straus of the Organization for Security and Cooperation in Europe estimated costs at \$100 billion each year, and Edward Amoroso, AT&T's chief security officer went so far as to say that cybercrime was generating illicit revenues of \$1 trillion a year.

"How can this be?" Herley asked. "How can you have estimates of the same problem ranging across three orders of magnitude?" threats are coming from. Are the criminals making most of their money from key logging? Highly targeted phishing attacks? Brute-force attacks on people's passwords?"

"It's distressing," he concluded.

In investigating the matter further, he found that the methods used to calculate these estimates were insufficient to yield accurate results.

The majority of the data was based on surveys which asked respondents to report if they had been the victims of cybercrime and how much they lost.

"Surveys are hard," Herleyexplained.



Unlike other polls, cybercrime surveys seek to measure specifically how much money was lost which makes an individual's response much more important and varying numbers could alter the survey's results. For instance if respondent claims to have lost \$500,000 when in fact they only lost \$500,000 that could dramatically change the survey.

In addition, a survey's relatively small numbers has a tendency to skew the significance of data. In a 2006 survey conducted by Gartner Research, 128 out of 4,000 people claimed to have been victims. Based on Herley's calculation 59 percent of losses came from the top 1 percent of respondents who had been victimized which was just one person.

Julie Ryan, a professor in information security management at George Washington University, shares Herley's concerns.

"Understanding the impact of any crime is problematic," but cybercrime is particularly problematic as most people don't know enough about the technical aspects behind the attack she said.

Survey respondents rarely know how to distinguish if they were thevictims of a phishing attack or if anything was actually stolen or corrupted.

"So here we have a problem," Ryan said. "Potential crime that is potentially undetectable, compounded by a target space that is mostly ignorant."

Furthermore, Ryan said there is an information bias as most big corporations are reluctant to share their cyberattack history for fear of losing customers, while cyber security firms benefit from these details.

To provide more accurate statistics, Herley is pushing the companies and organizations that conduct surveys to be more transparent about their survey methods so that researchers can evaluate their accuracy.

In particular, Herley hopes that organizations publish median figures instead of averages as they are less likely to be affected by outliers and are therefore less susceptible to exaggeration.

# America's power grid too vulnerable to cyberattack, US report

#### warns

Source: http://www.jewishworldreview.com/0711/power\_grid\_attack.php3



America's power grid remains vulnerable to cyberattack, a result of sluggish

implementation of weak computer security standards and insufficient federal oversight

says a tough new report from the US Department of Energy Inspector General.

The North American Electric Reliability Corp. (NERC), the lead grid-reliability organization for the power industry, has had approved standards in place since January 2008. Power companies were to have fully implemented those "critical infrastructure protection" (CIP) cyberstandards a year ago, but the standards still aren't doing an effective job, the inspector general's audit found.

"Our testing revealed that such standards did not always include controls commonly recommended for protecting critical information systems," including tough password and log-in protections, the report said. The plodding implementation is "not adequate to ensure that systems-related risks to the Nation's power grid were mitigated or addressed in a timely manner."

Among its other findings are the following:

- The new CIP standards set weaker requirements for password and log-in protections than is common for other types of critical infrastructure.
- The Federal Energy Regulatory Commission (FERC), which approved the security standards that NERC developed, is partly to blame. The commission ultimately "did not have authority to implement its own reliability standards or mandatory alerts in response to emerging threats or vulnerabilities," the report said. In instances where FERC did have authority to strengthen CIP standards, "the commission had not always acted to ensure that cyber security standards were adequate."
- The standards don't "clearly define what constituted a critical asset or critical cyber asset," the report found. Instead, utilities "were permitted to use their discretion when identifying critical assets and critical cyber assets...." As a result, "if an entity determined that no critical assets or critical cyber assets existed, it was exempt from the remaining original CIP standards," the report said.

How to define "critical infrastructure" is a big part of the problem. "Lack of stringent requirements for defining critical assets contributed to a significant underreporting of these assets," the IG found. Both the federal commission and NERC officials said power companies had probably undercounted their critical assets and associated critical cyberassets.

"Much of the problem stems from ... lack of definition," says Michael Assante, former chief security officer for NERC. "The concepts of what need to be protected have not been firmly established."

Critical assets could include, for instance, control centers, transmission substations, and power generators. But on a compliance selfsurvey, only 29 percent of power generators and less than 63 percent of transmission owners identified one or more critical assets, NERC reported in April 2009.

The IG's office also found that NERC and eight other regional electricity reliability organizations appear to have ignored federal demands to toughen the original CIP standards. One FERC official noted that 95 percent of the changes the commission requested of NERC had not been addressed, the IG said.

The result is that federal regulators have made little progress toward accurately assessing what needs protecting on the grid. The IG's office recommends these fixes: that Congress give FERC greater authority to ensure grid cybersecurity; that tougher cybersecurity standards be adopted; that FERC intensify its oversight of NERC and other grid-reliability entities; that FERC adopt measurements to assess the performance of NERC and the other regional overseers.

"We found that these problems existed, in part, because [FERC] had only limited authority to ensure adequate cyber security over the bulk electric system," the IG report states.

In a response to the IG's report, FERC chairman Jon Wellinghoff agreed with most of its recommendations.

Mr. Assante, now president of the National Board of Information Security Examiners, a standards-setting body for cybersecurity experts, characterizes the CIP standards as only "a minimum set of sound security practices that reinforces the need for utilities to protect themselves and each other."

Given the advent of cyberweapons that can destroy computer-controlled critical infrastructure, such as the Stuxnet worm that was aimed at Iran's nuclear facilities, the IG's report correctly identifies the issues needed to improve grid security, say grid cybersecurity experts.

"The standards have not been implemented with a strong sense of risk in mind," Assanted

says. "The complexity of enacting a new regulatory regime has taken our collective eye

off security and turned it toward administrative issues and compliance."

#### **Detecting fake Web sites**

Source: http://www.homelandsecuritynewswire.com/detecting-fake-web-sites

Sign In

eBay members, sign in to save time for bidding, se

Keep me spred in on the computer unless I sign est.

st protection, sign 1 Secure Alen. In (1954)

A team of researchers develop a new -- and more reliable -- way to detect fake Web sites; the team developed five categories with thousands of cues, finding that the best results were attained when utilizing thousands of highly visible and also deeply embedded cues, such as placement, URL length, the number of links, characters types on the site and how thorough the site's "frequently asked questions" section is detailed, among other features.

4 + G + Ohttp://signin.ebay.com.account.rndsystems.co.kr 7308/ebay.htm

Aiready an ellay user?

Bay User ID

fortet in

(Sign In 2-)

Accountements | Register 1 Security Center | Policies 1 Feedback Forum | About eBay

III Apple All News + Subplog 703 +

Sign In

iew to eBay?

(Begister or)

Sign In an

If you want to sign in, you'll need to register first.

Registration is fast and free

more accurate detections of spoof sites – better than a human can.

The team's subsequent article, "Detecting Fake Websites: The Contribution of Statistical Learning Theory," was published last year in an issue of MIS Quarterly, or MISQ, a leading journal in the field of management information systems. A university of Arizona release reports that MISQ has since been named the article its top paper for 2010.

"Even to get into MISQ is very difficult, and this is probably the first technical paper to receive

+ Q+ Comp

the Best Paper award,"
said Hsinchun Chen, the
UA Artificial Intelligence
Lab director, one of the
paper's five authors.

"The topic of detecting fake websites and also our computational approach are both considered major contributions. This topic has great relevance to the industry, the society and the citizens in general," said Chen, also McClelland the Professor of Management Information Systems.

"This award is not something just for me, or my lab, but also for our

department," he said, adding that the team's eventual goal is technology transfer.

UA alumnus Ahmed Abbasi, now a University of Virginia assistant professor of information technology, is lead author on the paper. Chen served as his dissertation adviser. Other coauthors are UA Eller College's department of management information systems faculty members Zhu Zhang and Jay F. Nunamaker Jr.; and David Zimbra, a doctoral student in the Artificial Intelligence Lab.

For the research, the team used the prototype and several other detection systems to evaluate the authenticity of 900 Web sites.

# This web page is not what it appears to be // Source: sillydog.org

You can also register or sign in using the following service

235-2554 eBay Inc. All Rights Reserved. Indemarks and brands are the property of th

Do you go online to pay bills, shop, transfer funds, sign up for classes, send e-mail or instant messages, or search for medical information? If so, read on.

Members of a University of Arizona Eller College of Management team and a UA alumnus developed a prototype system to detect fake Web sites. When tested against other existing commercial systems, the team found that its system resulted in effective and

TRUBT

It is easy to pick up on a site's authenticity by checking whether the URL contains "http" when it should read "https," when it was last updated, if a security key is missing or if images appear strangely pixelated.

The team found that its system – founded on statistical learning technology, which evaluates a large accumulation of data – was more apt to detect imitation sites and those that were entirely concocted, said Abbasi, who earned his doctoral degree in management information systems from the UA in 2008.

The major difference between the authors' prototype and the other systems? Their system relied on a tremendously rich set of fraud cues. The team developed five categories with thousands of cues, finding that the best results were attained when utilizing thousands of highly visible and also deeply embedded cues, such as placement, URL length, the number of links, character types on the site, and how thorough the site's "frequently asked questions" section is detailed, among other features.

The release notes that the project's origins were born out of the Artificial Intelligence Lab, where Abbasi developed the mathematical formula the team eventually used while working as a project lead and research associate. He continued the work after having taken a faculty position at the University of Wisconsin-Milwaukee.

"It creates a greater awareness for a problem that has been around for a while yet still remains an issue as we increasingly move to the Internet for everything – online banking, online health initiatives and medical information," Abbasi said. Given the pervasive nature of online phishing scams, being able to readily and frequently detect a site's validity is crucial, Abbasi said, also noting research that indicates people are less than 60 percent accurate in detecting fake sites, and other security issues.

"The problem we're looking at is quite big. Fake websites constitute much of the Internet fraud's multi-billion dollar industry, and that is monetary loss...we can't even quantify the social ramifications," Abbasi said. "That's the whole motivation. It is so profitable for fraudsters, and it is slipping through the cracks."

Today, Chen and more than one dozen of his collaborators are continuing to investigate fake sites. Meanwhile, Abbasi is undertaking an investigation of peoples' abilities to detect fake sites through a grant funded by the National Science Foundation.

Today, Chen and more than one dozen of his collaborators are continuing to investigate fake sites. Meanwhile, Abbasi is undertaking an investigation of users and peoples' abilities to detect fake sites.

Abbasi said developing better detection systems requires improved statistical learning technology that utilize larger quantities of cues. It also is important to dismiss long-held perceptions about how fake sites might and should appear.

"The idea of protecting from the front level has been around for a while," Abbasi said, adding that companies have begun to employ software that better detects fake sites. "But we are not where we need to be, and there is a lot of potential in future development."

### Al-Qaeda's cyber jihad on Facebook

#### Fanatics target social network sites

Source:http://www.thesun.co.uk/sol/homepage/news/3691372/Al-Qaedas-cyber-jihad-on-Facebook. html?OTC-RSS&ATTR=News

AL-QAEDA is plotting a devastating "cyber jihad" against Britain and the West, it was revealed yesterday. Terrorists have even tried to "invade" Facebook in their campaign of electronic warfare. The extremists have launched crack units to target key computer systems. And Google Earth and Street View are being used to help plan atrocities.

The warnings came as Home Secretary Theresa May unveiled the Government's new counter-terrorism strategy. Senior security



officials say cyber-terrorism will become an ever growing threat. One source said; "At the

moment incidents are few and far between but it's a taste of things to come."

A 123-page counter-terror blueprint reveals that a special unit - the Tariq bin Ziyad Brigades for Electronic Jihad - attacked computers last year. The document said: "Since the death of Osama Bin Laden, al-Qaeda has called not only for acts of lone or individual terrorism but also for cyber jihad." Hate preachers are making increased use of the internet.

Experts estimate there are thousands of terrorist-related websites. The report adds: "A few dozen are highly influential and frequented

by terrorists. "Use of social networking sites and video sharing is now commonplace. There have been a number of attempts by terrorist and extremist groups to 'invade' Facebook."

Twitter is used to flag up extremist articles and websites. Mrs May said: "Terrorists are increasingly using online technology, including Google Earth and Street View, for attack planning. "The attacks in Mumbai in 2008 were directed by people using off-the-shelf secure communications technology." Terrorists also use hi-tech encrypted mobile phones and texts to avoid detection.

# The top 10 Chinese cyber attacks (that we know of)

Source:http://thecable.foreignpolicy.com/posts/2010/01/22/the\_top\_10\_chinese\_cyber\_attacks\_that\_we \_know\_of

With all about the chatter about China's hacking of Google and Secretary of State Hillary Clinton's drive to deliver "consequences" to bad actors in cyberspace, it's worth noting that the problem of cyber attacks either promulgated or supported by the Chinese government is far from new.

In a previous life, your Cable guy broke a story that revealed senior military officials believe the Chinese government is supporting hackers that attack "anything and everything" in the U.S. national security infrastructure on a constant basis. And while it's difficult to prove guilt, the scale, organization, and intent of the attacks leads experts and officials alike to one sponsor: the Chinese government. The Defense Department has said that the Chinese government, in addition to employing thousands of its own hackers, manages massive teams of experts from academia and industry in "cyber militias" that act in Chinese national interests with unclear amounts of support and direction from China's People's Liberation Army (PLA).

According to SANS Institute research director Alan Paller, "The problem is 1,000 times worse than what we see." But the tip of the iceberg is still large. Here are some of the most damaging attacks on the U.S. government that have been attributed to Chinese government sponsorship or endorsement over the past few years:

#### 1) Titan Rain

In 2004, an analyst named Shawn Carpenter at Sandia National Laboratories traced the origins of a massive cyber espionage ring back to a team of government sponsored researchers in Guangdong Province in China. The hackers, code named by the FBI "Titan Rain," stole massive amounts of information from military labs, NASA, the World Bank, and others. Rather than being rewarded, Carpenter was fired and investigated after revealing his findings to the FBI, because hacking foreign computers is illegal under U.S. law. He later sued and was awarded more than \$3 million. The FBI renamed Titan Rain and classified the new name. The group is still assumed to be operating.

#### 2) State Department's East Asia Bureau

In July 2006, the State Department admitted it had become a victim of cyber hacking after an official in "East Asia" accidentally opened an email he shouldn't have. The attackers worked their way around the system, breaking into computers at U.S. embassies all over the region and then eventually penetrating systems in Washington as well.



# 286

#### 3) Offices of Rep. Frank Wolf

Wolf has been one of the most outspoken lawmakers on Chinese human rights issues, so it was of little surprise when he announced that in August 2006 that his office computers had been compromised and that he suspected the Chinese government. Wolf also reported that similar attacks had compromised the systems of several other congressmen and the office of the House Foreign Affairs Committee.

#### 4) Commerce Department

The Commerce Department's Bureau of Industry and Security had to throw away all of its computers in October 2006, paralyzing the bureau for more than a month due to targeted attacks originating from China. BIS is where export licenses for technology items to countries like China are issued.

#### 5) Naval War College

In December 2006, the Naval War College in Rhode Island had to take all of its computer systems offline for weeks following a major cyber attack. One professor at the school told his students that the Chinese had brought down the system. The Naval War College is where much military strategy against China is developed.

#### 6) Commerce Secretary Carlos Gutierrez and the 2003 blackout?

A National Journal article revealed that spying software meant to clandestinely steal personal data was found on the devices of then Commerce Secretary Carlos Gutierrez and several other officials following a trade mission to China in December 2007. That same article reported that intelligence officials traced the causes of the massive 2003 northeast blackout back to the PLA, but some analysts question the connection.

#### 7) McCain and Obama presidential campaigns

That's right, both the campaigns of then Senators Barack Obama and John McCain were completely invaded by cyber spies in August 2008. The Secret Service forced all campaign senior staff to replace their Blackberries and laptops. The hackers were looking for policy data as a way to predict the positions of the future winner. Senior campaign staffers have acknowledged that the Chinese government contacted one campaign and referred to information that could only have been gained from the theft.

#### 8) Office of Sen. Bill Nelson, D-FL

At a March 2009 hearing, Nelson revealed that his office computers had been hacked three separate times and his aide confirmed that the attacks had been traced back to China. The targets of the attacks were Nelson's foreign-policy aide, his legislative director, and a former NASA advisor.

#### 9) Ghostnet

In March, 2009, researchers' in Toronto concluded a 10-month investigation that revealed a massive cyber espionage ring they called Ghostnet that had penetrated more than 1,200 systems in 103 countries. The victims were foreign embassies, NGOs, news media institutions, foreign affairs ministries, and international organizations. Almost all Tibet-related organizations had been compromised, including the offices of the Dalai Lama. The attacks used Chinese malware and came from Beijing.

#### 10) Lockheed Martin's F-35 program

In April, 2009, the Wall Street Journal reported that China was suspected of being behind a major theft of data from Lockheed Martin's F-35 fighter program, the most advanced airplane ever designed. Multiple infiltrations of the F-35 program apparently went on for years.



# Biggest-ever series of cyber attacks uncovered

Source: http://www.reuters.com/article/2011/08/03/us-cyberattacks-idUSTRE7720HU20110803

Security experts have discovered (Aug 2011) the biggest series of cyber attacks to date, involving the infiltration of the networks of 72 organizations including the United Nations, having stolen the other team's playbook), the loss represents a massive economic threat." McAfee learned of the extent of the hacking campaign in March this year, when its



governments and companies around the world. Security company McAfee, which uncovered the intrusions, said it believed there was one "state actor" behind the attacks but declined to name it, though one security expert who has been briefed on the hacking said the evidence points to China.

The long list of victims in the five-year campaign include the governments of the United States, Taiwan, India, South Korea, Vietnam and Canada; the Association of Southeast Asian Nations (ASEAN); the International Olympic Committee (IOC); the World Anti-Doping Agency; and an array of companies, from defense contractors to high-tech enterprises.

In the case of the United Nations, the hackers broke into the computer system of its secretariat in Geneva in 2008, hid there for nearly two years, and quietly combed through reams of secret data, according to McAfee. "Even we were surprised by the enormous diversity of the victim organizations and were taken aback by the audacity of the perpetrators," McAfee's vice president of threat research, Dmitri Alperovitch, wrote in a 14page report released on Wednesday. "What is happening to all this data ... is still largely an open question. However, if even a fraction of it is used to build better competing products or beat a competitor at a key negotiation (due to researchers discovered logs of the attacks while reviewing the contents of a "command and control" server that they had discovered in 2009 as part of an investigation into security breaches at defense companies.

It dubbed the attacks "Operation Shady RAT" and said the earliest breaches date back to mid-2006, though there might have been other intrusions. (RAT stands for "remote

access tool," a type of software that hackers and security experts use to access computer networks from afar).

Some of the attacks lasted just a month, but the longest -- on the Olympic Committee of an unidentified Asian nation -- went on and off for 28 months, according to McAfee.

"Companies and government agencies are getting raped and pillaged every day. They are losing economic advantage and national secrets to unscrupulous competitors," Alperovitch told Reuters.

"This is the biggest transfer of wealth in terms of intellectual property in history," he said. "The scale at which this is occurring is really, really frightening."

#### China connection?

Alperovitch said that McAfee had notified all 72 victims of the attacks, which are under investigation by law enforcement agencies around the world. He declined to give more details.

Jim Lewis, a cyber expert with the Center for Strategic and International Studies who was briefed on the hacking discovery by McAfee, said it was very likely China was behind the campaign because some of the targets had information that would be of particular interest to Beijing. The systems of the IOC and several national Olympic Committees were breached in the runup to the 2008 Beijing Games, for example.

And China views Taiwan as a renegade province, and political issues between them remain contentious even as economic ties have strengthened in recent years. "Everything points to China. It could be the Russians, but there is more that points to China than Russia," Lewis said.

McAfee, acquired by Intel Corp this year, would not comment on whether China was responsible.

#### Stone age

Vijay Mukhi, an independent cyber-expert based in India, says some south Asian governments, including India, are highly vulnerable to hacking from China as it strives to broaden its influence and strategic interests in the region. "I'm not surprised because that's what China does, they are gradually dominating the cyberworld," he said. "I would call it child's play (for a hacker to get access to Indian government data) ... I would say we're in the stone age."

An Indian telecommunications ministry official declined to say whether he was aware of the hacking on the government.

The UN said it was aware of the report, and that it has started an investigation to ascertain if there was an intrusion.

But Hwang Mi-kyung, with leading South Korean cyber security firm Ahnlab, cautioned against assuming China was the only one involved. "I think we're beyond the stage where we should be focusing on the technical aspect of addressing individual attacks and instead we should think more in terms of what we can do policywise. For that, the involvement of Chinese government is very important," she said.

McAfee released the report to coincide with the start of the Black Hat conference in Las Vegas on Wednesday, an annual gathering of security professionals and hackers who use their skills to promote security and fight cyber crime.

In the scorching desert heat, they will meet to talk about a series of recent headline-grabbing hacks, such as on Lockheed Martin Corp, the International Monetary Fund, Citigroup Inc, Sony Corp and EMC Corp's RSA Security.

The activist groups Anonymous and Lulz Security have recently grabbed the spotlight for temporarily shutting down some high-profile websites and defacing others.

But attacks like Operation Shady RAT are far more costly and often undisclosed, as victims fear reputational damage or attention from other hackers. McAfee sees Operation Shady RAT as the tip of the iceberg.

"I am convinced that every company in every conceivable industry with significant size and valuable intellectual property and trade secrets has been compromised (or will be shortly), with the great majority of the victims rarely discovering the intrusion or its impact," Alperovitch wrote in the report.

"In fact, I divide the entire set of Fortune Global 2000 firms into two categories: those that know they've been compromised and those that don't yet know."

#### Stuxnet can morph into new threat

Source: http://www.homelandsecuritynewswire.com/dhs-officials-stuxnet-can-morph-new-threat

Government cyber-security experts warn that the Stuxnet virus, which damaged Iran's nuclear centrifuges, could morph into something even more destructive.

After the virus initially came to light last year, DHS officials began dissecting the sophisticated code to better understand it. Experts learned that the virus targets industrial control systems that regulate production in every sector ranging nearly from pharmaceuticals to nuclear power and chemical factories to water utilities.

Last Tuesday, in a joint statement before the House Energy and Commerce Subcommittee

on Oversight and Investigations, Roberta Stempfley, the acting assistant secretary with of Cyber Security the Office and Communications, and Sean McGurk, the director of the National Cybersecurity and Communications Integration Center, said, "This code can automatically enter a system, steal formula for the product being the manufactured, alter the ingredients being mixed in the product, and indicate to the operator and the operator's anti-virus software that everything is functioning normally."

Anti-virus companies and industrial control system developers have since developed

software patches to protect against the Stuxnet virus, but the two DHS officials worry that hackers could design more complex versions that can evade detection.

"Attackers could use the increasingly public information about the code to develop variants targeted at broader installations of programmable equipment in control systems," the two officials said in their written testimony.

The hearing was aimed at securing the nation's critical infrastructure from cybersecurity threats especially in light of the recent cyberattacks on major government contractors like Lockheed Martin and RSA as well as viruses like Stuxnet.

Representative Cliff Stearns (R – Florida), the chairman of the subcommittee, said, "Since September 11, our infrastructure systems have become even more automated and more reliant on information systems and computer networks to operate. This has allowed our systems to become more efficient, but it has also opened the door to cyber threats and cyber attacks."

"We must identify and protect the very systems that make our country run: energy, water, healthcare, manufacturing, and communications," he added.

# Cyber Threat Resembles Pre-9/11 Terror Threat: Black Hat

Source: http://informationweek.com/news/government/security/231300137

Today's threat of cyber attacks is analogous to that from terrorists in the mid-1990s, Cofer Black, chairman of Total Intelligence Solutions and director of the CIA's counterterrorist center on 9/11, said in a keynote at Black Hat, a UBM TechWeb event, on Wednesday.

When al Qaeda was in the rise in the mid-1990s, and even until the 9/11 attacks, Black



said, terrorist threats were not well understood and were new to the country's top decision makers. "They didn't understand it. They had no personal experience with it," he said. "The decision-makers of today are in the same boat [with cyber]. They hear it, but they don't understand it."

There are major differences in user experience among some of the top

tablets. We take a deeper look at some of the strengths and weaknesses of Apple's iOS, Android/Honeycomb and RIM's QNX operating systems.



of Defense recently said that they could carry out physical counter-strikes in respond to cyber attacks on physical infrastructure.

In the future, Black said, cyber will be a key component of all conflicts. He said that, until recently, the security world has considered the key threats for causing mass destruction to be chemical, bacteriological, radiological, or nuclear, but that cyber has to be a part of the mix from now on.

"I am here to tell you, and you can quote me on this: The Stuxnet attack is the Rubicon of our future," he said. "It was really expensive, so a nation-state had to be involved. Second, [the world of cyber] has now morphed into physical destruction of national resources. This is huge."

The challenges such attacks present are huge, Black said, pointing to questions about how to respond to cyber attacks on physical infrastructure, and noting that the Department

Another analogy with terrorist attacks, and another challenge of responding to cyber attacks, Black noted, was the difficulty of attribution. "In my world, the concept is false flags, that everybody wants to look like they're

#### Why US Will Lose a Cyber War

#### By Jeffrey Carr

Source: http://the-diplomat.com/flashpoints-blog/2011/08/10/why-us-will-lose-cyber-war/

# US defence planners are stuck with western thinking over cyberspace. They could learn something from East Asia.

There's not another nation in the world that can wage kinetic warfare as effectively as the United States, and that's probably at the heart of the reason why the United States will lose a war fought in cyberspace.

It's not because we don't have skilled cyber warriors, because we do. It's because present leadership in the Defence Department is trying to fit the round peg of cyberspace into the square hole of meat space. A perfect example of this mindset is found in the Spring 2011 edition of Strategic Studies Quarterly 'Rise of a Cybered Westphalian Age' wherein the authors write:

'First, the technology of cyberspace is manmade. It is not, as described by the early

"cyber prophets" of 1990s. the an entirely new environment which outside operates human control. like tides or gravity. Rather, as its base, the grid is a vast complex system of machines, software code and services. cables. accepted protocols for compatibility,



graphical pictures for human eyes, input/output connections, and electrical supports. It operates precisely across narrow electronic bands but with such an amalgamation of redundancies, substitutions, workarounds, and quick go-to fixes that disruptions can be handled relatively well as long as everyone wants the system to work as planned.'

In the earliest days of the Internet, otherwise known as Web 1.0 (the Read-only Web), the above was certainly true. As we moved to Web somebody else, like Iran, who has surrogate groups," he says. "That's where you are, too, and it is fraught with danger because it's an emotional time, but confusion comes up in the normal course."

2.0 (the Read-Write Web), it became less true. The more integrated our physical and virtual lives become (Web 3.0), the farther away from that definition we land. The fact that the authors of the paper still believe that cyberspace is nothing more than a manmade piece of hardware says volumes about how the domain is misunderstood at the highest levels of the Defence Department, which is obvious with the miscategorization of cyberspace as a 5th domain:

'Though the networks and systems that make up cyberspace are man-made, often privately owned, and primarily civilian in use, treating cyberspace as a domain is a critical organizing concept for DoD's (the Department of Defence)

national security missions. This allows DoD to organize, train, and equip for cyberspace as we do in air, land, maritime, and space to support national security interests.'

I've touched upon the concept of n-dimensional conflict, and I'm writing a chapter on it for the 2nd edition of Inside Cyber Warfare. In the course of

my research, I've come across the work of theoretical physicist Basarab Nicolescu who argues that cyber-space-time (a more accurate name than 'cyberspace') is both artificial and natural at the same time:

'The information that circulates in CST is every bit as material as a chair, a car, or a quantum particle. Electromagnetic waves are just as material as the earth from which the calculi were made: it is simply that their degrees of materiality are different. In modern physics.

www.cbrne-terrorism-newsletter.com

290

matter is associated with the complex relationship: substance-energy-informationspace-time. The semantic shift from material to immaterial is not merely naive, for it can lead to dangerous fantasies.'

One of Nicolescu's influences was Nobel laureate Wolfgang Pauli and Pauli, in turn, was fascinated by Carl Jung's theory of Synchronicity. In fact, Pauli and Jung spent a great deal of time together because Pauli believed that there was a relationship between Jung's acausal connecting principle and quantum physics; specifically a conundrum known as 'quantum indeterminacy.' Even though Pauli's lifetime preceded the Internet age, he wrote extensively about a unifying connecting principle that bridged mind and matter. Nicolescu references Pauli's work and calls that connecting principle cyber-spacetime.

In a kind of ironic twist, Carl Jung's theory of synchronicity has its genesis in his fascination with an ancient Chinese oracle called The Book of Changes or Yijing. It's a divinatory oracle that dates back to the Qin dynasty and teaches that the universe is composed of parts that are interconnected. The yarrow stalks used in the Yijing symbolize those parts, while the casting of them symbolizes the mystery of how the universe works (Pauli's quantum indeterminacy). Chinese emperors and generals have used this oracle since approximately 300 BC, and it may still provide a glimmer of insight into the mysterious nature of this new age of cyber-space-time and how cyber battles may be fought and won.

Unfortunately for Western nations, synchronicity has its origins in the East. Western nations have a tradition in causality, not synchronicity. And the US Defense Department is deeply grounded in traditional western thinking and practicality. The decision to call cyberspace a domain was based on organizational necessity. That's how the Defence Department is set up. It's how budgets are created and funds distributed. It's how contracts get assigned. Simply put, it's how things get done at the Pentagon. This is why the United States will lose a war fought in cyberspace. A strategic doctrine built upon a flawed vision can't yield a victory against an adversary whose knowledge of the battle space is superior to our own.

#### New Windows worm spreading by exploiting weak passwords

Source:http://www.homelandsecuritynewswire.com/new-windows-worm-spreading-exploiting-weak-passwords

A new Windows worm is spreading through company networks by exploiting weak passwords; the worm, dubbed "Morto" spreads

using RDP, or Remote Desktop Protocol. the Microsoft-made protocol for controlling one computer by connecting to it from another Microsoft (in a writeup Sunday) and Helsinki-based



security firm F-Secure say that a new Windows worm is spreading through company networks by exploiting weak passwords.

Computerworld reports that the worm, called "Morto" has been circulating since at least last week, when company administrators noticed

systems generating large numbers of unexplained connections to the Internet (see this message on the Microsoft Support Forum).

According to Microsoft, Morto is the culprit. the "Although overall numbers of computers reporting detections are low in comparison to more established malware families, the traffic it generates is noticeable," said Hil Gradascevic, a researcher with the

Microsoft Malware Protection Center (MMPC), in a Sunday blog.

Computerworld notes that Morto spreads using RDP, or Remote Desktop Protocol, the Microsoft-made protocol for controlling one computer by connecting to it from another. All

versions of Windows from XP on include client software that uses RDP to remotely access machines. The software, called Remote Desktop Connection (RDC) in XP, Vista, and Windows 7, requires a username and password to log in to a remote system.

#### Report warns U.S. unprepared for cyber attacks

Source: http://www.foxnews.com/us/2011/09/12/study-warns-us-must-develop-cyber-intelligence/

A new report warns that the United States lacks the capabilities to defend against expanding cyber threats; the report found, "The impact has increased in magnitude, and the potential for catastrophic collapse of a company has grown," yet the businesses

community has failed to understand that

A new report warns that the United States lacks the capabilities to defend against expanding cyber threats. In recent years, cyber attacks have increased in sophistication making them more dangerous and damaging than ever before, the report said. The Intelligence and National Security Alliance (INSA), a nonpartisan national security organization led by Frances Townsend, a former homeland security adviser in the Bush administration. found, "The impact has

increased in magnitude, and the potential for catastrophic collapse of a company has grown," yet the businesses community has failed to understand that.

To better defend against these attacks, INSA recommends that the United States develop a coordinated cyber security strategy that is beyond the current "patch and pray" procedures, establish cyber intelligence policies, and improve information sharing between government agencies and businesses.



In addition the report also urges the government to develop more effective cyber intelligence so officials can assess and mitigate risks.

INSA points to failed states as well as the countries that tolerate criminal cyber activity

within their borders as the primary threats to the United States. The report does not name the countries, but U.S. officials have repeatedly pointed to Russia, China, and several Eastern European countries as safe havens for cybercriminals as well as governmentsponsored attacks.

The report also points to the growing problem of a complex global supply chain for computer components that allows malicious actors slip contaminated chips into U.S. networks that make it easier for hackers to surreptitiously steal sensitive data or introduce

dangerous viruses. Much of the development of computer chips has been outsourced, and chips are now shipped all around the world before they are eventually installed in computers in the United States.

"The present situation is as dangerous as if the United States decided to outsource the design of bridges, electrical grids, and other physical infrastructure to the Soviet Union during the Cold War," INSA concluded. The full report is scheduled to be released later this month



n Connection (RDC) in VD Visto

www.cbrne-terrorism-newsletter.com

292

# Terror News

# Profile of Dr. Ayman al-Zawahiri, Osama bin Laden's Heir as Leader of Al-Qaeda<sup>1</sup>

Source: http://www.terrorism-info.org.il/malam\_multimedia/English/eng\_n/html/gj\_e008.htm



Ayman al-Zawahiri, left, sitting next to Osama bin Laden, praises those who attacked the United States on September 11, 2001 (YouTube video, April 15, 2002).

#### Overview

1. On June 16 Al-Qaeda announced that after a period of consultations, Dr. Ayman al-Zawahiri had been appointed as Osama bin Laden's heir. The announcement stressed Al-Qaeda's commitment to jihad, which was the "personal duty of every Muslim." The jihad would be waged against the various "infidels" – the United States, Israel and the Arab-Muslim rulers, "until the Resurrection."2 This study profiles Ayman al-Zawahiri, his ideology and activities, and evaluates the possible outcome of his appointment as leader of Al-Qaeda.

2. Sheikh Dr. Ayman Mohammed Rabi'a al-Zawahiri (Abu Mohammed) was born in 1951 to a wealthy family whose members held senior the positions in Egyptian religious establishment. His piety was evident from an early age, and at 14 he joined the Muslim Brotherhood. In his youth he was influenced by the ideology of Sayyid Qutb, a central figure in the Muslim Brotherhood, who developed the radical Islamic ideology from which the extremist faction of the Muslim Brotherhood sprang. He began studying medicine at the University of Cairo in 1968 and graduated with honors in 1974. He specialized in surgery at a

university in Pakistan, receiving a PhD, again graduating with honors.

3. When Sayyid Qutb was executed by Nasser in 1966 and thousands of Muslim Brotherhood activists were imprisoned, al-Zawahiri, along with a number of other young men, set up an underground cell (1966-1967) with the intention of overthrowing the Egyptian regime and establishing an Islamic government. During the 1970s, while still at school, he joined an extremist Islamic organization called the Islamic Jihad, which was behind a wave of terrorist attacks in Egypt, and became one of its most prominent operatives. In 1991 he formally became the organization's head.

4. Following the assassination of Anwar Sadat in October 1981, al-Zawahiri was arrested along with other radical Islamic operatives. He cleared of involvement the in was assassination because of lack of evidence, but convicted of membership in a terrorist organization and having weapons and explosives in his possession. He was sentenced to a term of three years in prison, which he served from 1981 to 1984. In his book Knights Under the Prophet's Banner he said that assassinating Sadat was part of 1

comprehensive program of assassinating senior figures in the Egyptian regime and using the army to take over vital broadcasting stations.

5. After his release from prison he went from Egypt to Jeddah in Saudi Arabia to practice medicine and to promote the activities of the Egyptian Islamic Jihad beyond the borders of Egypt. There he apparently met Osama bin Laden for the first time, and from Saudi Arabia he went to Pakistan and Afghanistan to wage his jihad against the Egyptian regime. While in Peshawar, Afghanistan, he founded an

organization called -Talai'i al-fath ("pioneers of conquest"), which in effect served as the operational wing of the Egyptian Islamic Jihad. He established а network of bases, training camps and headquarters, all with the support of Osama bin Laden. 6. At the beginning of the 1990s al-Zawahiri and bin Laden went to Sudan, where they set up a network of bases. During the 1990s he also set up a new network in Yemen, from which he conducted a campaign of

terrorist attacks against Egyptian targets, both inside and outside Egypt. He was also involved in an attempt to assassinate Egyptian President Hosni Mubarak and the murder of tourists in Luxor in 1997. He was apparently also involved in the attempted assassination of President Mubarak in Ethiopia in July 1995. Because of his involvement in terrorist attacks, he was sentenced to death in absentia in Egypt, April 1999.

7. Al-Zawahiri's involvement in terrorism in the 1990s did not focus only on the Egyptian arena. In the middle of the decade, instructed by bin Laden, he constructed Al-Qaeda terrorist networks in Britain and the United States, strengthened the radical Islamic militias in the Balkans, supported radical Islamic groups in Somalia and Ethiopia and aided the rebels in Chechnya. In 1996, with two other operatives, he tried to enter Chechnya and was arrested by the Russian security forces, only to be released "for lack of evidence."

8. At the beginning of 1998 al-Zawahiri and Osama bin Laden founded the International Islamic Front for Jihad against Jews and Crusaders. It was an umbrella network for Al-Qaeda, the Egyptian Islamic Jihad and various radical Islamic organizations operating in countries such as Pakistan, Bangladesh,

> Kashmir and the Philippines. Al-Zawahiri became bin Laden's deputy in the Front and second in command of Al-Qaeda. In June 2001 al-Zawahiri announced the formal union of all the organizations, whose official name is [Tanzim] Qaedat al-Jihad (the formal name of Al-Qaeda to this day).

> 9. In February 1998 Qaedat al-Jihad issued an appeal calling for the killing of Americans throughout the world, saying it was the "personal duty" of every Muslim. In practical terms, Al-Qaeda initiated a campaign of global terrorism against the United States. beginning with the terrorist attacks of the American

embassies in Kenya and Tanzania in August 1998, and culminating with the September 11, 2001 attacks.

10. Al-Zawahiri continued holding key positions in Al-Qaeda (as far as is known, he was responsible for producing anthrax spores for the organization) and became even more dominant than bin Laden in Al-Qaeda's global propaganda campaign.

#### 11. His worldview and ideology:

a) As noted, al-Zawahiri was particularly influenced by the radical Islam of Sayyid Qutb, according to which the Arab-Muslim regimes ("the internal enemy") were no less dangerous than external enemies. His ideology

أيمن الظواهرى كما عرفته

منتصر الزيات

using violence and terrorism against them, since, it claimed, they had deviated from the precepts of Islam and did not govern according to religious Muslim law (the Shari'a). He was also influenced by Dr. Abdullah Azzam, a Palestinian from northern Samaria, who became Osama bin Laden's ideological mentor. Azzam developed and institutionalized the concept of jihad as the "personal duty" of every Muslim.

b) Based on experienced gained from decades of terrorist activity, al-Zawahiri formulated his worldview of radical jihadist Islam. According to his worldview, a global jihad movement was necessary, based on a territorial infrastructure which would serve as a "hothouse" for breeding

the iihadist campaign (in a region such as Afghanistan, although al-Zawahiri would have preferred to locate the hothouse in the Arab Middle East). Young men imbued with radical Islamic ideology would be sent from the hothouse to wage a violent campaign Islam's against various enemies: the "treacherous" Arab-Muslim regimes, the superpowers (the United States, the main enemy, and Russia), other countries hostile to Islam (especially those Western in Europe), and the State of Israel, as well as Jews around the world

12. Al-Zawahiri's ideology expresses particular hostility and hatred for the State of Israel, which he regards as the spearhead of the Christian West (the "Crusaders") in the Middle East, and to the Jews in general (his ideology incorporates anti-Semitic motifs directly from The Protocols of the Elders of Zion).

13. Al-Zawahiri calls for a violent jihad against Israel as the only way to "liberate Palestine," and advocates attacking Jews around the globe. Israel was also mentioned in the AlQaeda announcement naming al-Zawahiri as its leader. In our assessment, under al-Zawahiri Al-Qaeda will increase its attempts to attack Israel. As for the Jews, al-Zawahiri has often specifically instructed Muslims to attack Jews beyond the borders of Israel, and Al-Qaeda has been and will continue to be involved in attacks against Jewish targets all over the world. At the same time, he will pursue his activities against Christians, the United States and Western countries, and against the Arab-Muslim regimes.

14. The uprisings taking place in the Arab world during the first half of 2011 are an ideological challenge for Al-Qaeda. That is because they are based, at least partially, on

> an agenda of freedom, which is completely opposed to jihadist ideology. Moreover, Al-Qaeda and the Islamists have so far not played a significant role in Al-Zawahiri them. expressed support for the overthrow of regimes of Mubarak in Egypt and Ben Ali in Tunisia, accused them of corruption and serving the interests of the United States, encouraged the Libyan "jihad fighters" (mujahideen) for their actions against Qaddafi's regime, and called for the establishment of "just Islamic regimes" in the Arab countries, where religious Islamic law (Shari'a)

would prevail. He also expressed support for the uprisings in Syria and Yemen.

# The Significance of Appointing al-Zawahiri as Al-Qaeda's Leader

15. Al-Zawahiri's appointment to the leadership of Al-Qaeda was expected, although it took several weeks instead of occurring immediately. He had the reputation of being the "brain" behind Al-Qaeda and its head ideologue,3 amassed considerable operational

# His Own Words

A Translation of the Writings of Dr. Ayman al Zawahiri



by Laura Mansfield

and organizational experience in terrorism and possibly, at various times in recent years, even the de facto head of the organization.

16. According to Al-Qaeda's bylaws written 2002, which are apparently still in force, the organization's second in command is supposed to succeed the leader (emir) should he be killed or captured without hope of release.4 Appearing in a video issued on June 8, 2011, a month after the death of bin Laden, al-Zawahiri promised the United States he would continue Osama bin Laden's path of jihad, thus positioning himself as bin Laden's heir [at that time there had not yet been an official confirmation of his appointment, which came eight days later].

17. The possible consequences of al-Zawahiri's appointment for Al-Qaeda's nature and methods are the following: Ideologically, because of his usually close cooperation with bin Laden and their mutual worldview, it is unlikely that significant changes will be made in its concept of waging a global jihad against the United States and its allies. However, it is possible that changes may occur in Al-Qaeda's order of priorities, due to al-Zawahiri's worldview, personality, Egyptian origin and personal experience.

18. Al-Zawahiri's Achilles' heel, the fact that he does not have bin Laden's charisma and his leadership is not a foregone conclusion, may influence Al-Qaeda in the future. Thus potentially, power struggles may arise over the "inheritance" of the Al-Qaeda leadership, and charismatic local commanders with their own power bases or operational terrorist experience may make demands for leadership or act independently.

19. Al-Zawahiri may give high priority to terrorist attacks against Arab-Muslim regimes he considers Western collaborators and enemies of Islam, as well as against Israel (possibly from Al-Qaeda bases in the areas on its borders, especially the Gaza Strip) and against Jewish targets around that globe. He may emphasize terrorist activity in Egypt, exploiting the collapse of the Mubarak regime, the weakening of internal security control, the legalization of the Muslim Brotherhood and its return to the forefront of the political stage; and al-Zawahiri's long experience with subversion and terrorism within Egypt. At the same time, the United States and Western countries will continue to be perceived as a prime target.

20. Organizationally, Al-Qaeda's financial capabilities may be affected because al-Zawahiri lacks bin Laden's resources. If that happens, its operational and logistic capabilities may suffer. It is also possible that there will be changes in Al-Qaeda's structure and methods, with the decentralization of various local focal points, the result of possible power struggles and al-Zawahiri's difficulties in enforcing his authority on local commanders in distant confrontation arenas.

#### Sources Used in This Study

21. This study is based on the following sources: an analysis of videos and audio cassettes issued by al-Zawahiri (many of them on YouTube): his book. Knights Under the Prophet's Banner, translated into English by Laura Mansfield (first edition); a book in Arabic about al-Zawahiri by Montasser al-Zayat, an Egyptian lawyer affiliated with the Islamic movement, called Ayman al-Zawahiri As I Knew Him; an article by Dr. Nimrod Raphaeli about al-Zawahiri's life and activities (published 2002); books and reports, including those issued by research institutes dealing with global terrorism; Islamic Internet forums; interviews with experts on Al-Qaeda and the global jihad which appeared in the global media and information based on security sources.

22. The study is divided into the following sections:

1) Biography

2) Islamists who influenced al-Zawahiri's ideology

3) Overview of al-Zawahiri's ideology

4) Al-Zawahiri's position on the United States

5) Al-Zawahiri's position on Western Europe

6) Al-Zawahiri's position on the State of Israel and the Jewish people

7) Al-Zawahiri's position on the Arab and Muslim regimes

8) Al-Zawahiri's position on the Muslim Brotherhood

9) Al-Zawahiri's criticism of the Hamas movement

10) Al-Zawahiri's centrality in the battle for hearts and minds

11) Initial evaluation of the significance of al-Zawahiri's appointment as Al-Qaeda leader

1 The study is available in Hebrew, and the full English translation will shortly be posted on the ITIC website. 2 The Al-Fajr Media Center quoted by Al-Arabiya TV, June 16, 2011. The announcement was issued by other jihadist sites as well.

3 Laura Mansfield, His Own Words, The Translation of the Writings of Dr. Ayman al Zawahiri (USA: TLG, 2006), p. 13;http://www.csmonitor.com/2001/1031/p6s1-wosc.html

http://www.thefirstpost.co.uk/78454,news-comment,news-politics,hunt-is-on-for-ayman-al-zawahiri-brains-behind-osama-bin-laden

4 http://www.ctc.usma.edu/wp-content/uploads/2010/08/AFGP-2002-600048-Trans.pdf, April 18, 2002.

# Al-Qaeda's Zawahiri, Bigger Threat Than Osama?

#### By Raymond Ibrahim

Source: http://www.meforum.org/2971/al-qaeda-zawahiri-bigger-threat-than-osama



Zawahiri, preaching from an Egyptian prison cell 30 years ago

Now that Ayman Zawahiri has assumed leadership of al-Qaeda, it is important to end the widespread perception that he is a dour intellectual who is disconnected from young, would-be jihadists. The fact is, Zawahiri is a wily, dangerous and imposing leader who should be considered no less of a threat—and perhaps even more so—than his predecessor.

Like Osama bin Laden, the Egyptian Zawahiri has jihadi bona fides and served in the Afghan war against the Soviets, primarily as a physician. Moreover, Zawahiri's imprisonment and torture after the assassination

of Anwar Sadat by Islamic Jihad, which he headed, seems to have hardened him more than bin Laden. From his prison cell he memorably delivered a passionate speech—in English no less. Seeing a video of it dispels any notion that he is an uncharismatic leader.

Even so, focusing on charisma is misleading. Although charisma has its place in leadership positions in Islam, knowledge demands greater authority. After all, the guardians of Islam are called ulema—literally, "those who know." And compared with bin Laden, Zawahiri is certainly more knowledgeable. He has long been seen as the group's theoretician, and thus commands great respect.

Because I have always believed that Zawahiri was key to understanding al-Qaeda's worldview, when I compiled The Al Qaeda Reader in 2007, I included more of his writings than bin Laden's, specifically Zawahiri's three long treatises.

#### **Feign Friendship**

According to his own words, Zawahiri insists that Muslims must always harbor enmity for "infidels," or non-Muslims, particularly Jews and Christians. He advocates that Muslims feign friendship with infidels whenever it is advantageous: "We grin to the faces of some peoples, while our hearts curse them." He is a great proponent and articulator of the "superiority" of martyrdom/suicide operations.

and despises democracy because it creates "equality between the citizenry," allows



Al Qaeda's longtime theoretician and staunch advocate of jihad takes the helm

freedom of religion and abolishes "man's domination over woman."

Zawahiri's views may be best summed up by the following passage:

Warfare against infidels, loyalty to the believers, and jihad in the path of Allah: Such is a course of action that all who are vigilant for the triumph of Islam should vie in, giving and sacrificing in the cause of liberating the lands of the Muslims, making Islam supreme in its own land, and then spreading it around the world.

#### **Relentless Dedication**

Indeed, what makes Zawahiri so dangerous is his harsh and relentless dedication to jihad. Although many Islamist organizations have learned that violence isn't the best vehicle to power, Zawahiri has a long history of being a staunch upholder of the popular jihadist slogan "Jihad and the rifle alone: no negotiations, no conferences and no dialogues." He wrote a long book in the early 1990s, Al Hisad Al Murr ("The Bitter Harvest"), condemning Egypt's Muslim Brotherhood for taking the nonviolent course to power and actually participating in elections. It's worth noting, in retrospect, that the Brotherhood's approach has been more successful at achieving political influence.

Likewise, Zawahiri is primarily responsible for redirecting the jihadists' terror attacks from Middle East targets to the U.S. in order to foment a mass conflagration between the West and Islamists—an all or nothing strategy.

#### Would-be Jihadists

Will his severity turn off aspiring jihadists, as some analysts suggest? Perhaps. But it will make those who remain that much more committed and lethal. Moreover, numbers don't matter much when it comes to engaging in terrorism: the Sept. 11 attacks were committed by 19 jihadists.

Finally, when it comes to questioning the popularity, charisma or even efficacy of Zawahiri, al-Qaeda's new leader himself once made a relevant point. Asked about the status of bin Laden and other jihadists, Zawahiri waxed philosophically:

Jihad in the path of Allah is greater than any individual or organization. It is a struggle between truth and falsehood, until Allah Almighty inherits the Earth and those who live in it. Mullah Muhammad Omar and Sheikh Osama bin Laden—may Allah protect them from all evil—are merely two soldiers of Islam in the journey of jihad, while the struggle between truth (Islam) and falsehood (non-Islam) transcends time.

As independent jihadists increasingly take action into their own hands—whether the would-be shoe bomber and Christmas bomber, the Madrid and London bombers, or Nidal Hasan and the Fort Hood army base attack we must acknowledge that the doctrine of jihad, the idea itself, is more dangerous than the jihadists who come and go, including bin Laden and Zawahiri himself.

Raymond Ibrahim is associate director of the Middle East Forum, editor/translator of The Al Qaeda Reader, and author of the al-Qaeda entry for the World Almanac of Islamism. The opinions expressed are his own.



298

# Cash-Strapped AI Qaeda Turns to Kidnapping and Ransoms to Pay Operational Costs

Source:http://www.foxnews.com/world/2011/06/19/turn-to-kidnapping-showed-bin-ladens-interest/#ixzz 1Pq89HK98



2011 on a website affiliated with the network.

Pressured by increased scrutiny of terrorist money sources and strikes aimed at its financiers, Al Qaeda's core organization in Pakistan has turned to kidnapping for ransom to offset dwindling cash reserves, according to U.S. officials and information in files retrieved from Usama bin Laden's compound.

Bin Laden's interest in kidnapping as a cashraiser bolsters accounts that the financial squeeze has staggered Al Qaeda, forcing it to search for alternative funding sources. Officials would not detail Al Qaeda's role in specific crimes, but the group's affiliates have targeted diplomats, tourists and merchants.

His awareness of Al Qaeda's growing use of kidnapping is evidence that even in isolation behind high walls in Abbottabad, Pakistan, bin Laden kept tabs on how his network moved its money. The Al Qaeda founder was killed last month by U.S. Navy SEALs.

"There are clearly times for them when money is tight," said Rep. C.A. Dutch Ruppersberger of Maryland, the top Democrat on the House Intelligence Committee. "We've seen that their donors have been less dependable and we're seeing them turning more to kidnapping as a way of keeping the money coming in."

Experts from the CIA's National Counterterrorism Center, the Treasury Department and the FBI and military are trying to learn more from the recovered files about AI Qaeda's money sources and the impact of bin Laden's death on the group's financial future. They hope to identify important AI Qaeda In this 1998 file photo made available Friday, March 19, 2004, Ayman al-Zawahri, left, poses for a photograph with Osama bin Laden, right, in Khost, Afghanistan. Al-Qaida has selected its longtime No. 2, Ayman al-Zawahri, to succeed Osama bin Laden following last month's U.S. commando raid that killed the terror leader, according to a statement posted Thursday, June 16,

donors, especially wealthy Persian Gulf figures who dealt with bin Laden dating to his work with Afghan fighters in the campaign against Soviet occupiers in the late 1980s.

The Treasury Department's acting undersecretary for terrorism and financial intelligence, David Cohen, said U.S. efforts are focused on disrupting Al Qaeda's cash flow from donors, fundraisers and facilitators. "Al Qaeda's supporters ought to be wondering if their identities have been revealed," Cohen said.

Analysts are examining lists of numbers found in bin Laden's files, hoping to find bank accounts, credit cards or ledgers depicting the financial underpinnings of network known to demand strict accounting from its operatives.

Al Qaeda's leadership inside Pakistan rarely championed kidnappings publicly and was not known previously to widely support its use as a funding source. The group historically relied on donations through a pipeline of couriers and money-changing operations. At the time of the Sept. 11 attacks, the network took in as much as \$30 million annually, but that money flow has tightened. Ruppersberger said.

CIA drone attacks, combined with economic penalties by the U.S. and its allies, have cut into that stream. At the same time, Al Qaeda affiliates have shown that abductions could rake in millions of dollars. As a result, attitudes about ransom operations inside the core group changed.

"That kind of money could go a long wa

sustaining a terrorist organization," said Scott Helfstein, director of research at the U.S. Military Academy's Combating Terrorism Center.

A U.S. official familiar with the review of bin Laden's files cautioned that the kidnapping-forransom material found in the seized files was outweighed by bin Laden's more copious notes on terrorist plots and long-range planning.

The official, who insisted on anonymity to discuss the continuing review of classified files, would not elaborate on bin Laden's interest in kidnapping or the precise role Al Qaeda's core played in any operations.

The official said the material is consistent with other evidence showing that AI Qaeda had turned to abductions within the past two years as money from sympathetic donors dried up and that the group resorted to "basic criminal tactics" to compensate. "People paid up, helping the terrorist group reline its coffers," the official said.

Al Qaeda in the Islamic Maghreb, the offshoot in North Africa, long has used kidnapping as a terrorist tool and a major funding source. Canadian diplomats, Italian tourists and Algerian merchants have been abducted; some ransoms have approached \$2 million per hostage.

The ransoms have totaled more than \$80 million for this branch since 2008, according to Matthieu Guidere, a former French military counterterrorism trainer.

The terrorist group's affiliate in Yemen, Al Qaeda in the Arab Peninsula, and its affiliates in Iraq, Pakistan and Afghanistan, have used kidnapping for ransom, too.

Figures from the National Counterterrorism Center show that 1,264 hostages were taken in Pakistan in 2008, compared with 3,366 in 2009. Pakistanis were the usual victims. Foreign hostages included a Chinese engineer, a Polish oil worker and an American, John Solecki, who worked for the U.N. refugee agency and was released after two months in captivity.

A similar wave plagued Afghanistan from 2008 to 2009 as the number of hostages taken climbed from 584 to 2,088. Four Americans were targeted, including New York Times reporter David Rohde, later released by militant captors.

Officials in Pakistan and Afghanistan say criminal gangs account for many ransom plots,

though they are known to work with militant nodes like the Pakistani Taliban.

Citing the recent kidnapping of a European journalist in Afghanistan, a security consultant in Kabul said hostages are sometimes sold or traded to militants. Insurgents also can levy "taxes" on groups transporting hostages through their turf, said the consultant, who insisted on anonymity to discuss the handling of sensitive abduction cases.

Bin Laden justified the use of kidnapping in an audio message sent last October, but solely as an instrument of vengeance. He said the abduction of five French nationals by the North African affiliate was a reaction to that country's ban on Muslim veils and support for the war in Afghanistan. "It is a simple and clear equation," bin Laden said. "As you kill, you will be killed. As you capture, you will be captured."

Al Qaeda for years relied primarily on donations as its main source of income, using its cash stream mostly for sustenance, including training, weapons, pay for operatives and their families and money for bribes and hideouts, officials said.

Terrorist plots rarely require large amounts of cash. The Sept. 11 attacks cost an estimated \$500,000, but tens of thousands of dollars in unspent funds were sent back by the hijackers to Al Qaeda accounts. Last year, Yemeni operatives bragged that their failed attempt to ship package bombs on two airlines cost a paltry \$4,500.

Bin Laden styled Al Qaeda's network's financial operation similarly to an international corporation. A financial wing oversaw finances, headed by skilled money men who monitored the books and primed streams of donated cash. Donations were ferried from militant clerics, charities and social service organizations and money-changing hawalas in the Gulf and central Asia that made tracing the money pipelines almost impossible.

Much of the group's heavy funding is believed to originate from wealthy Gulf donors who either knew bin Laden from past dealings or viewed him as an inspiration. Some dealt with him in his days as a logistics commander and fundraiser for the mujahedeen in Afghanistan. Others were royals and merchants who reportedly met him during on hunting expeditions in Afghanistan in the late 1990s, said Michael Scheuer, the former head of the CIA unit that tracked bin Laden.

Scheuer said bin Laden's death probably would mean only a temporary setback to donors who reflexively give in support of Al Qaeda's brand of jihad. But Cohen and others insist that bin Laden's death will cause lasting damage. Ayman al-Zawahri, the Al Qaeda second-incommand who was elevated to bin Laden's leadership post Thursday, according to a communique from the group, does not approach bin Laden either in donor contacts or quixotic sway, they said.

"Bin Laden was a symbolic and galvanizing figure for Al Qaeda's fundraising efforts, and Al Qaeda's donor base will likely be less willing to contribute to an Al Qaeda that has lost its founder, not knowing who is in charge or how their money might be used," Cohen said.

The Treasury Department's terrorist finance unit and allies in the U.N. and other nations have cut into Al-Qaeda's money pipeline by adding more than 500 individuals to a list whose assets should be frozen, Ruppersberger said. Last month, the U.S. Office of Foreign Asset Controls reported it had frozen a total of \$13.5 million in Al Qaeda funds since first targeting bin Laden in 1998.

Stuart Levey, the department's former top official on terrorist finance, described that effort as a success. But he said freezing the assets of terrorists won't work alone in the long term and needs to be augmented by criminal prosecutions and penalties aimed at their donors and supporters.

### **Somali Pirates Turn Violent**

Source: http://allafrica.com/stories/201106200192.html

Over 4,000 international seafarers were violently attacked by Somali pirates last year, says a new report, signaling the rising human



cost of piracy.

The Human Cost of Somali Piracy report states that seafarers captured by Somali pirates have faced beatings, been used as human shields The CIA's ramped-up program of pilotless drone aircraft over Pakistan also took a toll on the group's internal financiers. A year ago, a drone missile attack killed Mustafa al-Yazid, al-Qaida's third in command and a critical overseer who managed the bank accounts used to launch the Sept. 11 attacks. Other operatives with financial duties have also been targeted, officials said.

"Al Qaeda became sensitive to the risks that their financial system posed to their security," Levey said. "They were under real financial stress. We knew about that stress from their pleas for more money and from the fact that they passed up some (plot) opportunities."

The situation grew so dire, Levey said, that some operatives had to pay their own room and board, training and weapons. In one instance in 2008, Saudi authorities seized memory cards from the cell phones of arrested militant suspects that contained an audio message from al-Zawahri.

The man who succeeded bin Laden was pleading for donations.

and undergone other forms of torture over the past year.

The findings indicate that in the course of 2010, some 4,185 seafarers were attacked with firearms and rocket propelled grenades, 1,090 seafarers were taken hostage and 516 seafarers were used as human shields.

However, despite the violent nature of these crimes, the new study says the human cost of piracy is still under-reported and misunderstood. "There is very little reporting of the personal violence against seafarers in the waters off Somalia," says Kaija Hurlburt, the lead researcher.

#### New methods of torture



Per Gullestrup, the C.E.O. of a shipping company, the Clipper Group said, "Somali piracy has a tendency to be discussed in economic terms, but the real issue is the untold misery and trauma imposed on our colleagues at sea and their relatives by the criminals."

The report said seafarers were sometimes locked in freezers, hung from ships' masts or meat hooks or had their genitals attached to electric wires. Pirates also sometimes called seafarers' families from their mobile phones, then beat them in their families' hearing -- a tactic to increase pressure on ship owners to pay ransoms.

The new tactics break a previous code of conduct, that had kept violence to a minimum. This year has seen the first deliberate murders of hostages off Somalia - four American tourists in February and two crew members from the Beluga Nomination in January.

The pirates' change of tactics reflects the shift of activity away from the relatively easily monitored Gulf of Aden to attacks off the East African coast and in the Indian Ocean.

The tactical shift has seen pirates capturing merchant vessels and forcing their crew to let their ships be used as floating bases for attacks.

Pirates typically deter international naval forces' efforts to intercept the mother ships by parading captive seafarers on deck with guns held to their heads.

### Improved tracking system being developed for firefighters

Source: http://www.gizmag.com/firefighter-tracking-system/18969/

Even though firefighting is one of the most dangerous jobs in the world, firefighters still



communicate using analog radio signals, that can be blocked by concrete walls. This means that, upon venturing into a burning building, a firefighter might have no way of letting their commander know their present location - a situation that could prove deadly, if they ended up trapped or injured. In order to address the situation, the U.S. Department of Homeland Security's Science and Technology Directorate has created a new three-part system that lets fire crews keep track of the location and wellbeing of every member of their team, all the time. The first part of the system is a paperback book-sized tracking device known as the Geospatial Location

The WISPER routers (top left), the WISPER dispenser (middle) and base station modules (bottom) are all part of the new firefighter tracking system (Image: Department of Homeland Security)

Accountability and Navigation System for Emergency Responders (GLANSER). Using its microwave radio, lightweight battery and various navigation devices, GLANSER sends and receives signals to and from a small base station module, which is plugged into a laptop located back at the fire truck. On the laptop's screen, a graphic display constantly indicates the firefighter's location within the building, no matter where they go.

Besides GLANSER, firefighters would also wear a Physiological Health Assessment System for Emergency Responders (PHASER). The PHASER monitors body temperature, blood pressure, and pulse, and relays these parameters back to the base station. If the firefighter were to pass out, the PHASER output would indicate as much. Using

It sounds good so far, although in order to remain portable, the transmitters for the two devices are quite small - potentially too small, in fact, to generate a signal that can penetrate walls. That's where the Wireless Intelligent Sensor Platform for Emergency Responders (WISPER) routers come in.

Each disposable WISPER unit measures one square inch by half an inch thick (6.45 sq.cm. x 1.27 cm.), is waterproof, and heat resistant up to 500F (260C). It contains a two-way digital radio, antenna, and 3-volt lithium battery. Every firefighter would wear a belt-mounted waterproof canister, that contained five of the units.

As soon they stepped behind a concrete wall or otherwise went out of GLANSER contact, the base station would instruct the canister to automatically drop a WISPER router. It would continue dropping them periodically, as long as the firefighter was out of contact. The dropped units would form a network, each relaying the GLANSER and PHASER signals, until they reached back to the base station. Even if one of the units got kicked or hosed out of place, the network would be able to reconfigure itself. In order to get the most life out of each unit's tiny battery, WISPER utilizes the low-power Zigbee communications protocol. At no more than 100 kilobits per second, it's over 99 percent slower than Wi-Fi. That may be slow, but still fast enough to transmit the basic data required.

While GLANSER and PHASER are already existing products, Homeland Security is now trying to find a company interested in manufacturing the WISPER routers. Once production is under way, the entire system will be tested for performance and consistency.

### The al-Qaeda Crescent in Yemen

#### **By Daniel Green**

Source: http://www.washingtoninstitute.org/templateC05.php?CID=3374

The key battle with al-Qaeda in Yemen is in the countryside, where the U.S. government is paying too little attention.

The June 22 jailbreak of dozens of al-Qaedalinked prisoners in southern Yemen's Hadramawt province is the latest evidence that the main battle with the group has been taking place in the countryside. Although conflicts in the capital -- such as the ongoing faceoff between supporters of President Ali Abdullah Saleh and members of the Hashid tribal confederation -- will affect Yemen's future course as a nation, efforts to control the provinces more directly affect U.S. national security interests.

Poor Government Control Benefits al-Qaeda Even before the current unrest in Sana'a, the Yemeni regime was never able to attain full control of the country beyond the major cities and provincial capitals. Large areas of the countryside lack government security oversight, economic development, and other services. In many of these areas, a robust tribal government system with extended kinship groups has effectively assumed responsibility for local governance. Tribal sheiks are often granted state patronage, including direct monetary payments and quasi-legal authority in the regions they control. The regime has also used its security forces to sanction tribal groups and punish individual leaders through incarceration or direct military operations.

Currently, however, many security personnel are preoccupied with either regime survival or regime change in Sana'a, creating a security vacuum in the countryside. The government's mechanisms of patronage and control have also broken down, allowing al-Qaeda in the Arabian Peninsula (AQAP) and tribal elements to assert themselves and expand their power. On May 29, for example, more than two hundred alleged AQAP members overran the town of Zinjibar, the capital of Abyan province in southern Yemen. This followed a similar operation in the same area, where supposed AQAP members seized a munitions factory in the town of Jaar on March 27.

In addition to these widely noted episodes, the past year has seen numerous smaller-scale killings, thefts, and assassinations by AQAP. These incidents have contributed to a general sense of lawlessness and may indicate that the group is planning attacks on foreign targets as it raises money for future operations,

intimidates security forces, and weakens local

government.

#### War in the Provinces

AQAP's activities are largely concentrated in five provinces in central and eastern Yemen, located along the old border between north and south Yemen and stretching from the country's northern border with Saudi Arabia to the Gulf of Aden in the south:

- Marib. Located next to the capital, this province sits astride the Incense Road, one of the main arteries out of Sana'a. It also contains one of Yemen's three main oil fields and a number of archeological sites visited regularly by tourists. An oil and gas pipeline originates in Marib and flows west until it reaches al-Salif, one of five Yemeni ports configured to handle hydrocarbon shipments. In 2006, AQAP launched an unsuccessful attack in Marib and Hadramawt in which four suicide car bombs were destroyed by security forces before they could harm the facilities. And in May 2010, an alleged U.S. strike against AQAP killed the deputy governor of Marib, which led to riots in the region and deeply alienated the local population from the government. The two largest tribes in the area are the Murab and the Abida.
- Shabwa. Similar to Marib, this province contains a number of oil and gas fields and has pipelines flowing south to the ports of Bir Ali and Balhaf. The Incense Road passes through this area as well. Shabwa is the ancestral home of al-Qaeda leader Anwar al-Awlaki, a key recruiter who participates in some operational planning. The al-Awlaki and al-Dhiyayb are the largest tribes in the area.
- ☑ Hadramawt. This province, located directly in the middle of Yemen, contains a number of oil fields and a pipeline that flows south to the port of al-Shihr. It also has the longest border with Saudi Arabia and, together with al-Jawf, serves as a key infiltration route for AQAP members, weapons, explosives, and money. Al-Qaeda's 2002 attack on the French oil tanker Limburg, in which a bomb-laden boat severely damaged the ship, was launched from the province's al-Mukalla port. AQAP has also killed a number of tourists in Hadramawt, including two Belgians in 2008 and four South Koreans in 2009. Moreover, the previously mentioned June 22 prison break occurred in al-Mukalla. The al-Tamim and al-Kinda are the largest tribes in the area.
- Al-Jawf. This province borders Saudi Arabia as well as the Yemeni governorate of Sadah, the site of the Houthi rebellion for the past several years. Al-Jawf has also experienced AQAP violence. In November 2010, a car bomb killed more than a dozen Shiites, including a local councilman. The attack indicated a sectarian tinge to AQAP's strategy in Yemen and is consistent with the group's January 2011 proclamation of "holy war" against Houthi-led northern Shiite rebels. The Dhaw Husayn and Baqil are the largest tribes in the area.
- Abyan. This province is located next to Aden, the former capital of South Yemen, and borders the Arabian Sea. As mentioned previously, it was the site of the March 27 and May 29 AQAP attacks on Jaar and Zinjibar, respectively. The al-Yafi and the al-Fadhli are the largest tribes in the area.

#### Focus U.S. Efforts on the Countryside

Much like AQAP, the U.S. approach must be decentralized, locally based, long-term, and holistic, blending military and civil approaches. Saleh has typically been the greatest impediment to an expanded U.S. presence in the countryside. Yet with the president convalescing in Saudi Arabia and Yemen's political factions in a stalemate, now is the time to offer Sana'a an expanded aid package to help the government stabilize the provinces.

Specifically, Washington should propose a more robust training program for Yemen's security services, concentrating on both its conventional forces and counterterrorism units. In particular, U.S. trainers should be embedded with Yemeni units deployed in the provinces. Government forces could then benefit directly from U.S. training and equipment as they confront AQAP in the countryside. Additionally, Washington's understanding of provincial dynamics would improve.

Once this security initiative is underway, the United States could evaluate the practical aspects of decentralizing its governance and development programs, moving some of them from the capital to the countryside in partnership with provincial governors. This approach would bolster local governance and mitigate some of the underlying grievances that AQAP exploits to increase its support.

Washington should also consider a dedicated effort to map Yemen's human terrain and gain a better understanding of local communities, which would in turn help in the effort against AQAP. Specifically, the State Department, United States Agency for International Development, and the U.S. military should extend the tours of selected personnel at the U.S. embassy in Sana'a in order to facilitate a deeper understanding of the local situation. The United States should also develop a "Yemen Hands" initiative similar to the "Afghan Hands" program, wherein U.S. personnel work in the country for a number of years. These approaches would also even out the continuity problems that result from constant personnel rotations.

Although any U.S. strategy for Yemen will be difficult to implement, it will be harder if little is known about the country outside the major cities. Only through a better understanding of local dynamics in the provinces will U.S. policymakers be able to make the crucial

decisions needed to defeat AQAP and thwart any new attacks it may be planning on the United States.

**Daniel Green**, a Soref fellow at The Washington Institute, has served with the U.S. Navy and State Department in Afghanistan and a tour with the U.S. Navy in Iraq. He is currently working on a province-by-province examination of AQAP operations in Yemen.

# Checkbook Jihad

#### By Matthew Levitt

Source: http://www.washingtoninstitute.org/templateC06.php?CID=1625

Terrorist financiers must be under tremendous stress since news broke that U.S. Navy SEALs killed Osama bin Laden and seized hard drives and other electronic media from his safe house. Intelligence analysts and document exploitation ("Doc X") specialists are reportedly already sifting through this intelligence treasure trove and have found evidence of notional al Qaeda plots, including aspirational plans to attack the U.S. train system, and more. In all likelihood, the files will include clues pointing to bin Laden's money trail as well.

This puts people like Abd al-Hamid al-Mujil in an uncomfortable position. Described by fellow jihadists as the "million-dollar man" for his successful fundraising on behalf of al Qaeda and other jihadi groups, Mujil directed the office of the International Islamic Relief Organization (IIRO), a charity in the Eastern Province of Saudi Arabia. Both he and the IIRO office he headed were designated as terrorist entities by the U.S. Treasury Department in 2006.

But even if being "named and shamed" forced Mujil out of the terror-finance business, there are many others just like him. Just this week, David Cohen, the head of the Treasury Department's Terrorism and Financial Intelligence branch, told CNN that major donors from the Gulf states remain the key sources of funding for the al Qaeda core. There are no doubt dozens of radical funders now worrying that their names, bank accounts, or addresses will comes up in bin Laden's spreadsheets -- or "pocket litter" -- and for good reason.

It would not be the first time authorities have recovered revealing documents about al Qaeda's finances in a raid. In March 2002, Bosnian authorities raided the Sarajevo offices of the Benevolence International Foundation, a charity designated by the Treasury Department as an al Qaeda front. Among the material found on the seized computers was an al Qaeda memorandum from 1988 or 1989 listing 20 Saudi financial backers described by bin Laden as the "Golden Chain," so named because they were a reliable source of funding for his organization. According to the 9/11 Commission report, the Golden Chain was put together mainly by bin Laden's financial backers in Saudi Arabia and other Gulf states. But even if the files seized in bin Laden's Abbottabad safe house do not include explicit references to the next "million-dollar man" or "golden chain," they will likely contain information that could help expose the money trail sustaining the al Qaeda core. First, they may point to who covered bin Laden's personal expenses, which could have added up quickly. Think of the 500 euros sown into his clothes, the costs of feeding his 18-person entourage. the salaries of his bodyguards and couriers, the expense of building and renovating his compound, and the cash that may have been needed to bribe Pakistani authorities not to look too closely at his fortified three-story ville

The files may even reveal information about the current balance sheets of al Qaeda, which, as of October 2009, was said to be "in its weakest financial condition in several years." Even then, though, U.S. authorities were guick to add they were not "taking any victory laps," because there were still likely new donors willing to step in. At the time, Cohen warned that the international community's success in disrupting al Qaeda's finances might only be temporary, because "we have not vet dissuaded nearly enough donors from wanting to give in the first place." News of the Abbottabad raid alone may dissuade many of those donors in the near term, and the intelligence windfall from the raid may lead to more tangible disruptions of some donor channels. That could place the al Qaeda core under still further financial strain, but it would have little if any impact on the funding of key al Qaeda franchises such as al Qaeda in the Arabian Peninsula (AQAP), affiliated groups like Lashkar-e-Taiba, foreign-directed al Qaeda networks like those recently arrested in Germany, or the homegrown violent extremists like Maj. Nidal Hassan, who present the most immediate terrorist threats to the United States and its allies.

Whereas al Qaeda directly funded and controlled operations from its base in Afghanistan before the 9/11 attacks, today al Qaeda franchises and homegrown extremists are self-financed. We know that al Qaeda provided funding for the East Africa embassy bombings in 1998, the 2000 attack on the USS Cole in Yemen, and the 2001 World Trade Center attacks. Even after 9/11, al Qaeda continued to provide money for operations, such as the \$20,000 it furnished for the 2002 Bali bombings.

The terrorist threat is far more decentralized today, and al Qaeda's central command is not funding operations as it once did. To help finance the Bali bombings, Jemaah Islamiyah operatives had to resort to robbing jewelry stores because the al Qaeda core's contribution was not enough to foot the bill. Al Qaeda in the Islamic Maghreb (AQIM), the group's North African branch, raises significant funds through kidnapping and other types of organized crime. AQAP, now based in Yemen, has worked hard to develop its own network of major donors. For example, in September 2009, Saudi security forces found a video clip of AQAP leader and former Guantanamo detainee Saeed al-Shihri making a pitch for money to help "jihad to keep going," calling the need for funding "the core of life and the core jihad."

Left to their own devices, budding terrorist cells have resorted to criminal activity to raise funds for attacks or have used personal funds or government welfare benefits. Some of these cells, such as the terrorists who carried out the July 7, 2005, attacks on the transportation system in London, may have connections to al Qaeda's senior leadership but are independently and locally funded. In that case, while several members of the cell traveled to Pakistan for training and met up with al Qaeda. they were on their own when it came to the funding for the attack. One cell member provided the majority of the money, defaulting on a 10,000-pound personal loan and overdrawing from his multiple bank accounts. The cell also obtained funding through credit card fraud. In the end, British investigators found "no evidence of external sources of income" and stressed that the group raised the necessary funds by "methods that would be extremely difficult to identify as related to terrorism or other serious criminality." The cell that executed the devastating 2004 Madrid train bombing is another good example, partially financing the attack by selling hashish. A rare exception to this new pattern was the 2007 "Dagger" case in Copenhagen, in which the alleged perpetrator, Hamad Khurshid, reportedly received \$5,000 from al Qaeda core to conduct a bombing attack in Copenhagen. Increasingly, however, terrorism watchers see the money going the other way. In Spain, for example, authorities have seen Pakistani jihadists not only finance their local activities through petty crime, such as money laundering and credit card fraud, but also send millions of dollars back home -- some of which, it is suspected, finances extremist groups there. In Singapore, a self-radicalized cell leader collected contributions from fellow cell

to support violent causes abroad. In other cases, terrorist recruits are often being asked to bring funds with them to cover their expenses. For example, in January 2008, five members of a Bahrain-based cell were convicted of terrorist activities, including receiving explosives and weapons training, engaging in terrorism overseas, and financing terrorism. According to Bahraini officials, one of

members with the intent of sending the money

306

the individuals acknowledged having traveled to Afghanistan to engage in combat against coalition forces, and several members of the cell traveled from the kingdom to Afghanistan via Iran. Two of the suspects admitted bringing funds to cover their expenses (one cell member provided 3,000 euros and 1,000 dinars, while a second gave thousands of dinars to his handler). In another case in December 2008, Belgian and French counterterrorism authorities arrested 14 individuals with ties to core al Qaeda, some of whom had visited Pakistan's tribal areas and had been instructed to bring 2,400 euros with them to pay their travel and training costs.

At times, al Qaeda has explicitly asked its affiliates for financial support. In 2005, bin Laden's deputy, Ayman al-Zawahiri, sent a letter to Abu Musab al-Zarqawi, then the head of al Qaeda in Iraq. In the letter, which was intercepted by the U.S. government and subsequently declassified, Zawahiri asked Zarqawi for 100,000 (without specifying a currency), noting that "many lines [of support] had been cut off."

More recently, al Qaeda has received assistance from Lashkar e-Taiba (LeT), its powerful and dangerous affiliate in South Asia. In July 2009, the U.S. Treasury Department designated Arif Qasmani, whom it described as the "chief coordinator" for the group's dealings with other terrorist organizations. According to Treasury, Qasmani has provided a wide variety of financial and other support to al Qaeda since 2001, including facilitating al Qaeda members' travel and providing supplies and weapons. In exchange, al Qaeda provided Qasmani with operatives that helped LeT carry out the 2006 train bombing in Mumbai, India, and the 2007 attack on the Samjhauta Express in Panipat, India.

The Abbottabad files may help analysts better understand the current nature of the financial relationship, if any, between al Qaeda core and its regional franchises. And beyond the files themselves, bin Laden's killing may also have an impact. For example, if fissures break out between Zawahiri and other al Qaeda leaders, freelance fundraisers who have raised funds for both the al Qaeda core and affiliated groups could shift away from Zawahiri and toward groups like AQAP, which U.S. authorities unanimously describe as the greatest terrorist threat to the United States today. Consider someone like Mubarak al-Bathali, a Kuwaiti designated a terrorist financier by the United States in December 2006 and by the United Nations in January 2008. According to the Treasury Department, Bathali raised funds in Kuwait for a range of terrorist organizations -including al Qaeda, Ansar al-Islam, and Lashkar-e-Taiba.

Al Qaeda's late leader may still bring in the big bucks for a while, as his old videos get passed around like "greatest hits." But while bin Laden served as a unifying figurehead, Zawahiri is a divisive figure whose presumed accession to the top spot in the al Qaeda hierarchy may well rekindle simmering tensions between the organization's Egyptian and Yemeni factions. Moreover, the al Qaeda core -- lacking the power of the purse and stripped of its founding icon -- may find itself less able to exert authority over its self-financed franchises. The death of bin Laden does not mark the end of al Qaeda, but it may mark the beginning of the end of its core -- and the rise of al Qaeda affiliates and homegrown violent extremists.

*Matthew Levitt* is director of the Stein Program on Counterterrorism and Intelligence at The Washington Institute.

# The United States and the Policy of Targeted Killing

By Schweitzer, Yoram and Yogev, Einav

Source: http://www.inss.org.il/publications.php?cat=21&incat=&read=5282

United States policy on targeted killings in the war on terror made headlines with the May 2011 raid by the Navy SEALs in the heart of Pakistan that killed al-Qaeda leader Osama Bin Laden. The SEALs were previously involved in commando actions of this type against other senior al-Qaeda figures. In September 2009, a SEALs team killed Saleh Ali Saleh Nabhan, an al-Qaeda commander in Somalia, in a land operation that was carried out in Somalia. Nabhan was the partner of Fazul Abdullah Mohammed, who was killed two weeks ago by Somali security forces. Fazul was sought by the United States for his involvement in the 1998 al-Qaeda suicide attacks on the US embassies in Kenya and Tanzania

operational chief on the ground, and for his involvement as a commander, alongside Nabhan, in the coordinated al-Qaeda terror attack in Kenya in 2002. This attack included the attempted use of an anti-aircraft missile to shoot down an Arkia passenger plane departing from Kenya to Israel, at the same time that a suicide attack, which killed fifteen people, including three Israelis, was underway in the Mombasa Paradise Hotel. Another important object of US targeted killings was Ilyas Kashmiri, who was killed in early June in an aerial operation. Kashmiri was also in al-Qaeda's external branch unit and was a senior operational commander in a Pakistani jihad organization. His name was tied to fatal terrorist attacks executed

and planned in India, Pakistan, and Europe.

These targeted killings are part of an intensive campaign in the war against global terrorism begun by the United States immediately after September 11. In the course of this campaign the United States has

become entangled in a conventional war and in other ongoing, expensive, and bloody subconventional battles in a number of states. Given the complexity and the prolonged nature of the war against al-Qaeda and its affiliates, public opinion has come to feel that the terrorists have succeeded in making a mockery of the world's largest superpower and its allies. However, a careful examination of the terror fighting strategy, and especially the operational conduct of the United States, indicates that the combination of technology and human resources, along with actions by armed unmanned aerial vehicles, has allowed the Americans to carry out effective targeted attacks within the territories in which their ground forces' freedom of movement is limited. In this way, the United States and its allies have succeeded in killing or capturing the commanders of the special al-Qaeda unit that is responsible for carrying out terror attacks abroad. They have also been able to expel many additional senior military commanders and most of the senior activists of al-Qaeda and its main affiliates in the Taliban and other terrorist organizations and networks that operate in the Afghanistan-Pakistan sector. At



the same time, the United States and its allies have succeeded in foiling most of the attempted terrorist attacks by al-Qaeda and global jihad activists.

In spite of the protests heard recently, mostly in Afghanistan and Pakistan, against the aerial killings because of the harm done to uninvolved civilians – harm caused both by the terrorist organizations' deliberate custom of taking shelter among a civilian population, and by human error – the United States, which is leading the struggle against al-Qaeda and its affiliates, has unmistakably and publicly adopted this pattern of action and is in particular implementing it in the subconventional battles underway in these

> theaters. Furthermore, the Americans have also recently been preparing to step up the use of targeted killings from the air in politically unstable Yemen, which against the backdrop of the increased activity of al-Qaeda in the Arabian Peninsula has been marked as another

central theater of conflict. The United States, which about a decade ago had already used targeted killings sporadically in Yemen, recently began using them again when it attempted an aerial killing of Anwar al-Awlaki, a radical Muslim cleric and an official of al-Qaeda in the Arabian Peninsula.

The faint criticism of the intensive targeted killings campaign by the United States, which is heard only rarely around the world, is especially noteworthy in light of the serious condemnations Israel has received for the same conduct. For decades Israel has fought terrorism that threatened its citizens, and during this period it made sparing use of the tools of targeted killings against prominent terrorist leaders. The murderous large scale terrorism carried out against Israeli citizens during the second intifada, which was manifested largely in suicide terrorism, led to the government of Israel's developing and expanding the use of this operational tool and aiming it at the most prominent and dangerous planners and perpetrators of terrorism. Targeted killings played a major though not exclusive role in Israel's success in rooting out suicide terrorism and undermining the violence

of the first years of the second intifada. Significantly, the use of targeted killings was regulated by Israel's Supreme Court and was permitted only against those who beyond a doubt were actively engaged in terrorism aimed at harming the civilian population. Needless to say, there was no similar criticism of the United States following the killing of Bin Laden, or even after the killings of the rest of the officials of al-Qaeda, who were also perceived as a threat to the security and stability of the international community. Furthermore, the clear threat made by American officials that Ayman Zawahiri, whose official selection as Bin Laden's successor was announced publicly by the organization on June 16, is a target for assassination, makes it clear that the United States and its allies do not intend to stop this policy.

The coordinated activity among many of the world's security services, including from rival states that collaborate ad hoc, demonstrates that in spite of moral dilemmas and legal restrictions, the selective and precise use of targeted killings is deemed an effective and essential option, and therefore cannot be relinguished as one of the tools in democratic states' arsenals. Nevertheless, it is clear that decision makers and public opinion in democratic countries must understand that the problem of worldwide terrorism cannot be solved by means of one operational tool, no matter how effective, because of the possible albeit unintentional - collateral damage. Therefore, adoption of the tool of targeted killings always requires prudent and cautious implementation, subject to ongoing scrutiny and review by the attacking state. This scrutiny must consider the level of concrete threat from the objects of the targeted killings and the circumstances in which they are acting, with serious consideration given to the long and short term ramifications on the overall policy of the fight against terror.

#### Einav Yogev is a research assistant in the Terrorism and Low Intensity Conflict Program at INSS.

#### Israel drills for potential mass missile attacks

Source: http://news.xinhuanet.com/english2010/world/2011-06/22/c\_13944486.htm

The Israeli government, the military, rescue services, 80 municipalities, and millions of civilians on Wednesday drilled responses to a simultaneous mass missile strikes across the country.

This year's test, which was the high point of the week-long " Turning Point 5" drill, marks the first time in the five years the exercise has been held that the entire population was instructed to seek cover.

In the drill's scenario, it is the 13th day of a fullscale war, and Israel's foes have lobbed some 7,000 missiles, hitting Tel Aviv, Jerusalem, and other major population centers. Hundreds are dead and thousands wounded, according to Home Front Command Minister Matan Vilna'i, who led the government's civilian responses to the mass attack.

"In last year's exercise, about 47 percent of the population entered protected areas," Col. Efi Mishov, head of the Home Front Command's Population Department, told the Yisrael Hayom newspaper.

"The past several years have seen a moderate increase in exercise participation, and this

trend is expected to continue this year, but not in drastic numbers," Mishov said.

The government security cabinet, as part of the drill, met for the first time in a secret underground bunker in the Jerusalem area. Israeli Prime Minister Benjamin Netanyahu and government ministers would use the facility in such a missile attack. Part of the drill included direct missile hits on the Knesset parliament building and on the nearby Prime Minister's Office.





Members of Israeli Army participate in an exercise which simulates a rocket attack on Ashdod Port, Israel, on June 22, 2011. Israel is holding a nation-wide, week-long emergency drills simulating simultaneous mass-casualty events. (Xinhua/Rafael Ben-Ari)

The sirens were to sound once, as a part of the drill, and a second only in the event of a real attack. In several cities, among them coastal

Ashkelon and Ashdod, and Beer Sheba in the northern Negev, malfunctioning sirens went off twice, scaring residents who thought it was a



A member of Israeli Army participates in an exercise which simulates a rocket attack on Ashdod Port, Israel, on June 22, 2011. Israel is holding a nation-wide, week-long emergency drills simulating simultaneous mass-casualty events. (Xinhua/Rafael Ben-Ari)

genuine emergency.

In hospital parking lots, police and Israeli Defense Forces soldiers, and civilian firstresponders garbed in chemical warfare protection suits practiced mass intake and triage, spraying down adults, and -- using baby dolls -- infants suffering from chemical burns and wounds.

Dozens of ambulances pulled up, one after another, to discharge patients, in order to test the logistics of dealing with mass- casualty attacks on a scale Israel has not seen before. As sirens across the country wailed, the country's 7.5 million citizens were instructed to enter bomb shelters and other " protected spaces," and remain inside for a short period. Schools across the country practiced quickly

and calmly entering prepared bomb shelters, and remaining inside for 15 minutes.

"At first I thought it was real, but then they told me it wasn' t real," said nine-year-old Maya Firestone, a student at Jerusalem 's Evelina De Rothschild school. "It was a little crazy because everyone was running around," Firestone said. Before its 400 pupils filed out of the shelters and back to their classes, school principal Yossi Ohana, using a bullhorn, debriefed the students.

"Our goal was to evacuate all of the students within one-and-a- half minutes into this shelter," Ohana told Xinhua after the drill concluded.

The exercise, which was widely publicized in radio and television spots, as well as online, is meant to ready the populace for the worst, and comprehensively synchronize crisismanagement responses to salvos of rockets from neighboring areas slamming into Israeli cities.

One of the simulation's goals is also to warn potential foes that such an attack would cause little damage to a government, public and military protected and readied for the worst.

"Our enemies know perfectly well that if they attack us, we will strike them with very tough blows, but we must prepare," Israel's Home Front Command Minister, Matan Vilnai, told Army Radio on Sunday, "because they have the capacity to fire missiles and rockets at all of our territory."

The Israeli army's former intelligence chief Amos Yadlin said on Wednesday that "these missiles will not disappear, even if a peace agreement with the Palestinians is signed."



A member of Israeli Army participates in an exercise which simulates a rocket attack on Kiryat Malachi industrial site, Israel, on June 22, 2011. Israel is holding a nation-wide, week-long emergency drills simulating simultaneous mass-casualty events. (Xinhua/Rafael Ben-Ari)





Members of Israeli Army participate in an exercise which simulates a rocket attack on Ashdod Port, Israel, on June 22, 2011. Israel is holding a nation-wide, week-long emergency drills simulating simultaneous mass-casualty events. (Xinhua/Rafael Ben-Ari)



Members of Israeli Army participate in an exercise which simulates a rocket attack on Ashdod Port, Israel, on June 22, 2011. Israel is holding a nation-wide, week-long emergency drills simulating simultaneous mass-casualty events. (Xinhua/Rafael Ben-Ari)



# Al-Qaeda and the Libyan Rebellion

Source:http://www.nationalreview.com/articles/270293/al-qaeda-and-libyan-rebellion-john-rosenthal? page=1

A new report from two French think tanks concludes that jihadists have played a predominant role in the eastern-Libyan rebellion against the rule of Moammar Qaddafi, and that "true democrats" represent only a minority in the rebellion. The report, furthermore, calls into question the justifications given for Western military intervention in Libya, arguing that they are largely based on media exaggerations and "outright disinformation."

The sponsors of the report are the Paris-based International Center for Research and Study on Terrorism and Aide to Victims of Terrorism (CIRET-AVT) and the French Center for Research on Intelligence (CF2R). The organizations sent a six-member expert mission to Libya to evaluate the situation and consult with representatives on both sides of the conflict. From March 31 to April 6, the mission visited the Libyan capital of Tripoli and the region of Tripolitania; from April 19 to April 25, it visited the rebel capital of Benghazi and the surrounding Cyrenaica region in eastern Libya.

The report identifies four factions among the members of the eastern Libyan National Transitional Council (NTC). Apart from a minority of "true democrats," the other three factions comprise partisans of a restoration of the monarchy that was overthrown by Qaddafi in 1969, Islamic extremists seeking the establishment of an Islamic state, and former fixtures of the Qaddafi regime who defected to the rebels for opportunistic or other reasons.

There is a clear overlap between the Islamists and the monarchists, inasmuch as the deposed King Idris I was himself the head of the Senussi brotherhood, which the authors describe as "an anti-Western Muslim sect that practices an austere and conservative form of Islam." The monarchists are thus, more precisely, "monarchists-fundamentalists."

The most prominent of the defectors, the president of the NTC, Mustafa Abdul Jalil, is likewise described by the authors as a "traditionalist" who is "supported by the Islamists." The authors point out that Jalil played an important role in the "Bulgarian nurses affair," so called for five Bulgarian

nurses who, along with a Palestinian doctor, were charged with deliberately infecting hundreds of children with AIDS in a hospital in Benghazi. As chair of the Appeals Court in Tripoli, Jalil twice upheld the death penalty for the nurses. In 2007, the nurses and the Palestinian doctor were released by the Libyan government following negotiations in which French president Nicolas Sarkozy's then wife, Cecilia, played a highly publicized role.

The report describes members of the al-Qaeda-affiliated Libyan Islamic Fighting Group as the "main pillar of the armed insurrection." "Thus the military coalition under NATO leadership is supporting a rebellion that includes Islamic terrorists," the authors write. Alluding to the major role played by the Cyrenaica region in supplying recruits for al-Qaeda in Iraq, they add, "No one can deny that the Libyan rebels who are today supported by Washington were only yesterday jihadists killing American GIs in Iraq."

The full composition of the NTC has not been made public. But, according to the authors, one avowed al-Qaeda recruiter, Abdul-Hakim al-Hasadi, is himself a member of the NTC. Al-Hasadi is described by the authors as the "leader of the Libyan rebels." Although Western media reports commonly say that he is in charge of the defense of his home town of Darnah in eastern Libya, the CIRET-CF2R report suggests that in mid-April, al-Hasadi left Cyrenaica by boat in order to participate in the battle of Misrata. He is supposed to have taken arms and 25 "well-trained fighters" with him. Misrata is in western Libya, a mere 135 miles from Tripoli.

Regarding the effects of western military intervention in support of the rebels, the authors conclude:

Western intervention is in the process of creating more problems than it resolves. It is one thing to force Qaddafi to leave. It is another thing to spread chaos and destruction in Libya to this end and to prepare the ground for fundamentalist Islam. The current moves risk destabilizing all of North Africa, the Sahel, and the.

Middle East and favoring the emergence of a new regional base for radical Islam and terrorism.

### Some parts from this study:

### On the Battle of Misrata:

Little by little, the city is starting to appear like a Libyan version of Sarajevo in the eyes of the "free" world. The rebels from Benghazi hope that a humanitarian crisis in Misrata will convince the Western coalition to deploy ground troops in order to save the population.

... During the course of April, the NGO Human Rights Watch published casualty figures concerning Misrata that reveal that, contrary to the claims made in the international media, Qaddafi loyalist forces have not massacred the residents of the town. During two months of hostilities, only 257 persons including combatants - were killed. Among the 949 wounded, only 22 - or fewer than 3 percent - were women. If regime forces had deliberately targeted civilians, women would have represented around half of the victims. It is thus now obvious that Western leaders first and foremost. President Obama - have grossly exaggerated the humanitarian risk in order to justify their military action in Libya. The real interest of Misrata lies elsewhere.... The control of this port, at only 220 kilometers from Tripoli, would make it an ideal base for launching a land offensive against Qaddafi.

### On Benghazi and the Cyrenaica Region:

Benghazi is well-known as a hot-bed of religious extremism. The Cyrenaica region has a long Islamist tradition going back to the Senussi brotherhood. Religious fundamentalism is much more evident here than in the western part of the country. Women are completely veiled from head to foot. They cannot drive and their social life is reduced to a minimum. Bearded men predominate. They often have the black mark of piety on their foreheads [the "zebibah," which is formed by repeated prostration during Muslim prayers].

It is a little-known fact that Benghazi has become over the last 15 years the epicenter of African migration to Europe. This traffic in human beings has been transformed into a veritable industry, generating billions of dollars. Parallel mafia structures have developed in the city, where the traffic is firmly implanted and employs thousands of people, while corrupting police and civil servants. It was only a year ago that the Libyan government, with the help of Italy, managed to bring this cancer under control.

Following the disappearance of its main source of revenue and the arrest of a number of its bosses, the local mafia took the lead in financing and supporting the Libyan rebellion. Numerous gangs and members of the city's criminal underworld are known to have conducted punitive expeditions against African migrant workers in Benghazi and the surrounding area. Since the start of the rebellion, several hundred migrant workers — Sudanese, Somalis, Ethiopians, and Eritreans — have been robbed and murdered by rebel militias. This fact is carefully hidden by the international media.

## On African "Mercenaries" and Tuaregs:

One of the greatest successes [of Qaddafi's African policy] is his "alliance" with the Tuaregs [a traditionally nomadic population spread over the region of the Sahara], whom he actively financed and supported when their movement was repressed in Mali in the 1990s.

... In 2005, Qaddafi accorded an unlimited residency permit to all Nigerian and Malian Tuaregs on Libyan territory. Then, in 2006, he called on all the tribes of the Sahara region, including Tuareg tribes, to form a common entity to oppose terrorism and drug trafficking ...

This is why hundreds of combatants came from Niger and Mali to help Qaddafi [after the outbreak of the rebellion]. In their view, they were indebted to Gaddafi and had an obligation to do so....

Many things have been written about the "mercenaries" serving in the Libyan security forces, but few of them are accurate....

In recent years, foreigners have .... been recruited [into the Libyan army]. The phenomenon is entirely comparable to the phenomenon that one observes on all levels of Libyan economic life. There is a very large population of foreign workers in search of employment in the country. The majority of the recruits originally come from Mali, Chad, Niger, Congo, and Sudan. ...

The information from rebel sources on supposed foreign intrusions [i.e. mercenaries] is vague and should be treated with caution....

On the other hand, it is a proven fact — and the mission was able to confirm this itself that Tuaregs from Niger came to Tripoli to offer their support to Qaddafi. They did so spontaneously and out of a sense of debt.

... It seems that Libyans of foreign origin and genuine volunteers coming from foreign countries are being deliberately confused [in the reports on "mercenaries"]. Whatever the actual number [of foreign fighters], they form only a small part of the Libyan forces.

### On the role of the international media:

Up until the end of February, the situation in western Libyan cities was extremely tense and there were clashes — more so than in the east. But the situation was the subject of exaggeration and outright disinformation in the media. For example, a report that Libyan aircraft bombed Tripoli is completely inaccurate: No Libyan bomb fell on the capital, even though bloody clashes seem to have taken place in certain neighbourhoods....

The consequences of this disinformation are clear. The U.N. resolution [mandating intervention] was approved on the basis of such media reports. No investigative commission was sent to the country. It is no exaggeration to say that sensationalist reporting by al-Jazeera influenced the U.N.

As soon as the protests started, Islamists and criminals immediately took advantage of the situation in order to attack high-security prisons outside Benghazi where their comrades were being held. Following the liberation of their leaders, the rebellion attacked police stations and public buildings. The residents of the city woke up to see the corpses of policemen hanging from bridges.

Numerous atrocities were likewise committed against African workers, who have all been treated as "mercenaries." African workers were expelled, murdered, imprisoned, and tortured.

# On the insurrection in Zawiya (a town in western Libya):

During the three weeks [that the town was controlled by the rebels], all public buildings were pillaged and set on fire.... Everywhere, there was destruction and pillaging (of arms, money, archives). There was no trace of combat, which confirms the testimony of the police [who claim to have received orders not to intervene]....

There were also atrocities committed (women who were raped, and some police officers who were killed), as well as civilian victims during these three weeks.... The victims were killed in the manner of the Algerian GIA [Armed Islamic Group]: throats cut, eyes gauged out, arms and legs cut off, sometimes the bodies were burned ...

### On the insurrection in Benghazi:

### John Rosenthal writes on European politics and transatlantic security issues.

**NOTE:** Full report [in French] can be downloaded from the Newsletter's website – section: "CBRNE-CT Papers"

# U.S. no longer mandating 100 percent screening of cargo containers

Source:http://www.homelandsecuritynewswire.com/us-no-longer-mandating-100-percent-screening-cargo-containers

DHS Secretary Janet Napolitano announced that the United States is no longer going to screen every cargo container before it enters the United States.

On a visit to the Netherlands' Rotterdam port, the fourth largest in the world, Napolitano said, "We believe the so-called 100 percent requirement is probably not the best way to go."

In 2007 Congress mandated that all containers entering the United States must be scanned at their ports of exit by 2012, but Napolitano said, "We at this point are not going to insist on that." Earlier this week, Napolitano met with Home Secretary Theresa May, her British counterpart, as well as with other EU ministers to explain the U.S. position on the security mandate.

The 2007 bill empowers DHS to extend the 2012 deadline if the agency believed that the goal was not achievable and in the past Napolitano has expressed doubts about the

feasibility of screening 100 percent of the cargo entering the United States.



Napolitano says rather than scanning all cargo containers, DHS prefers a "layered approach"

that includes increased cooperation between countries and better intelligence sharing and

analysis in addition to screening some containers. She explained, "I think what we have learnt over time is that there are many different ways to achieve a security objective. You have to have multiple layers that operate effectively." Napolitano is currently abroad on week-long visit to Britain and other European nations to bolster support for global efforts to secure the supply chain.

So far about fifty ports around the world have signed on to the U.S.-led Container Security Initiative (CSI) which is aimed at preventing terrorist attacks and the smuggling of

dangerous materials by mandating that port authorities pre-scan and evaluate containers.

# Background Report on Suicide Attack on Intercontinental Hotel in Kabul, Afghanistan

Source: http:// www.start.umd.edu/gtd

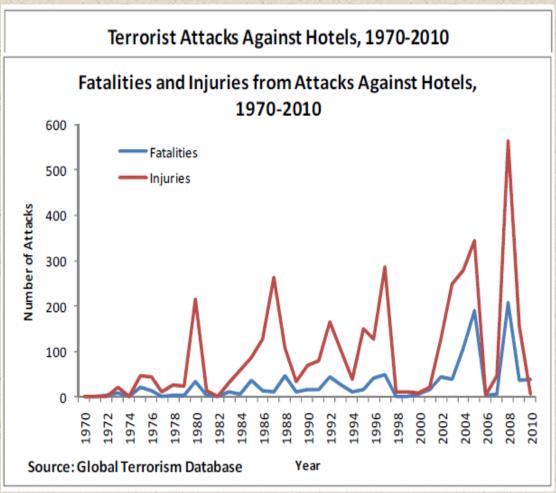
Following June 28th, 2011 coordinated attack by the Taliban on the Intercontinental Hotel in Kabul, Afghanistan, National Consortium for the Study of Terrorism and Response to Terrorism [START] has released a background report featuring information on terrorist activities in Afghanistan, attacks by the Taliban, attacks using complex tactics, and attacks by terrorist groups against hotels.



Key findings from the report include:

- ☑ Since 1970, there have been 2,417 terrorist attacks in Afghanistan, with the majority of those occurring since the fall of the Taliban in 2001.
- ☑ The Taliban are now the most active terrorist organization in Afghanistan, accounting for 1,323 attacks against civilians, or 57.7% of all attacks in Afghanistan since 1970.
- Since 1970, terrorist groups throughout the world have conducted 2,515 tactically complex attacks (using both firearms and explosives in the commission of a single attack).
- More than 660 attacks against hotels have occurred in the past 40 years, with at least three attacks occurring each year.
- Hotels appear to be of increasing interest to terrorist organizations, targeted in more than 100 attacks since 2005 alone.





These data were collected and compiled from the Global Terrorism Database. An updated version of the database, with information on incidents through 2010, was released in June 2011. Unlike many other event databases, the GTD includes systematic data on domestic as well as transnational and international terrorist incidents that have occurred during this time period. For each GTD incident, information is available on the date and location of the incident, the weapons used and nature of the target, the number of casualties, and—when identifiable—the perpetrator.

Notable instances of hotel attacks include:

- March 2002 a Hamas suicide bomber detonated an IED inside the Park Hotel in Netanya, Israel, killing 20 and wounding 72.
- July 2005 three coordinated vehicle bombs targeted resorts and hotels in Sharm el-Sheikh, Egypt, killing 91 and wounding over 100. The attack was claimed by the Abdullah Azzam Brigades.
- November 2005 three bombings of hotels in Amman, Jordan, by Al Qaeda in Iraq killed 57 and wounded over 100.
- January 2008 an attack by the Taliban using suicide bombers and gunmen targeted the Serena Hotel in Kabul, killing eight people.
- September 2008 a truck bomb detonated at the Marriott Hotel in Islamabad, Pakistan, killing 60 and injuring more than 200.
- November 2008 a coordinated attack by Lashkar-e-Taiba in Mumbai targeted the Taj Mahal Palace and Tower Hotel and the Oberoi Trident Hotel, among other sites, killing 171 and wounding 250.

NOTE: Full report can be downloaded from the Newsletter's website - section: "CBRNE-CT Papers".

317

# Taliban Hotel Attack: Low Death Toll, High Psychological Value

### **By Scott Stewart**

Source: http://www.stratfor.com/weekly/20110706-taliban-hotel-attack-low-death-toll-high-psychological-value?utm\_source=freelist-f&utm\_medium=email&utm\_campaign=110707&utm\_term=sweekly&utm\_content=readmore &elg=b42deeac504248dc9a0a3f42a89f4a93

At about 10 p.m. on June 28, a group of heavily armed militants attacked the Intercontinental Hotel in

Kabul, Afghanistan. According to government and media reports, the attack team consisted of eight or nine militants who were reportedly wearing suicide vests in addition to carrying other weapons. At least three of the attackers detonated their vests during the drawn-out fight. Afghan security forces, assisted by International Security Assistance Force (ISAF), needed some eight hours to clear the hotel of attackers. One group of militants even worked their way up to the roof of the hotel, where they



fired several rocket-propelled grenades.

The attack resulted in the deaths of 12 people, as well as all the militants. The Taliban had a different take on the attack, posting a series of statements on their website claiming responsibility and saying the assault was conducted by eight operatives who killed 90 people and that the real news of their success was being suppressed. (Initially, the Taliban claimed to have killed 200 in the attack but reduced the toll to 90 in later statements.)

NATO and ISAF spokesmen have noted their belief that, due to the location and use of suicide bombers in the attack, the Haqqani network was involved in the operation. On the evening of June 29, a NATO airstrike killed Ismail Jan, a senior Haqqani leader in Afghanistan who NATO claims was involved in planning the hotel attack.

When viewed in the context of other recent attacks in Kabul and other parts of Afghanistan,

the attack on the Intercontinental Hotel was not all that spectacular. It certainly did not kill the 90 people the Taliban claim, although it does have a number of interesting security implications.

### Past Attacks

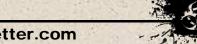
Militants in Afghanistan have conducted several armed-assault style attacks in Kabul in recent years. In April 2011, a group of militants dressed in Afghan army uniforms stormed the



Ministry of Defense in Kabul and killed two people in what the Taliban later claimed was an assassination attempt aimed at the visiting French defense minister.

On Jan. 18, 2010, the day that the Afghan Cabinet was sworn in, 11 militants conducted a wave of armed assaults against a variety of high-profile targets in Kabul that included the presidential palace, the Central Bank and the Defense and Justice ministries. The most prolonged fighting occurred at the newly opened Grand Afghan Shopping Center. The shopping center was heavily damaged by a fire apparently initiated by the detonation of a suicide device. In spite of the large number of militants participating in this attack, it resulted only in seven deaths.

In February 2009, eight militants attacked the Justice Ministry, the Department of Prison Affairs and the Education Ministry. The attack killed 21 people and took place the day before



former U.S. envoy Richard Holbrooke was scheduled to arrive in Kabul.

The Taliban have also targeted hotels in Kabul. In January 2008, the Serena Hotel was attacked by four militants who used an explosive device to breach the front security perimeter and then stormed the hotel. One of the attackers detonated his suicide vest in the lobby and another roamed through the hotel shooting guests. The attack, which resulted in six deaths, occurred while the Norwegian foreign minister was staying there.

In October 2009, three militants attacked a guest house being used by U.N. personnel in



Kabul. The attack resulted in the deaths of five U.N. staff members and three Afghans. The Taliban took credit for this attack, which targeted U.N. election workers in an attempt to disrupt the November 2009 Afghan election.

### Sending a Message

When STRATFOR began looking at these Kabul attacks from a tactical viewpoint, we

were initially surprised by the relatively low death toll considering the number of militant operatives employed. None of the Taliban's armed assaults in Kabul have produced the high casualty count of the November 2009 Mumbai attacks. However, over time it became quite apparent that the objective of these armed assaults in Kabul was not only to cause carnage. If so, the Taliban would have discontinued conducting such attacks due to the relatively low return on investment they were providing. Instead, the Taliban have shown that they like to use such attacks at strategic times to make sure the threat they

> pose is not forgotten. Consider the context of the attacks described above. They all happened in relation to other events that were occurring at the time over which the Taliban wished to voice their displeasure. The attack on the Intercontinental Hotel occurred during а conference to discuss the security transfer of authority from the ISAF to the Afghan government an event the Taliban certainly wanted to comment on, and did.

> These multi-man armed attacks in Kabul were true acts of terrorism - attacks conducted their for symbolic propaganda value - and not acts conducted to be tactically significant from a military standpoint. When taken together, these less than spectacular individual attacks were conducted with enough frequency to

cultivate a perception of instability and lack of security in the Afghan capital — an important goal for the Taliban.

In their official statement claiming responsibility, the Taliban said the Intercontinental Hotel attack was intended to disrupt the handover conference. They also claimed their primary goal was to target U.S. and NATO spies and agents who would be

staying at the hotel, but that was obviously a red herring since very few Western government employees stay at that hotel, though some do attend meetings there.

This attack also illustrated some other facts about the Taliban movement: First, the Taliban do not appear to have any shortage of men. Despite almost 10 year of war, they have the international luxury hotel and was a part of the international chain of hotels with the same name, now known as the InterContinental Hotels Group. Following the 1979 Soviet invasion of Afghanistan, the hotel ceased to be part of the InterContinental Hotels brand, but the hotel's local ownership continued to use the Intercontinental name.



resources to burn through eight suicide operatives on a mission that did not appear to be strategically significant. Second, they do not appear to be suffering from morale problems. They are able to readily recruit militants willing to sacrifice their lives for the cause. And they



are able to make outlandish propaganda claims — that they killed 90 people in the hotel attack, for example — to a target audience that will take their statements at face value. This brings us to our final point, a discussion of the Kabul Intercontinental Hotel itself.

### The 'Intercontinental'

Kabul's Intercontinental Hotel, known widely as the "Intercon," opened for business in 1969. At that time it was the Afghanistan's first This is not an uncommon situation, particularly in countries like Afghanistan where it is hard for large corporate hotel groups to enforce their trademarks. One potential downside of this type of arrangement is that it can give an international traveler a false sense of security. Generally, the large hotel chains are very serious about security, and if a chain does not own a specific hotel property, the local owner of the property who wants to use the chain's name will be forced to adhere to the chain's stringent security standards. Therefore, anyone seeing the Intercontinental Hotel name would assume that the Intercon in Kabul would adhere to the global chain's security standards. In this case, they would be wrong.

Most U.S. and Western visitors to Kabul stay at the Serena Hotel rather than the Intercon because the Serena has better security. The Intercon tends to get more local traffic, which belies the Taliban's claim that the primary reason they attacked the Intercon was to kill U.S. and NATO spies. We have heard rumors that the operation may have been intended to target a specific VIP who was supposed to be visiting the property but have not been able to confirm this. If a VIP was indeed the target, the operation failed to kill him or her. The false assumption that the Kabul Intercon would adhere to the stringent security standards of the InterContinental Hotels Group illustrates the importance of properly preparing for a trip by thoroughly researching your destination before traveling. This week, STRATFOR began publishing a series of reports on travel security that are designed to assist travelers during the busy summer travel season in the Northern Hemisphere.

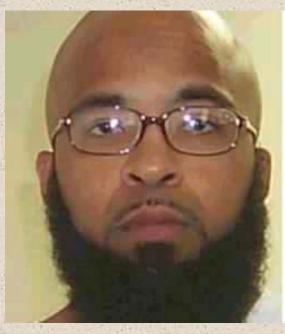
As U.S. and other international forces begin withdrawing from Afghanistan, we can expect the Taliban and their allies to continue conducting high-profile attacks in the heart of Kabul that coincide with significant events. Such attacks will be a fact of life in the city for the foreseeable future, and people traveling to and from or living in Kabul should pay close attention to events that could trigger Taliban attacks and plan their activities and make personal security arrangements accordingly. Even the Taliban cannot attack without conducting preoperational surveillance, which highlights the utility of surveillance detection and counterintelligence to uncover Taliban agents who have penetrated facilities in order to turn them into targets.

# The Seattle Plot: Jihadists Shifting Away From Civilian Targets?

### **By Scott Stewart**

Source:http://www.stratfor.com/weekly/20110629-seattle-plot-jihadists-shifting-away-civilian-targets? utm\_source=freelist-f&utm\_medium=email&utm\_campaign=20110630&utm\_term=sweekly&utm\_ content=readmore&elq=917231c43be74001822827c30f49275b

On June 22 in a Seattle warehouse, Abu Khalid Abdul-Latif pulled an unloaded M16 rifle to his shoulder, aimed it, and pulled the trigger small number of hand grenades were to be used in an upcoming mission: an attack on a U.S. Military Entrance Processing Station



repeatedly as he imagined himself gunning down young U.S. military recruits. His longtime friend Walli Mujahidh (photo – right) did likewise with an identical rifle, assuming a kneeling position as he engaged his notional targets. The two men had come to the warehouse with another man to inspect the firearms the latter had purchased with money Abdul-Latif had provided him. The rifles and a



(MEPS) in an industrial area south of downtown Seattle.

After confirming that the rifles were capable of automatic fire and discussing the capacity of the magazines they had purchased, the men placed the rifles back into a storage bag intending to transport them to a temporary cache location. As they prepared to leave the warehouse, they were suddenly swarmed by

large number of FBI agents and other law enforcement officers and quickly arrested. Their plan to conduct a terrorist attack inside the United States had been discovered when the man they had invited to join their plot (the man who had allegedly purchased the weapons for them) reported the plot to the Seattle Police Department, which in turn reported it to the FBI. According to the federal criminal complaint filed in the case, the third unidentified man had an extensive criminal record and had known Abdul-Latif for several years, but he had not been willing to undertake such a terrorist attack.

While the behavior of Abdul-Latif and Mujahidh in this plot demonstrates that they were amateur "wannabe" jihadists rather than seasoned terrorist operatives, their plot could have ended very differently if they had found a kindred spirit in the man they approached for help instead of someone who turned them into the authorities. This case also illustrates some important trends in jihadist terrorism that we have been watching for the past few years as well as a possible shift in mindset within the jihadist movement.

### Trends

First, Abu-Khalid Abdul-Latif and Walli Mujahidh, both American converts to Islam, are prime examples of what we refer to as grassroots jihadists. They are individuals who were inspired by the al Qaeda movement but who had no known connection to the al Qaeda core or one of its franchise groups. In late 2009, in response to the success of the U.S. government and its allies in preventing jihadist attacks in the West, al Qaeda in the Arabian Peninsula (AQAP) began a campaign to encourage jihadists living in the West to conduct simple attacks using readily available items, rather than travel abroad for military and terrorism training with jihadist groups. After successes such as the November 2009 Fort Hood shooting, this theme of encouraging grassroots attacks was adopted by the core al Qaeda group.

While the grassroots approach does present a challenge to law enforcement and intelligence agencies in that attackers can seemingly appear out of nowhere with no prior warning, the paradox presented by grassroots operatives is that they are also far less skilled than trained terrorist operatives. In other words, while they are hard to detect, they frequently

lack the skill to conduct large, complex attacks and frequently make mistakes that expose them to detection in smaller plots.

And that is what we saw in the Seattle plot. Abdul-Latif had originally wanted to hit U.S. Joint Base Lewis-McChord (formerly known as Fort Lewis and McChord Air Force Base), which is located some 70 kilometers (44 miles) south of Seattle, but later decided against that plan since he considered the military base to be too hardened a target. While Abdul-Latif and Mujahidh were amateurs, they seem to have reached a reasonable assessment of their own abilities and which targets were beyond their abilities to strike.

Another trend we noted in this case was that the attack plan called for the use of firearms and hand grenades in an armed assault, rather than the use of an improvised explosive device (IED). There have been a number of botched IED attacks, such as the May 2010 Times Square attack and Najibullah Zazi's plot to attack the New York subway system.

These were some of the failures that caused jihadist leaders such as AQAP's Nasir al-Wahayshi to encourage grassroots jihadists to undertake simple attacks. Indeed, the most successful jihadist attacks in the West in recent years, such as the Fort Hood shooting, the June 2009 attack on a military recruitment center in Little Rock, Ark., and the March 2011 attack on U.S. troops at a civilian airport in Frankfurt, Germany, involved the use of firearms rather than IEDs. When combined with the thwarted plot in New York in May 2011, these incidents support the trend we identified in May 2010 of grassroots jihadist conducting more armed assaults and fewer attacks involving IEDs.

Another interesting aspect of the Seattle case was that Abdul-Latif was an admirer of AQAP ideologue Anwar al-Awlaki. Unlike the Fort Hood case, where U.S. Army Maj. Nidal Malik Hasan had been in email contact with al-Awlaki, it does not appear that Abdul-Latif had been in contact with the AQAP preacher. However. from video statements and comments Abdul-Latif himself posted on the Internet, he appears to have had a high opinion of al-Awlaki and to have been influenced by his preaching. It does not appear that Abdul-Latif, who was known as Joseph Anthony Davis before his conversion to Islam, or Mujahidh, whose pre-conversion name was Frederick Domingue Jr., spoke Arabic. This underscore

the importance of al-Awlaki's role within AQAP as its primary spokesman to the Englishspeaking world and his mission of radicalizing English-speaking Muslims and encouraging them to conduct terrorist attacks in the West.

### **Vulnerabilities**

Once again, in the Seattle case, the attack on the MEPS was not thwarted by some CIA source in Yemen, an intercept by the National Security Agency or an intentional FBI undercover operation. Rather, the attack was thwarted by a Muslim who was approached by Abdul-Latif and asked to participate in the attack. The man then went to the Seattle Police Department, which brought the man to the attention of the FBI. This is what we refer to as grassroots counterterrorism, that is, local cops and citizens bringing things to the attention of federal authorities. As the jihadist threat has become more diffuse and harder to detect, grassroots defenders have become an even more critical component of international counterterrorism efforts. This is especially true for Muslims, many of whom consider themselves engaged in a struggle to defend their faith (and their sons) from the threat of iihadism.

But, even if the third man had chosen to participate in the attack rather than report it to the authorities, the group would have been vulnerable to detection. First, there were the various statements Abdul-Latif made on the Internet in support of attacks against the United States. Second, any Muslim convert who chooses a name such as Mujahidh (holy warrior) for himself must certainly anticipate the possibility that it will bring him to the attention of the authorities. Abdul-Latif and Mujahidh were also somewhat cavalier in their telephone conversations, although those conversations do not appear to have brought them to the attention of the authorities.

Perhaps their most significant vulnerability to detection, aside from their desire to obtain automatic weapons and hand grenades, would have been their need to conduct preoperational surveillance of their intended target. After conducting some preliminary research using the Internet, Abdul-Latif quickly realized that they needed more detailed intelligence. He then briefly conducted physical surveillance of the exterior of the MEPS to see what it looked like in person. Despite the technological advances it represents, the Internet cannot replace the physical surveillance process, which is a critical requirement for terrorist planners. Indeed, after the external surveillance of the building, Abdul-Latif asked the informant to return to the building under a ruse in order to enter it and obtain a detailed floor plan of the facility for use in planning the attack.

In this case, the informant was able to obtain the information he needed from his FBI handlers, but had he been a genuine participant in the plot, he would have had to have exposed himself to detection by entering the MEPS facility after conducting surveillance of the building's exterior. If some sort of surveillance detection program was in place, it likely would have flagged him as a person of interest for follow-up investigation, which could have led authorities back to the other conspirators in the attack.

### A New Twist

One aspect of this plot that was different from many other recent plots was that Abdul-Latif insisted that he wanted to target the U.S. military and did not want to kill people he considered innocents. Certainly he had no problem with the idea of killing the armed civilian security guards at the MEPS - the plan called for the attackers to kill them first, or the unarmed still-civilian recruits being screened at the facility, then to kill as many other military personnel as possible before being neutralized by the responding authorities. However, even in the limited conversations documented in the federal criminal complaint. Abdul-Latif repeated several times that he did not want to kill innocents. This stands in stark contrast to the actions of previous attackers and plotters such as John Allen Mohammed, the so-called D.C. sniper, or Faisal Shahzad, who planned the failed Times Square attack. Abdul-Latif's reluctance to attack civilians may be a reflection of the debate we are seeing among jihadists in places like Afghanistan, Pakistan and even Algeria over the killing of those they consider innocents. This debate is also raging on many of the English-language jihadist message boards Abdul-Latif frequented. Most recently, this tension was seen in the defection of a Tehrik-i-Taliban Pakistan faction in Pakistan's Kurram agency. If this sentiment begins to take wider hold in the jihadist movement, and especially the English-speaking jihadist community in the

West, it could have an impact on the targetselection process for future attacks by grassroots operatives in the West. It could also mean that commonly attacked targets such as subway systems, civilian aircraft, hotels and public spaces will be seen as less desirable than comparably soft military targets. Given the limitations of grassroots jihadists, and their tendency to focus on soft targets, such a shift would result in a much smaller universe of potential targets for such attacks — the softer military targets such as recruit-processing stations and troops in transit that have been targeted in recent months. Removing some of the most vulnerable targets from the potential-target list is not something that militants do lightly. If this is indeed happening, it could be an indication that some important shifts are under way on the ideological battlefield and that jihadists may be concerned about losing their popular support. It is still too early to know if this is a trend and not merely the idiosyncrasy of one attack planner — and it is contrary to the target sets laid out in recent messages from AQAP and the al Qaeda core — but when viewed in light of the Little Rock, Fort Hood and Frankfurt shootings, it is definitely a concept worth further examination.

# Questions arise surrounding the assassination of Ilyas Kashmiri

Source: http://www.jamestown.org

As images of a dead Muhammed Ilyas Kashmiri have yet to surface or be produced by either Pakistani government officials or any of the myriad militant organizations operating freely in the Federally Administered Tribal Areas (FATA), some in both Pakistan and Washington have expressed doubts over the veracity of the claim that Kashmiri was wiped out in a South Waziristan drone attack on June

3. Kashmiri has been a major militant leader heading both the 'Brigade 313' of Harakat-ul-Jihad al-Islami (HuJI) and al-Qaeda's Lashkar-e-Zil (LeZ) 'shadow army' (For more on Kashmiri, see Militant Leadership Monitor, January 2010). At the time of his supposed assassination, he was in

assassination, ne was in an area of South Waziristan controlled by Maulvi Nazir in the village of Ghwakhwa when the compound he

was in was leveled by a missile launched from a CIA-operated unmanned aerial vehicle (The News International, June 5). As some American officials began to express doubts about whether Kashmiri had indeed been eliminated from the theater, Pakistani Interior Minister Rehman Malik told the media that



there was a "98 percent chance he is dead" (Reuters, June 5). Pakistan's Prime Minister Yousaf Raza Gilani asserted that American officials were on board with the Pakistani narrative that Kashmiri had been eliminated but when pressed neither the United States Department of State or Department of Defense was willing to publicly line up with PM Gilani's statement (Economic Times [New Delhi], June 7). CIA-run drones continue to

7). CIA-run drones continue to pummel the Wana area of South Waziristan in the weeks after Kashmiri's alleged death, while Pakistani authorities have still not been able to confirm beyond a shadow of a doubt that Kashmiri has been removed from the militant scene in that agency (AFP, June 15).

It has been speculated that Kashmiri has been involved in a host of terror plots across the wider region including the bombing of a restaurant frequented by foreigners on February 13, 2010 in Pune, India that killed 17 (The Hindu, June 17). Kashmiri's lifelong enmity

toward India stems from his jihadi involvement in the Kashmir conflict and his hatred of the Indian state. His desire to attack India proper may have been part of a strategy to divert Pakistani military attention back toward the Indian border thereby depriving Pakistan of the troop numbers it would need to hereby

operations in North Waziristan and elsewhere in the FATA. Pakistan, constantly seesawing back and forth between American pressure to go to war against its own citizenry in the FATA and its military stance toward India, would be much more comfortable in its traditional mode of mobilizing against India to the east than or the Tehrik-e-Taliban Pakistan (The Express Tribune [Karachi], May 24). After Syed Saleem Shahzad reported the depth of Kashmiri's Brigade 313 penetration into the Pakistan Navy for Asia Times Online, he was subsequently abducted and killed while en route to a television interview in Islamabad. An



facing Kashmiri's militants in the west.

The most recent operation attributed to Kashmiri, a May 22 attack on the Pakistan Naval Station Mehran in Karachi - home of the Pakistan's Navy's air wing - led many, including Pakistani journalists and police, to believe that Kashmiri's arm of al-Qaeda had tentacles inside the Pakistani military (Asia Times Online, May 27). Initial reactions in Pakistan were colored by two consecutive bombings on buses transporting Pakistani navy personnel in late April. Islamabad promulgated the notion that ethno-nationalist Balochi separatists were behind these attacks and that perhaps the attack on the Mehran base was a continuation of a spate of said attacks. A Pakistani counter-terrorism official described a Pashto-language phone intercept after the April 26 and 28 IED attacks which greatly lessened the idea that Balochi radicals were involved and pointed to either Pakistan-based al-Qaeda

anonymous Inter-Services Intelligence official stated that it may be in Kashmiri's interest for the world to believe he is gone, as he is (or was) well aware of his being targeted by the United States government (Asia Times Online, June 8). The U.S. Department of State website links Kashmiri to a March 2, 2006 suicide bombing on the American consulate in Karachi which resulted in the death of a U.S. diplomat and three others. [3] HuJI purportedly released a photo said to be Kashmiri's corpse but upon closer inspection, it was in fact an image of one of the killed Lashkar-e-Taiba attackers involved in the November 2008 Mumbai siege (Frontline [Chennail, June 15), If the ISI officer's comment is accurate, that would make HuJI's claim that Kashmiri has been killed part of a ruse aimed at helping him go even deeper underground as the drone war in the FATA grinds on.

#### Notes:

1. Robert I. Rotberg, Battling Terrorism in the Horn of Africa, (Washington D.C.: Brookings Institution Press, 2005), p.184.

То 2. view Fazul Abdullah Mohammed's Rewards for Justice listing, see: http://www.fbi.gov/wanted/wanted terrorists/fazul-abdullah-mohammed. Muhammed Rewards 3. To view Ilvas Kashmiri for Justice listing. see: http://www.state.gov/r/pa/prs/ps/2011/04/160071.htm.

Money, men in short supply to execute Al Qaeda's terror plans

Source: http://www.firstpost.com/fwire/money-men-in-short-supply-to-execute-al-qaedas-terror-plans-35596.html

That all is not well with Al Qaeda is obvious from the plethora of electronic data accessed from Osama bin Laden's last hideout in Pakistan's Abbottabad as the decoding of communication details among the top brass reflects a serious financial crunch in the terrorist oraganisation including a shortage of manpower in lead positions due to killing of leaders by US drone attacks.

During the six weeks of intensive study of the materials obtained from Abbottabad compound of Osama bin Laden, where he was killed by special US forces on 2 May, the CIA-led interagency team prepared some 400 intelligence reports.



Al Qaeda chief Ayman al-Zawahri warns the US of terror attacks. But where is the money and men for this terror network? Reuters

The most important information gleaned from the 15 computers and 100 storage devices recovered from his compound is the information about the internal strains of the terrorist outfit and the repeated attempt of bin Laden to carry out attacks on the US, The Washington Post reported. "The trove makes it clear that bin Laden's primary goal—you can call it an obsession— was to attack the US homeland," a senior US counter-terrorism official was quoted as saying. "He pushed for this every way he could," he added.

According to The Washington Post over the past year, the AI Qaeda leader fielded e-mails from followers lamenting the toll being taken by CIA drone "explosions" as well as the network's financial plight.

"Bin Laden approved the creation of a counterintelligence unit to root out traitors and spies, only to receive a complaint in mid-2010 from the unit's leader that it was losing the 'espionage war' and couldn't function on its

paltry budget," it said.

"Just months before the Arab Spring took hold, bin Laden warned affiliates in Yemen and elsewhere that it was too soon to create an Islamic state. The Saudi native, whose family had made its fortune in construction, concluded that there wasn't 'enough steel' in Al Qaeda's regional support structures to warrant even tentative steps toward reestablishing the caliphate," the daily said.

One of bin Laden's principal correspondents Atiyah abd al-Rahman, who served as No 3 in Al Qaeda before his death, expressed

concern over the US drone strikes.

"A 2010 message from Rahman expressed frustration with the CIA drone campaign, a source of particular concern because many of his predecessors in the third-ranking slot had been killed in strikes by the unmanned aircraft," it said.

"He was saying in the letter that their guys were getting killed faster than they could be

replaced," the US counter-terrorism official was quoted as saying.

Other messages sounded a similar theme. At least two came from the head of Al Qaeda's security unit, a group that had been established to protect against penetrations by informants who might provide targeting tips to the CIA, the daily said.

The unit leader complains "about having a very low budget, a few thousand dollars", the official said. "The letter refers to 'ideas' about how to better guard against informants and electronic eavesdropping. But the most obvious solutions, including restricting meetings and movements, would also hamper Al Qaeda's ability to function," the daily said. Other messages make frequent mention of the organisation's financial hardships, including emails in which bin Laden himself complains about the lack of funds.

One bin Laden message sent in spring 2010 "instructed a deputy to form a group that would get money through kidnapping and ransom of diplomats", the US official said.

"The term 'financial hardship' was used" in the message," the US official was quoted as saying.

But there are no files that provide specific figures or a comprehensive picture of Al Qaeda's financial position, the daily reported.

# The Brutal Mind of Al-Qaeda's New Boss

### By Jamie Glazov

Source: http://frontpagemag.com/2011/06/28/the-brutal-mind-of-al-qaeda%E2%80%99s-new-boss/

# Jamie Glazov is Frontpage Magazine's editor. He holds a Ph.D. in History with a specialty in Russian, U.S. and Canadian foreign policy. He is the author of the critically acclaimed and best-selling, United in Hate: The Left's Romance with Tyranny and Terror. His new book is Showdown With Evil.

FrontPage Interview's guest today is al-Qaeda expert Raymond Ibrahim. His work includes the al-Qaeda entry for the World Almanac of Islamism; an analysis of al- Qaeda's worldview for the Middle East Review of International Affairs; and most recently an article on Ayman al-Zawahiri for Bloomberg. He is best known for compiling, translating, and annotating The Al Qaeda Reader (Doubleday, 2007), the definitive work on the terrorist organization's writings. Because the book contains al-Zawahiri's premiere treatises and provides a snapshot of his mind, it takes on renewed relevance now that al-

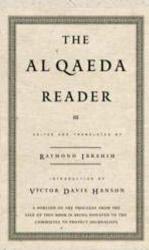


Zawahiri has been declared the leader of al-Qaeda.

**FP:** Raymond Ibrahim, welcome to Frontpage Interview. I would like to talk to you today about what you know about Ayman al-Zawahiri. But I think it would be best to begin

with The Al Qaeda Reader. Tell us what the book is about and why you wrote it. Ibrahim: Sure, Jamie. I primarily wrote The Al Qaeda Reader (AQR) to demonstrate the

organization's doubletalk. After the strikes of 9/11, al-Qaeda's messages to the West began to be translated and disseminated in the media; and their theme was one—that al-Qaeda's terrorism was in retaliation to any number of Western crimes. Then, back in 2005 when I was working at the Library of Congress, I came across unknown Arabic texts written by bin Laden and al-Zawahiri that articulated their violence and terrorism purely within a jihadist paradigm; the temporal and emotive language directed at the West, when re-directed at fellow Muslims, was discarded for the eternal and immutable language of Islam.



For example, for all of al-Qaeda's talk that Israel is the heart of the problem, bin Laden exposed his true position when he wrote to fellow Arabic-speaking Muslims not long after the 9/11 strikes the following:

Our talks with the infidel West and our conflict with them ultimately revolve around one issue—one that demands our total support, with power and determination, with one voice—and it is: Does Islam, or does it not, force people by the power of the sword to submit to its authority corporeally if not spiritually? Yes. There are only three choices in Islam: [1] either willing submission [conversion]; or [2] payment of the jizya, through physical, though not spiritual, submission to the authority of Islam; or [3] the sword — for it is not right to let him [an infidel] live. The matter is summed up for every person alive: Either submit, or live under the suzerainty of Islam, or die. (AQR, p. 42)

As you can see, this view, which is well codified in Sharia, is the ultimate source of conflict—not political, temporal grievances.

### FP: Ok, so how does al-Zawahiri fit into the AQR?

**Ibrahim:** I have always believed that al-Zawahiri was the key to understanding al-Qaeda's worldview. When I compiled the book between 2005-2006, I intentionally included more of his writings than bin Laden's (an approach deemed unconventional then, as most people were more interested in learning what the more visible and notorious bin Laden had to say). The ironic result is that today the AQR exposes the philosophy of al-Qaeda's new chief more than other al-Qaeda books, which had focused on (the now moot) bin Laden.

FP: What does the book tell us of al-Zawahiri and what can be learned from his words?

**Ibrahim:** I split the book into two sections, "Theology" and "Propaganda." In the theology section, I included three long treatises by al-Zawahiri amounting to over 100 pages:

According to his "Loyalty and Enmity" (AQR pgs. 63-115), the Muslim believer is "obligated to befriend a believer—even if he is oppressive and violent towards you and must be hostile to the infidel, even if he is liberal and kind to you." Al-Zawahiri bases this doctrine on Koranic verses that prohibit Muslims from befriending non-Muslims, specifically Jews and Christians (e.g., 5:51, 60:4).

He advocates deception, or taqiyya—that Muslims feign friendship with non-Muslims whenever it is advantageous; he quotes early Muslims saying "We grin to the faces of some peoples, while our hearts curse them" and recommending "lamenting and mourning in order to dupe the infidels."

In "Sharia and Democracy" (AQR pgs.116-136), he advocates strict enforcement of Sharia law and animosity for democracy—complaining that democracy creates "equality between the citizenry," allows freedom of religion, and abolishes "man's domination over woman."

In "Jihad, Martyrdom, and the Killing of Innocents," (AQR, pgs. 137-171), al-Zawahiri goes to great lengths to promote suicide operations, grounding them in little known hadiths and historical anecdotes, as well as Koranic verses like 9:111; he quotes Islam's prophet saying that the "martyred" jihadist "will couple with 72 maidens" in paradise. And he adheres to a very narrow definition as to who is considered "innocent" during the jihad—which precludes women, children, and even Muslims, if necessity calls for it.

The propaganda section of the book makes clear that al-Zawahiri also plays the double-talk game. For example, even though he too tries to frame al-Qaeda's terrorism as retaliation to Western aggression, when writing to Muslims he says things like

"Warfare against infidels, loyalty to the believers, and jihad in the path of Allah: Such is a course of action that all who are vigilant for the triumph of Islam should vie in, giving and sacrificing in the cause of liberating the lands of the Muslims, making Islam supreme in its own land, and then spreading it around the world (AQR, p.113)."

Note that last part about "spreading it [Islam] around the world," which again indicates that, once Islam is strong enough, it should, in accordance to Islamic law and history, go on the offensive.

**FP:** What do you think of al-Zawahiri as a leader? Do you think he'll steer al-Qaeda in a different direction than his predecessor?

**Ibrahim:** Al-Zawahiri, who just turned 60, is a seasoned veteran, who founded his first jihadi cell in Egypt when he was only 15 years-old, i.e., he's been at it for 45 years. Like bin Laden, al-Zawahiri has jihadi bona fides and served in the Afghan war, primarily as a physician; unlike bin Laden, al-Zawahiri

was imprisoned and tortured for his convictions in the early 1980s following the assassination of Anwar Sadat—an experience which seems to have hardened him more than bin Laden.

While many argue that he is lacking in charisma, it should be noted that in leadership positions in Islam, knowledge demands more authority. Even the guardians of Islam are collectively called ulema—literally, "those who know." In comparison to bin Laden, al-Zawahiri is certainly more knowledgeable—as his treatises demonstrate—and commands greater respect in this regard.

As for the direction al-Zawahiri will steer al-Qaeda, he may believe that, unless al-Qaeda steps up with something spectacular, its credibility will wane; and he only recently promised an attack of the magnitude of 9/11. Still, al-Zawahiri's 45 years of jihadi experience will probably prevent him from acting precipitously.

It also bears mentioning that because al-Qaeda has not achieved another major terrorist attack on American soil since 9/11, it does not mean that it is incapable. Moreover, it has other factors to consider. After all, if one let's their imagination stray for a bit, there are many ways to terrorize civilian populations with little chance of being caught—an especially moot point for suicide bombers. So I believe al-Zawahiri's decision to attack is guided by many factors, including the fact that another attack may undermine all the subversive efforts of his nonviolent Islamist colleagues.

**FP:** I assume you don't think the death of Osama bin Laden was as severe a blow to al-Qaeda as some portray?

**Ibrahim:** Right. Whenever a jihadist is killed—including top leaders like bin Laden—I like to point out that jihadists are not the cause of hostilities; they are symptoms of a much greater cause. Individually killing them off is like a doctor temporarily treating a sick patient's symptoms without eliminating the cause of sickness—the 1400 year-old doctrine of jihad.

Bin Laden for a decade was the face of radical Islam to the West; now it looks to be al-Zawahiri. Others—remember all the hoopla surrounding the killing of Zarqawi?—have come and gone, but the ideology is still there, still motivating others to emulate al-Qaeda.

This is also why questions concerning al-Zawahiri's popularity, charisma, and even efficacy are a bit irrelevant. Al-Qaeda's new leader himself once made this clear. Asked about the status of bin Laden and other jihadists, al-Zawahiri waxed philosophically:

Jihad in the path of Allah is greater than any individual or organization. It is a struggle between Truth and Falsehood, until Allah Almighty inherits the earth and those who live in it. Mullah Muhammad Omar and Sheikh Osama bin Laden—may Allah protect them from all evil—are merely two soldiers of Islam in the journey of jihad, while the struggle between Truth [Islam] and Falsehood [non-Islam] transcends time. (AQR, p.182)

Accordingly, as independent jihadists start taking action into their own hands—whether the Shoe Bomber, the Christmas Bomber, the Madrid and London bombers, or Nidal Hasan and Fort Hood—we must acknowledge that the very idea of perpetual jihad is more dangerous than the jihadists who come and go, be they bin Laden or al-Zawahiri.

**FP:** Raymond Ibrahim, thanks for helping to place al-Qaeda's new leader in better context for us. **Ibrahim:** Of course, Jamie; thanks for the invite.

### Belgium: Muslim extremists moving to the suburbs

Source:http://www.hln.be/hln/nl/957/Belgie/article/detail/1287767/2011/07/04/Islamitisch-extremismeniet-langer-enkel-in-grootsteden.dhtml

Manifestations of extreme Islam are now being observed not only in the big cities, but also in small towns and municipalities, according to the Belgian security service report of 2009 which was published today. religious extremism. In 2009 the security service followed the activities of diverse extreme Muslim entities: individuals, mosques, centers, groups and organization who continuously and systematically spread extremist ideas. According to the report, the most radical elements preach hatred towards.

Among other issues the report also deals with

anybody who doesn't agree with their point of view.

These extreme Muslim entities are geographically spread out more than ever before. The phenomena was observed more

# **Russian Navy captures Somali pirates**

Source: http://true-turtle.livejournal.com/85315.html

This video shows Russian Navy commandos on a Somalian pirate ship shortly after the pirates had captured a Russian oil

The soldiers freed their compatriots and the tanker. The Russian Navy Commandos moved the pirates back to their own ship, searched it

and more often in small towns

pure big city phenomenon.

municipalities, and the security service now

considers Islamic extremism less and less as a



tanker. Reportedly, the Euro Union Navy which patrols these waters would not interfere because they feared there could be casualties. All explanations are in Russian with a single exception when a wounded pirate says something in English and the Russian soldier says "You lied to me, this is not a fishing boat." All conversations between the commandos are in Russian. If you don't understand Russian, the pictures speak for themselves. for weapons and explosives which they commandeered and then left the ship and exploded it with all remaining pirates handcuffed to it.

The ship burned and sank along with the pirates and without any court proceedings, lawyers etc., using the anti-piracy laws of the 18th and 19th centuries where the captain of the rescuing ship has the right to decide what to do with the pirates. Usually, they were hung,

and





I lost metters	· Editorial triac mace	- reaches critical decision makers both in the government and the corporate world.	will continue to break new ground as defence and security perimeters expand and	- plays the leadership role in the domain of defence and security journalism.	- the first place defence and security experts, concerned citizens, researchers and students	turn for in-depth coverage of the latest developments in defence and security arena.		
	Î		Ĵ					
	Ubtar thends,	Girettings from DSAr DSA was launched in October 2009 and frankly speaking these 21 months have been a great and exciting experience for iteam DSA. Detence and Security Alert (DSA) magazine is being halled as the harbinger of a revolution in India's detence and security journalism.	For almost 80 years our group has been providing publishing solutions to renowned indian and international authors and publishing world class books on various solpicots. So far we have had the privilege of publishing over 5,000 titles. This pedigree has given us the wherewithal and confidence to sther <b>DSA</b> on the success highway. Highway a is and we are in a for the long hauf. As new challenges and opportunities becon, team <b>DSA</b> is alming at horizons beyond the national borders with vision to be the first choice in the realm of defence and security journalism for our valued readers, distinguished	As BMA covers the entire spectrum of defence and security issues and developing scenarios impacting Indian and global strategic concerns, its insightful and thought providing conterns command serious reading by the decision makers at the highest level in the government as well as the corporate work. Ensuring that these decision makers spend long enough time with DSA to notice your advertisement / message. Brief profile of our distinguished contributors is also given in the Most. Jour advertisement / DSM is the ideal platform in its genre to showcase your products, bechnologies and services. JDA is widely is these people who will guidy work makers and policy makers in the poverment and renotes. JDA is widely is these people who will guidy work works and policy makers in the poverment and renotes. JDA is widely	years ahead, <b>DSA</b> is poised not only to make your world connected with them, but also anny it closer to them and make the connection mutually rewarding. <b>Term DSA</b> stands ready with its highly dependenced editorial associates to bring you closer to and to the people who with help project and promote your company's vision more effectively and profitably. WillCome aboard! Together we can make our country and this beautital world more safe and secure.	Pawan Agrawal Publisher & CED DSM Magazine Ceo@dsalert.org	and the second	



# ICE lists Israel among countries that promote, produce, or protect terrorists

Source: http://www.homelandsecuritynewswire.com/ice-lists-israel-among-countries-promote-produceor-protect-terrorists

In May 2011 DHS released a report titled Supervision of Aliens Commensurate with Risk. The report describes the methodology on which the Immigration and Customs Enforcement (ICE) relies to arrest, detain, and, if necessary, deport undesirable aliens.

What has drawn attention to this otherwise rather dry bureaucratic report was the fact that an appendix, which is attached to the report, lists "specially designated countries" whose detained nationals should be more closely examined. The Algemeiner reports that among the countries whose nationals should be paid special attention as potential terror risks is Israel — which the report considers a "Promoter, Producer, or Protector" of terrorists ICE spokeswoman Gillian Christensen told the Algemeiner that the list was initiated at least seven years ago, and was not created by ICE. Only five countries listed do not have majority Muslim populations — but each of those five countries has had significant problems with radical Muslim terrorist groups or insurgencies — including Israel.

Christensen also told the Algemeiner that DHS list of thirty-six nations does not necessarily fault a listed government's policies, but rather, examines the possibility that a suspect from that country might have terrorist ties.

The list includes a number of other close U.S. allies, including Turkey, Bahrain, Morocco, and Philippines, as well as nations experiencing internal fighting, such as Sudan and Somalia. Israel was not on the list released in 2008, but is on the list released in 2011. ICE declined to say who put Israel on the list or when Israel was put there.

**NOTE (8 July):** DHS officials are now saying Israel's inclusion on a list of countries that promote, produce, or protect terrorists was a mistake; John Morton, director of the U.S. Immigration and Customs Enforcement (ICE), said, "The addition of Israel to the list--- was based on inaccurate information provided to the OIG during the course of its audit"; a May 2011 report contained an appendix which lists "specially designated countries" that promote terrorism; the list instructed ICE agents to pay special attention to, and investigate more thoroughly, individuals from these countries arrested by ICE; ICE spokesperson suggested that Israel was included not because its government supports terrorism, but because some individual Israelis do pose a terror threat; 1.5 million of Israel's 7.5 million citizens are Arabs (Source: http://www.ynetnews.com/articles/0,7340,L-4092186,00.html)

**NOTE 2:** You can download the report from the website hosting the Newsletter at "CBRNE-CT Papers" section.

## Germany says Islamic terrorism still a threat

Source:http://www.google.com/hostednews/ap/article/ALeqM5gfNmVypUbgXcpe\_T2OtF71SUu6oQ?do cld=735e7259d20a4449b61f954ede7a19d7

Germany's top security official said Friday that



the terrorist threat to the country hasn't

decreased and the number of radicals continues to grow, even with the death of Osama bin Laden.

Security officials saw no reason to lower Germany's threat level following the death of the al-Qaida leader, said Interior Minister Hans-Peter Friedrich (photo), presenting the annual report by Germany's domestic intelligence agency.

"The Islamist terrorist threat is widely varied and has not concentrated on a single leader of al-Qaida for a long time," he said.

"We have had a general threat situation in Germany and Europe that has not changed for two years, but there are no concrete dangers." Though there have been several unsuccessful or foiled attacks by Islamic radicals in Germany, the first fatalities attributed to a Muslim extremist came this year in March when a 21-year-old Kosovo-born ethnic Albanian allegedly gunned down two U.S. airmen outside Frankfurt's airport. Overall, the number of people in Germany "Not every Salafi is a terrorist but almost every terrorist that we are aware of has had contact with a Salafi." Fromm said.

In other findings, the report said the number of right-wing extremists dropped to 25,000 last year from 26,600 in 2009 — but the number considered to be neo-Nazis rose to 5,600 from 5,000.

About one-fifth of the neo-Nazis are now considered part of a growing group of violence-prone extremists who target leftist radicals,



# Küresel emperyalistlere karşı dik durmak demektir...

linked to radical Islamic groups rose to 37,470 in Germany in 2010, up from 36,270 the year before, according to the report from the Office for the Protection of the Constitution.

Most of those — 31,370 — were connected to Turkish groups, nearly all of them in **Milli Gorus**, a group whose founder advocates creating an Islamic state in Turkey.

Most worrying was the increase in numbers in "Salafi" groups that espouse an ultraconservative interpretation of Islam and have been especially successful at recruiting young people, said Heinz Fromm, who heads the domestic intelligence agency.

He noted that the suspect in the March killing of the two U.S. airmen outside Frankfurt's airport had allegedly been inspired by watching Salafi videos online. Friedrich said.

"Their target group is no longer foreigners, but political enemies," he said.

Incidences of right-wing criminality dropped to 15,905 in 2010 from 18,750 in 2009 — or 4,521 cases in 2010 when excluding "propaganda" crimes like the scrawling of swastikas or other banned symbols on walls.

By contrast, far-left criminality, for which there is no "propaganda" category, was down to 3,747 in 2010 from 4,734 in 2009.

Friedrich warned, however, that a spike in leftist criminality — such as the torching of cars in Berlin and elsewhere and attacks on police — in the first five months of 2011 indicate that that drop was an anomaly.

The number of left-wing extremists grew to 32,200 last year from 31,600 in 2009. That included a rise to 6,800 violent radicals from 6,600 the previous year.

### Somali Piracy becoming an industry

Source: http://www.timeslive.co.za/africa/2011/07/01/somali-piracy-becoming-an-industry

Somali pirates are taking 'f piracy to an industrial scale' says Pottengal Mukundan, director of the International Maritime Bureau's piracy reporting centre. The centre has been for 61 percent of all attacks on ships, with 362 crew members taken hostage, he said. Mukundan said Somali pirates were still holding 21 vessels and 405 hostages for



monitoring incidents worldwide since 1991. Mukundan said the pirates were using hijacked vessels as bases to extend their range of operations against ships in the Indian Ocean, Arabian Sea and Gulf of Aden.

In March the Indian navy captured 61 heavily armed pirates aboard a hijacked Mozambiqueflagged ship in the Arabian sea which was being used as a mother-ship.

Piracy has surged in recent years off Somalia, a lawless, war-torn country that sits alongside one of the world's most important shipping routes.

The IMB is concerned that some countries which have deployed naval assets off the Horn of Africa may cut their anti-piracy surveillance in the area.

### The impact

Mukundan, who is based in London, told AFP that so far this year there were 162 attacks off Somalia with 21 ships captured. Hijackings off the coast of the east African country accounted ransom. "Since 2007 there has been 62 fatalities as a result of piracy," he said, adding that "the situation is getting very serious." "We are calling for more naval ships be made available to protect ships off Somalia," he said. Mukundan said this year despite the monsoon period (June to August), Somali pirates had escalated their attacks off the Gulf of Aden. "It is an important shipping lane for very large crude carriers which sail from the Arabian Gulf to Asian countries such as Japan, China and Singapore," he said. In previous years, there was a respite in attacks during the monsoon period due to strong winds and heavy seas.

### Violence and ransoms rise

Mukundan said another worrying trend was the increase in violence against seafarers and hostages in the past six months.

In one incident, Mukundan said two senior officers were put in a ship's meat storage refrigerator for 40 minutes and in another case pirates carried out mock executions. "The violence and threat used is unprecedented and unacceptable," he said. Mukundan warned that.

the IMB expects the number of attacks to be higher than last year. "Pirates are getting more ransom, so they are escalating their attacks," he said.

Mukundan urged countries to prosecute pirates captured at sea and not to release them. "We

want captured pirates to be prosecuted and punished. Now more than 80 percent of the captured pirates are freed. It is sending the wrong signal to the pirates," he said.

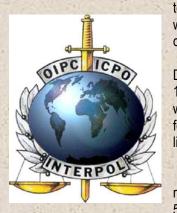
# EUROPOL: TE-SAT 2011 – EU Terrorism Situation and Trend Report

Source:

### Key judgements

### The threat of attacks by Islamist terrorists in the EU remains high and diverse.

In the past year, several EU Member States have successfully prevented attacks by Islamist



terrorist groups, which aimed to cause mass casualties. During 2010. 179 individuals arrested were for offences linked to Islamist terrorism. representing a 50% increase

compared with 2009. Furthermore a higher proportion of those arrests related to the preparation of attacks in the EU (47% compared with 10% in 2009). Additionally, the high number of threat statements to the EU (46) posted by Islamist terrorist organisations or their media fronts indicates terrorist groups' clear intent to target the European Union.

Islamist terrorist groups are changing in composition and leadership. Terrorist groups are becoming multi-national, command and control from outside the EU is decreasing and more lone actors with EU citizenship are involved in terrorist activities.

**Returning jihadists from conflict zones** continue to be a threat to the EU. They return with specific contacts, skills and modi operandi, and the potential intent to apply these in EU Member States. The political situation in the Northern Caucasus is increasingly reflected by the activities of members of the Caucasian diaspora in the EU, supporting activities of terrorist groups in the Northern Caucasus financially and otherwise. The turmoil in North Africa that began in January 2011 is likely to impact al-Qaeda's core and affiliated organisations, in both the short and long term. The current situation could lead to a setback for al-Qaeda but it could also result in more powerful terrorist organisations impacting the EU, and an increase in the radicalisation of individuals both in North Africa and the EU. In the short term, the absence of terrorist organisations amongst the mass Arab protests across the region has left al-Qaeda struggling for a response. Should Arab expectations not be met, the consequence may be a surge in support for those terrorist organisations. and an increase in radicalisation, both in North Africa and elsewhere. The current and future flow of immigrants originating from North Africa could have an influence on the EU's security situation. Individuals with terrorist aims could easily enter Europe amongst the large numbers of immigrants.

Although the goals of terrorist and organised crime groups (OCGs) are different, the connections between terrorist and organised criminal activities appear to be growing. Crime is being extensively used to finance terrorist activities. Criminal activities that terrorist groups are involved in, either through affiliation with individual criminals and criminal groups or through their own operations, can include the trafficking of illegal goods and substances such as weapons and drugs, trafficking in human beings, financial fraud, money laundering and extortion. Separatist terrorist groups such as the PKK/KONGRA-GEL and LTTE are involved in the trafficking of drugs and human beings to raise funds for their terrorism activities.



Separatist and ethno-nationalist terrorist groups rely substantially on extortion to finance their activities. It is unlikely that ceasefire declarations by separatist terrorist groups will mark the end of terrorist attacks or activities. In 2010, 123 individuals in France and 104 in Spain were arrested on terrorist offences related to violent separatist activities. These figures represent a decline from 2009 levels.

The economic recession is conducive to political tensions and. in a number of Member States, is triggering both leftand right-wing extremists to demonstrate their views both on the recession's causes and on the solutions required. This is raising public order



concerns and threatening social cohesion. Growing unemployment, especially among young people seeking to enter the job market, has radicalised some youths, even those with relatively high levels of education. In 2010, 45 left-wing and anarchist attacks occurred. The increased use of violence led to six fatalities. Evidence shows increased international cooperation between terrorist and extremist groups in and outside the EU. Left-wing, but also separatist groups, are collaborating

internationally. During 2010, clear links between ETA and FARC were determined. The coordination of activities is greatly facilitated by the wide availability of online communication tools and applications, and the rise of social media. The professionalism of right-wing propaganda shows that right-wing extremist groups have the will to enlarge and spread their ideology, and still pose a threat in EU Member States. If the unrest in North Africa leads to a major influx of immigrants into Europe, **right-wing terrorism** might gain a new lease of life by articulating more widespread public apprehension about immigration.

> In 2010, protests by singleissue extremist groups increasingly focused on the fur industry. These groups are becoming increasingly network-based- they use various methods of communication to prioritise, coordinate and support direct action. Campaigns of **animal-rights** activists indicate a shift of activities

from the UK towards the European mainland which started in 2008/2009 and continued in 2010. There are indications that some members of animal rights, anarchist and environmental extremist

groups are moving towards a shared ideology. Environmental extremism is on the increase.

Terrorist and extremist groups are demonstrating increased professionalism in using web-based technologies to present themselves and communicate their ideologies to a larger audience. The **internet is developing into a crucial facilitator** for both terrorists and extremists.

**NOTE:** You can download the report from the website hosting the Newsletter at "CBRNE-CT Papers" section.

# Is AI Qaeda Planning Terrorist Attack on AeroVironment Inc? Here's the L.A. County Firm's 5 Coolest Spy Drones

Source:http://blogs.laweekly.com/informer/2011/07/al\_qaeda\_planning\_terrorist\_attack\_on\_aerovironm ent\_inc\_spy\_drones.php



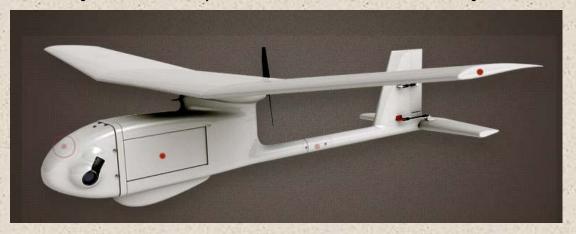
Reports abound this morning of a possible Al Qaeda attack plan against 11 officials at L.A. County's own AeroVironment Inc., a top drone manufacturer in the U.S. War on Terror. Employees of the Monrovia company tell the San Gabriel Valley Tribune they were called into a meeting Thursday afternoon and watned.

that the FBI was looking into a terrorist plot against AeroVironment -- part of the retaliation miniature robotic [unmanned aerial vehicles, or UAVs] like the Raven, Wasp and Digital Puma



effort against Osama Bin Laden's recent U.S. assassination. Creepy stuff. After combing an Al Qaeda-linked jihadist hit

that are being used over the battlefields in Afghanistan in the US-led war on Al Qaeda and the Taliban. The firm is the largest maker of the



list online, the Homeland Security Today blog confirmed:

tiny drone spy planes that are being used in the Global War on Terrorism (GWOT).



In addition to the top US military leaders targeted by AI Qaeda sympathizers, 11 top and senior executives of AeroVironment Inc., including CEO Timothy Conver, were identified by the jihadist forums members. ... AeroVironment manufactures the thousands of

Al Qaeda has every reason to hate AeroVironment execs: They're thinking up some of the nation's most advanced antiterrorist technology at a time we need it most (because romping around in the desert with an AK-47 doesn't always do the trick).



And given an attack is (hopefully) averted by the FBI, the Al Qaeda threat might be considered bragging rights for a cutting-edge drone manufacturer like Monrovia's. In honor of their badassery (forgive the barfy patriotism; this Fourth of July business is really getting to us), here are the five coolest spy bots being birthed over in east County right now:

5. The Global Observer is the hugest of the company's UAVs. Instead of buzzy street-level

spying (and we'll get to that), the unmanned Observer satellite floats 5,000 feet above Earth, providing "a 24/7/365 unblinking eye and continuous communications link over any location on the earth's surface for as long as needed."

4. Moving a bit closer to Earth but gliding far enough above to avoid enemy detection, the Raven, a small plane with 4.5-foot wingspan, can focus on land targets up to 10 kilometers down. In the day, it sends back exceptionally clear color imagery, and it's not so shabby by night.

3. Though this guy looks more like an old Amelia Earhart relic, AeroVironment's water-friendly

Puma is all parts 21st century. It can communicate up to 15 kilometers away, fly with almost no noise for two hours straight and can land on virtually any surface, free of gear.

2. The Wasp, weighing only 430 grams, is designed for front-line surveillance.

Awesomely, he (yes, we're sexist when it comes to UAVs) can either be controlled manually or left to navigate the warzone on his own. He can even dodge a bird of prey's most carnivorous advances.

1. By far the most inconspicuous of AeroVironment's war gadgets, the Nano Hummingbird got big press early in 2011 for its creepy realism and insane superpowers, like



an "autonomous 360 degree lateral flip." Pretty hardcore for an iridescent flower flitter.

Now that the tech company itself looks to be a terrorist target, it might think about putting some of its military dronage to personal use. Any former U.S. Defense Secretaries looking for a retirement project?









Petty Officer Jon Tumilson, 35, killed in a major U.S. helicopter crash in Afghanistan. Jon's Labrador retriever Hawkeye was loyal to the end, as he refused to leave his master's side during an emotional funeral





# Al-Qaeda's Egyptian Ideologues Planning Caliphate's Return to Egypt

## By Hani Nasira

Source: http://www.jamestown.org

While al-Qaeda focused on the global jihad under the leadership of the late Osama bin Laden, an examination of the speeches and publications of his Egyptian successor, Dr. Ayman al-Zawahiri, show that renewing his own failed jihad in Egypt has never been far from al-Zawahiri's mind.

- In speeches delivered before February 2010, al- Zawahiri mentioned Egypt 226 times, second only to the United States (mentioned 636 times).
- Al Zawahiri recently released the last in his six-part series about Egypt titled "The Message of Hope and Good Tidings for Our People in Egypt." The last four of its six parts focused on the Egyptian Revolution and ex-president Hosni Mubarak.
- In The Exoneration, his last and most important book, al-Zawahiri referred to Egypt 195 times and Mubarak 41 times while referring to Saudi leaders only once and the Kingdom not at all. The United States was mentioned 150 times. [1]

These works reveal the central position of Egypt in al Zawahiri's thought and suggest the direction al-Qaeda may take now that al-Zawahiri has assumed leadership of the movement.

Conditions in Egypt now provide a suitable environment for al-Qaeda following the chaos in the internal security services, the rise of Salafist movements and the release from detention of a number of jihadi ideologues and the return of others from abroad. Al-Zawahiri may see a golden opportunity to renew jihad activities in Egypt after he was forced to suspend the activities of the Egyptian Jihad movement in 1995 due to the movement's inability to cope with severe pressure from the Egyptian security forces.

Al-Qaeda is expected to witness a new phase of activity coinciding with the popular Arab revolutions that may see the movement grow stronger due to al-Zawahiri's pragmatism and deep and effective relations with a number of al-Qaeda sub-organizations in the Maghreb, the Horn of Africa, Iraq and the Arabian Peninsula.

Al-Zawahiri claims to support the revolutions in Syria, Libya and Yemen, insisting they will result in an Islamic state with the help of an alliance of Islamist and jihadist groups. The al-Qaeda leader's views are mirrored in the works of Anwar al-Awlaki on the Yemeni Revolution and those of Attiya Allah al-Libi on the Libyan Revolution (for Attiya, see Terrorism Monitor, August 12, 2010; June 9).

A process of ideological reconsideration is taking place in Egypt's Salafist leadership. Some have opted for political action while others have announced they will focus on the Islamic Call. All of them stress the need for an Islamic state and Shari'a rule.

This process requires very little departure from the decisions adopted by many of the Islamist movements in Egypt to renounce violence since 1997. Nonetheless, the debate within the Egyptian Islamic Group over its future course has ended with the departure of a number of its historically prominent leaders and the appointment of cousins Aboud and Tarek al-Zomor as new leaders. The two were freed from three decades of imprisonment during the revolution after being connected to the assassination of President Anwar al-Sadat in 1981. [2] Despite describing al-Zawahiri as "a man who loves his religion and justice," the cousins have been eager to reassure Egyptians that they have renounced violence and believe the Islamic state in Equpt will be established "at the ballot box" (The Daily News Egypt, March 21).

Al Zawahiri's view of the Arab revolutions and the role of Islamists and mujahideen were outlined in his series "The Message of Hope and Assurance for Our People in Egypt." In his perspective, America retreated from supporting the overthrown leaders in Tunisia and Egypt as a result of al-Qaeda's activities. Al-Zawahiri also warned of "predators" who would seek to manipulate the revolutions in their own interests and insisted that "secular change" was not an option for the people of Egypt, claiming Shari'a has been the demand of the vast majority of Egyptians since the death of: Muslim Brotherhood founder Hassan al-Banna in 1949.

Perhaps in keeping with the revolutionary demands for social reforms, al-Zawahiri also addresses "social injustice" in a nationalist fashion unfamiliar to most Salafi-Jihadi literature:

"Egypt must begin a popular campaign to regain the Egyptians' rights, especially those of the impoverished, and this campaign must seek to uproot the social injustice, poverty, needs and short-handedness in Egypt. Islamic advocacy must consider the social justice cases as one of its main priorities. The Prophet (p.b.u.h.) said: "the believer is one who doesn't feel fed while his neighbor is hungry next to him." The zakat obligation must be revived... Stealing Egypt's resources must stop, and the clearest example is exporting gas to Israel, which the Egyptian judiciary ruled on and disallowed, and in spite of that the military council keeps exporting it to Israel" (As-Sahab Media/al-Fajr Media Center, May 21).

Al-Zawahiri has repeatedly warned of U.S. attempts to install a secular leader in Egypt after having abandoned its ally, first in a February 28 statement, again in two parts of "The Message of Hope and Assurance for Our People in Egypt," and finally in "The Noble Knight Alighted," his June 8 eulogy of Bin Laden. Al-Zawahiri has highlighted in various speeches the need to prepare for an Islamic state after these revolutions and the importance of making alliances with other Islamic forces in revolutionary countries to prevent the establishment of a secular state. Explaining this vision was a recent essay

released by al-Qaeda entitled "The People's

Revolution and the End of Forced Rule" (al-Fajr Media Center, June 1). The document was written by Egyptian al-Qaeda member Abu Ubaydah Abdallah al-Adm, who appears to be very close to the movement's high command. The essay outlines a strategic vision for al-Qaeda in dealing with the popular revolutions and interpreting them in a religious way favorable to the various Islamist movements, especially those with a focus on restoring the Islamic state (the Caliphate), such as al-Qaeda and Egyptian Jihad.

In his paper, Al-Adm explains that the revolutions and overthrow of regimes represent the end of forced rule or tyrannies, a phase that followed the eras of the prophets and Caliphates. Al-Adm believes that these revolutions hasten the arrival of the Islamic state, though he notes that the establishment of such a state may be preceded by a period of chaos – possibly as long as 50 years, as suggested by Syrian jihad theorist Mus'ab al-Suri (a.k.a. Mustafa Setmariam Nasar). In al-Adm's view, God has driven these revolutions, supporting the mujahideen as the Muslim people wake up to reject everything else but Islamic Shari'a.

At the end of the paper, al-Adm emphasizes that "The Global Jihad Movement, no doubt, is waiting for the fruits of this popular movement in which it sacrificed the blood of its members and spent decades calling for it and fighting to plant the idea in the minds of Muslims who rose up today demonstrating [against] the tyrannical oppression they used to face. Al-Qaeda paved the way for these revolutions and waits for its fruits..."

### Notes:

1. Al-Zawahiri's book (Full title: A Treatise Exonerating the Community of the Pen and the Sword from the Debilitating Accusation of Fatigue and Weakness) was a March 2008 refutation of a book entitled Tarshid al-amal al-jihadi fi misr wa al-alam (Rationalizing the Jihadi Action in Egypt and the World) by the imprisoned founder of the Islamic Jihad organization, Sayed Imam Abdulaziz al-Sharif (a.k.a. Dr. Fadl). (See Terrorism Focus, April 30, 3008).

2. http://www.egyig.com//Public/articles/announce/index.shtml.

Hani Nasira is an Egyptian writer who specializes in ideological movements.



## Google Earth is Used by Terrorists

### By Matthew Uhlmann

Source: http://www.deathandtaxesmag.com/114992/google-earth-is-used-by-terrorists/

Say you plugged any random US city into Google Earth. Next, you plugged in the Israeli

satellite technology. It can be used to explore distant neighborhoods when apartment



town of Netivot, which borders the Gaza Strip to the east. You would notice that in comparison the image of Netivot is quite pixelated and blurry. It's because of the 1997 National Defense Authorization Act that the entirety of Israel can only be viewed in lowresolution.

### There's a good reason for this.

Palestinian fighters are pretty creative. In an interview with Slate, a Gaza militant explained how they use Google Earth to aim the infamous homemade Qassam rockets and Soviet-era Grads into the Israeli border towns surrounding the blockaded Gaza Strip. It's unclear exactly how the rudimentary artillery placement works, only that the Google program, despite its highly pixelated imaging of Israel, is used to locate targets.

### Does this mean that Google Earth is evil?

The software is a fantastic tool when not used maliciously. It allows all of us to momentarily make believe that we're spies with access to hunting. It can be used to keep tabs on an exgirlfriend's front driveway, to see if some other dude's car is parked out front (which I've never done).

Google Earth gives new potential to entertainment for the virtual globe trotters among us. It was the main tool used to build Arcade Fire's "The Wilderness Downtown" project last year, which totally reoriented the music video as we knew it. (For the first time in the history of internet advertising, the online interactive music video actually made entertaining use of the online pop-up.)

No, Google Earth isn't evil. But the best programs always seem to attract the biggest bastards who swoop in and tarnish all that's good about the internet.

Remember when online instant messaging came out? It was the grandfather of Facebook and it was fantastic—as were those online chat rooms where lonely people with common interests could all talk amongst themselves, anonymously. But then online predators ruined

it. One never knew if that person who claimed to be a 15 year-old kid was really some middleaged man living in his parents' basement. Google Earth and instant messaging are entirely different beasts. But what they both can do is make the world we live in feel smaller than it really is, less alienating, and more manageable. But while those among us like Arcade Fire will use tools like Google Earth to take viewers on a heart-warming virtual trip home, there's always someone else waiting to use that same tool to aim rockets into the sides of school buses.

As it's always been, I guess that's the price we pay for new technologies.

# Dewsbury, Bradford and Tower Hamlets ... where Islamic extremists want to establish independent states with sharia

#### law

Source: http://www.dailymail.co.uk/news/article-2011433/Islamic-extremists-set-independent-states-UK-fall-Shariah-law.html#ixzz1SKvmhLTb

Islamic extremists have called on British Muslims to establish three independent states



within the UK.

The notorious Muslims Against the Crusades (MAC) group have named Yorkshire towns Bradford and Dewsbury and Tower Hamlets in



East London as testbeds for blanket sharia rule.

The medieval 'emirates' would operate entirely outside British law, according to a document on the MAC website.

Veiled women in the London borough of Tower Hamlets which has seen a rise in extremism. The Muslims Against the Crusades group says the medieval 'emirates' would function as autonomous territories and operate entirely outside British law, according to a document published on their website

The MAC group, led by Abu Assadullah, was set up last year and has become notorious because of its violent protests, most provocatively burning poppies during the Remembrance Day silence.

Under the heading 'Muslims should set up Islamic emirates in the UK', MAC says: 'We suggest it is time that areas with large Muslim populations declare an emirate delineating that Muslims trying to live within this area are trying to live by the sharia as much as possible with their own courts and community watch and schools and even self sufficient trade.

'Likely areas for these projects might be Dewsbury or Bradford or Tower Hamlets to begin with.

'In time we can envisage that the whole of the sharia might one day be implemented starting with these enclaves.'

The call is likely to cause anger among moderate Muslims and community leaders in the areas concerned.

Ian Greenwood, leader of Bradford Council, said people would 'not allow extremists to provoke them into violence'.

London 7/7 bomber Mohammad Sidique Khan



lived in Dewsbury, which has battled to diffuse extremism in recent years. In 2007, it was alleged that a number of Muslims in Dewsbury were running an illegal Islamic court from a school and similar claims have been made in Tower Hamlets and Bradford.

Tower Hamlets council was last year accused of falling under the control of extremist groups following a documentary by the Daily Telegraph journalist Andrew Gilligan.

The plan is part of the MAC's response to the government's revised Prevent strategy to combat Islamic extremism.

A general view of Bradford in Yorkshire which Muslims Against the Crusades (MAC) group have named as one of three testbeds for blanket sharia rule

In its document, called Islamic Prevent, the fanatics also call for an end to CCTV cameras in and around mosques.

It says: 'Muslims must get rid of all CCTV cameras from Muslim institutions. Sadly many mosques have today adopted CCTV cameras to spy on Muslims on behalf of the police and local authorities.'

Other inflammatory instructions include demanding the release of all Muslim prisoners, a ban on Muslims joining the police or armed forces and a rejection of British democracy. The document ends: 'We can conclude that measures by the UK government are nothing more than an attempt by them to strip the Muslim community of their Islamic identity and to integrate them into the non-Islamic way of life.'

The revised Prevent programme, announced last month, is aimed at tackling home-grown terrorism and radicalisation of students.

It demands stricter controls on extremist literature and a more proactive approach by universities to prevent extremism.

Councillor Greenwood added: 'Extremism is less likely to emerge when people get the opportunity to come together.

'Local voluntary, community and faith groups, the council, and other public and private sector



partners, all work together in Bradford to strengthen community relations and encourage better understanding and respect between all our communities.

'We believe that this is one of the best ways to build a tolerant society in which extremism plays no part.'

Tower Hamlets and Kirklees Council, the local authority for Dewsbury, refused to comment.

#### **Exploring Memories Of The London Bombing**

Source: http://www.medicalnewstoday.com/releases/230618.php

Six years on from the devastating 7/7 London bombings and in the wake of the inquest into the attacks, a special issue of the journal Memory Studies, published by SAGE, explores new research into our collective memories of this tragic event.

"The London attacks make for a particularly

compelling case study of contemporary remembrance and commemoration," say authors of the lead editorial, Matthew Allen and Annie Bryan. "Significantly, it would seem that a wider social project of remembering the bombings is at odds with the inquest's aim of providing an official, finalized historical account of 7/7."

The three-year UK Arts and Humanities Research Council (AHRC)-funded research project set out to pioneer the study of masscommemoration. Researchers mediated analyzed both media coverage of the bombings, and personal memories of the events as part of the project, entitled Conflicts of Memory: Mediating and Commemorating the 2005 London Bombings.

Where commemoration results from social engagement, memorialization involves using

the media as a memory aid. Indepth analysis of television coverage both immediately following the event and the coverage of commemorative events a year later revealed interesting shifts.

In the paper **Dynamics** of

memory: Commemorating the 2005 London bombings in British television news, Nuria Lorenzo-Dus and Annie Bryan explore how images of the bombings as they unfolded shot on mobile phones spread rapidly around the globe, first via social media and then through more traditional media channels such as newspapers and television coverage. However the authors show that, despite this apparent breakthrough for citizen journalism, the mainstream media re-asserted generic conventions for coverage a year later. The camera-phone images were then displaced from commemorative programming by the theme of commemoration itself, as media channels gave a high news value to personal accounts of the events and to the theme of trauma a year on.

Anna Reading discusses in the paper The London Bombings: Mobile Witnessing, Mortal Bodies and Globital time how mobile phones represent not just the ultimate in convergence of digital media technologies in the early part of the 21st century but also a personal and globally networked prosthetic to human

memory. She compares media accounts of the 2005 bombing with a bombing of the London Underground in 1897 to explore the different time frames through which media technologies communicate, witness and commemorate public memory.

She argues that mobile and networked media appear to compress the time between the instant, the moment of the event and the instances, the repeatable moments in which that instant can be communicated. With mobile technologies images can be captured by

> witnesses and rapidly and widely circulated and reassembled across different connected media, dynamically traversing the private and public memory in new ways. But time, she argues, is not only compressed, since the process of

commemoration

of the terrorist atrocity also has its own time (s) tied to dates such as anniversaries and to events such as the Coroner's inquest with the London bombings. While the rapidity of mobile witnessing was important at the time, it is the slower mediated narratives of survivors, witnesses and rescuers from the coroner's inquest that help us understand the scars that remain to the mortal body over time.

These two papers form part of a series of articles in this special issue of Memory Studies resulting from the research project which explores some of the debates generated by the London bombings, illustrating the range of disciplines that can be brought to bear on the many issues and perspectives surrounding this event.

The London bombings: Mobile witnessing, mortal bodies and globital time by Anna Reading, London South Bank University, UK and University of Western Sydney, Australia and Dynamics of memory: Commemorating the 2005 London bombings in British television news by Nuria Lorenzo-Dus and Annie Bryan



Swansea University, UK, are published in

Memory Studies.

#### The Dog That Cornered Osama Bin Laden

Source: http://blogs.canoe.ca/parker/general/the-dog-that-cornered-osama-bin-laden/

When U.S. President Barack Obama went to Fort Campbell, Kentucky, last week for a highly publicized but very private meeting with the commando team that killed Osama bin Laden, only one of the 81

members of the super-secret SEAL DevGru unit was identified by name: Cairo, the war dog.

Cairo, like most canine members of the





elite U.S. Navy SEALs, is a Belgian Malinois. The Malinois breed is similar to

German shepherds but smaller and more compact, with an adult male weighing in the 30-kilo range.

#### Trends in Global Violence and Norway's Peace Diplomacy

#### **By Andrew Mack**

Source:http://www.regjeringen.no/nn/dep/ud/kampanjer/refleks/innspill/engasjement/mack.html?id=4927 50

At the end of 2006 just 32 armed conflicts were being fought around the world in which a government was one of the warring parties This was some 40% fewer than the post-World War II peak in 1992. High-intensity conflicts those with at least 1000 battle-related deaths a year—declined by 72% over the same period.

During the Cold War years the number of armed conflicts more than tripled, rising inexorably decade by decade.

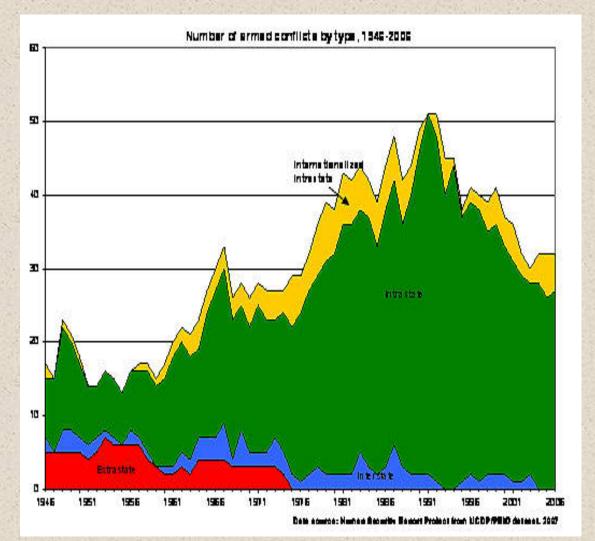
Most of the conflicts in the period under review were fought within states (the green band) in Figure 1 below. Interstate wars (blue band) have only been a small proportion of the total, while wars of colonial liberation (red band) were virtually over by the end of the 1970s.

The yellow band—'internationalised intrastate conflicts'—indicates the number of conflicts fought within a state but with military involvement from other states. The fighting in the Democratic Republic of the Congo at the

end of the 1990s and early in the new

Millennium is a case in point.

Figure 1



Some observers doubt that there has been a real improvement in global security and have suggested that while the number of conflicts may have decreased, their deadliness has increased—i.e., fewer wars, but more deaths.

This is not the case. In fact, the decline in the deadliness of armed conflict has been even greater and over a longer period than the decline in conflict numbers as Figure 2 below shows.

The average number of battle-related deaths per conflict in 1950 (the deadliest year with 700,000 plus deaths) was about 37,000; in 2006 it was little more than 500. This decline reflects changes in the nature of warfare—a

move away from major conventional wars fought with heavy weapons to so-called 'lowintensity conflicts' fought with small armies, light weapons, and few military engagements.

There have also been a number of short-lived, low-casualty, high-tech conventional wars fought by the US and its allies since the end of the Cold War—Gulf War I, Kosovo, Afghanistan and the conventional phase of the most recent Iraq war. In each case the US and its allies quickly prevailed over their weak opponents with relatively few casualties. Where the US has sought to fight insurgents on their own terms—from Vietnam to the current insurgency in Iraq—casualties have been high and victory illusive.



000	Number of batt	
020		■6. C-& S-Asia ■5. Americas ■4. Sub-Saharan Africa ■3. East-& SE-Asia-and-Oceani ■2.MENA ■1. Europe
000	λ	
009		
~		

However, the trend data in Figures 1 and 2 only deal with conflicts in which a government is one of the warring parties. They tell us nothing about the many armed conflicts fought between communal groups, militias, warlords and others—cases of armed violence with no direct government involvement. Until relatively recently no research institute collected data specifically on these 'non-state' conflicts.

Since 2002, however, Uppsala University's Conflict Data Program has been collecting data on 'non-state' conflicts for the Human Security Report. In that year there were actually more non-state conflicts than those involving a government (36 versus 32)—though death tolls were (and have continued to be) considerably lower.

Since 2002, there has also been a startling 33% decline in non-state conflicts. This has been driven by the remarkable, but largely unacknowledged, improvement in security in sub-Saharan Africa, where the number of non-

state conflicts dropped from 26 in 2002, to 12 in 2006—a 54% decline.

This improvement was also evident with respect to African conflicts in which the state was one of the warring parties. Here the change was from 12 in 2002 and 9 in 2006. The death tolls from these non-state conflicts have also declined significantly over the past four years.

The decline in armed conflicts has been mirrored by a sharp drop in the number of genocides and other campaigns of mass violence—mostly directed at civilians. Most such slaughters take place in the context of high–intensity conflicts. So it is not surprising that while the latter has declined by 72% since the end of the Cold War, the former should have declined by 80%.

This extraordinary reduction in all forms of armed conflict remains one of the leastexamined major security changes of recent.

Figure 2

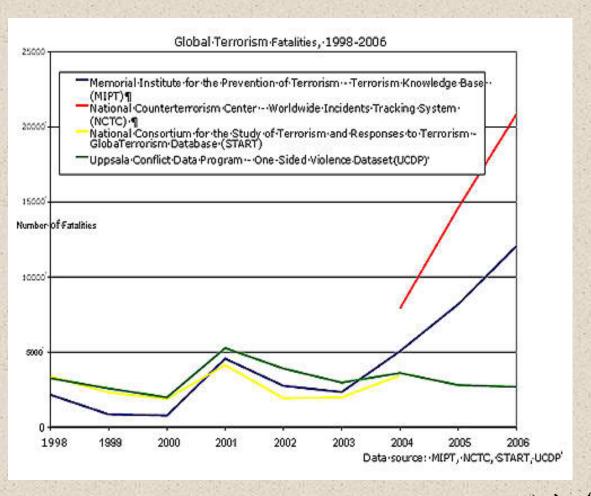
times. Not one full-length study has been devoted to explaining it. Indeed the very fact that there has been a decline is still cause for surprise—and skepticism—in some guarters.

#### Terrorism

The one apparent exception to this encouraging trend is terrorism. The official US National Counterterrorism Center (NCTC) shows the number of terrorist fatalities worldwide increasing from 4,911 in 2004, to 20,840 in 2006—an increase of more than 400% in two years.[1]

NCTC, which was created following major criticisms of the State Department's 'Patterns of Global Terrorism' dataset, only has data from 2004 to 2006. The Memorial Institute for the Prevention of Terrorism (MIPT), which is funded in part by the US Department of Homeland Security, has data—for domestic as

well as international terrorism-going back to 1998. MIPT's dataset shows global fatalities from terrorism increasing from 2,346 in 1998 to 12.065 in 2006, an increase of more than 500%. The apparently steep increase in the fatality toll from terrorism is not the only reason for concern. The Islamic terror groups that are perceived as the major threat are wellorganized and well-funded. Their members are resolutely committed to the cause, they have a substantial base of support around the world. their networks have a global reach, they communicate and propagandize via hundreds of radical Islamic websites, and they have launched major terror attacks on six continents. Terrorist weapons systems are becoming more sophisticated and lethal and this, together with increased resort to suicide missions, has driven the death rate per terrorist incident sharply upwards over the past ten years. Some analysts believe it is simply a matter of time before terrorists obtain weapons of mass destruction.



www.cbrne-terrorism-newsletter.com



#### Figure 3

The NCTC (red) and MIPT (blue) trend lines in Figure 3 not only support the contention that the threat of global terrorism has increased,[2] they also suggest that what the Bush Administration calls the Global War on Terror is failing.

However, the other two datasets tell a very different story. The yellow trend line is plotted from the new START dataset created by a research team at the University of Maryland. It records fatality data from 1998 to 2004.[3] START is also funded by the US Department of Homeland Security. The START yearly trend data (which are only available up to 2004) reveal far fewer fatalities from terrorism worldwide than NCTC and MIPT. More importantly, the fatality trend from 1998 to 2004 reveals only a relatively minor increase.

The green trend line is derived from a dataset

collated by Uppsala University's Conflict Data Program that tracks 'one-sided violence' politically motivated fatal attacks on civilians by non-state groups. This definition is very close to most definitions of terrorism.[4] Uppsala's data show a modest net decline from 1998 to 2006. If Iraqi fatalities from terrorism are removed from the datasets the picture changes dramatically as Figure 4 below demonstrates. This is not surprising. MIPT claims that in 2006 a remarkable 79% of the world's fatalities were in Iraq; NCTC puts the figure at 65%.

With Iraq out of the equation, the NCTC and MPT fatality levels for the rest of the world drop dramatically. The three datasets that go back to 1998 now reveal either a net decline in annual fatalities (Uppsala and START), or only a very modest increase (MIPT). Only NCTC shows a major increase (approximately 50% between 2004 and 2006) in fatalities.[5]

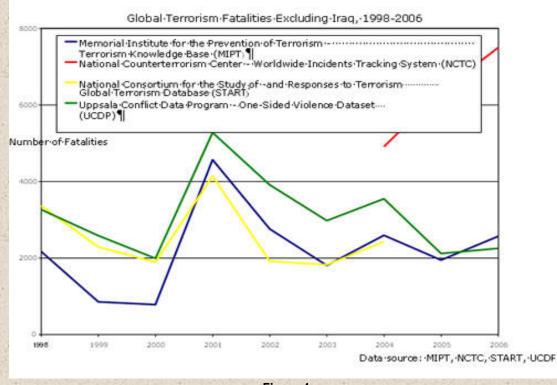


Figure 4

The difference between the global trend graphs with and without Iraq, clearly indicates that both NCTC and to a lesser degree MIPT, are counting as terrorist victims a very large number of the civil war deaths in Iraq. Defining sectarian and militia violence against civilians in a civil war as terrorism is unusual—and controversial. As a recent US Congressional Research Service report noted that:

"Some would argue ... that NCTC data concerning Iraq casualties—which are large

the product of sectarian violence, rampant criminal activity, and home–grown insurgency—grossly distort the global terrorism picture and perhaps should not be attributed to terrorist activity."[6]

The deliberate slaughter of civilians in the context of a war is usually described as a war crime, not terrorism. Indeed, Alex Schmid, former head of the UN's Prevention of Terrorism Branch in Vienna, has defined terrorism as the "peacetime equivalent of a war crime[7].

The controversial claim that Irag is the locale of 65-76% of the world's terrorist fatalities has obvious political implications. Critics can and have used MIPT data to argue that the war on Iraq has created a massive and everincreasing terrorist threat where previously none existed. But official Washington can also use the data to support Administration assertions that terrorism in Iraq is a major threat to US-and global-security. If we reject the conflation of war deaths in Iraq with terrorist fatalities, the global threat from terrorism appears far less alarming than that so often portrayed in the media. To put the terrorist toll in perspective, the average global fatality estimate for 2004 (less Iraq) is just over 4,000. This is one tenth the number of road deaths in the US and around one quarter the number of American homicides.

#### **Future Threats**

The data reviewed in this short paper suggest that there has been a major reduction in armed conflicts since the end of the Cold War and an even greater reduction in battle-related deaths over a longer period. This has been complemented by declines international crises, military coups and in genocides and other mass slaughters of civilians. (See www.humansecurityreport.info)

Will this improvement in global security be sustained, or are we likely to witness more and increasingly deadly conflicts in the future? It is impossible to answer this question with any degree of confidence. There are too many unknowables. We can however point to a number of changes in the international system that provide some grounds for optimism, as well as some reasons to reject complacency. The 2005 Human Security Report and 2006 Human Security Brief outlined some of the grounds for optimism.

- Two critically important drivers of global conflict vanished completely with the end of colonialism and the end of the Cold War. There is no prospect that either will return.
- Since the early 1990s there has been a dramatic explosion of international activism directed at:

o Preventing armed conflicts (primarily via preventive diplomacy)

o Stopping wars that cannot be prevented ('peacemaking' in UN-speak)

o Preventing those that have stopped from starting again ('peacebuilding').

- There have been many failures associated with these initiatives—the success rate is rarely much more than 50%. But their combined impact has helped drive the net decline in armed conflicts since 1992. In the 1990s, 42 conflicts were brought to an end by negotiation—some four times more than in any previous decade.
- The positive impact of this activism is likely to continue and even increase since the international community has been on a steep learning curve since the early 1990s. Peacemaking and peacebuilding missions are appreciably more effective today than they were in the early 1990s—and there are a lot more of them.
- In two regions of the world the decline in armed conflicts began well before the end of the Cold War. Here the decline clearly cannot be explained by the upsurge of international activism noted above—this did not start until the beginning of the 1990s.
- In East and Southeast Asia, war numbers started dropping in the mid-1970s. This decline was associated with the ending of major power military intervention, the spread of inclusive democracies and and

354

extraordinary and sustained increase in economic growth. The latter point is perhaps the most significant. One of the most robust findings from the statistical literature on armed conflict is that the risk of war declines as incomes rise. States that have a per capita GDP of US\$250 have a 15% risk of succumbing to armed conflict within five years; the risk is less than half of 1% for states with an income of US\$5.000. Since incomes are still rising throughout most of the developing world there is а reasonable expectation that this will have a continuing positive impact on security.

§ In the Middle East and North Africa, armed conflicts started falling in the early 1980s again well before the end of the Cold war that triggered the decline in most of the rest of the world. But here the decline can be attributed neither to increased economic development, nor to the spread of inclusive democratization. In this region the key factor driving down political violence appears to have been effective, and often ruthless, state repression. However while what might be called 'peace through coercion' may be effective in the short term it is hardly a recipe for human security in the long term.

What about terrorism? Has the threat increased or decreased? As noted above, the data on fatalities from terrorist attacks can be read in different ways. But the deaths tolls are not the only metric. Those who believe that the

During this period support for terrorist tactics declined as terrorist fatalities increased. There remains, of course, more than enough support among the very small minorities of deeply radicalized and alienated Muslims around the world to sustain terrorist operations. But the continued decline in popular support for Islamic terrorism throughout the Muslim world may well have profound and positive strategic consequences.

As longtime terrorism expert Audrey Kurth Cronin has argued, lack of public support for civilians increases the probability that terrorists will fail.[11] Loss of popular support was a major factor in the decline and demise of the threat is increasing point to compelling public opinion data that show hostility to the US and its anti-terror campaign increasing throughout the Muslim world. Nowhere is this more evident than in Iraq. As a New York Times report late last year noted:

".... 61 percent of Iraqis now approve of attacks on Americans. That figure, is up from 47 percent in January [2006] ... 78% of Iraqis now believe that the American military presence is provoking more conflict than it is preventing."[8]

A major poll released in April 2007 found that growing hostility to the US and its wars in Iraq and Afghanistan was evident throughout the Muslim world. [9]

Popular support for the anti-American insurgency, however, does not translate into support for al-Qaeda or Osama bin Laden in Irag or indeed anywhere else in the Muslim world. Quite the contrary. Jihadi terrorism, according to a September 2006 poll of Iragis, is "rejected by overwhelming majorities of Iraqi Shias and Kurds and large majorities of Sunnis." In fact, no less than 82% of Iragis have an unfavourable view of al-Qaeda.[10] Indeed, opinion polls taken over the past five years reveal that popular support for jihadi terrorism has been falling sharply throughout the Muslim world. In the case of Pakistan-a country widely believed in the US to be harbouring al-Qaeda fighters, including Osama bin Laden-the number of Pakistanis believing that acts of violence against civilians are 'never justified' increased from 38% in 2002 to 72% in 2007.

Real Irish Republican Army, Spain's ETA and Peru's Shining Path terror campaigns, for example.

This is not all. Evidence suggests that terrorist campaigns that persistently fail to achieve their strategic objectives will eventually be abandoned. A major quantitative study published in 2006 revealed that in this respect terrorist organizations fail in 90% of cases and that "the poor success rate is inherent in the tactic of terrorism itself."[12]

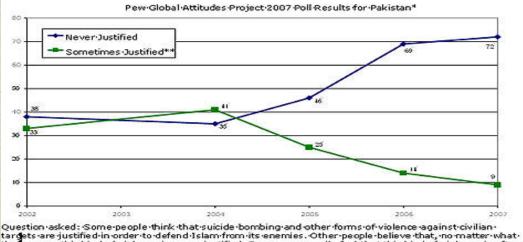
In the 1960s and 1970s, middle-class urban guerrilla/terrorist organizations were active in Europe (the Angry Brigade, Baader Mainton)

the Red Brigades, etc.) and Latin America (Tupamaros in Uruguay, the ALN, MR–8 and VLN in Brazil, etc.), but their violence alienated potential support bases and mobilized government action against them. Only a small percentage of the active members of these organizations were ever captured, killed or imprisoned. The rest simply gave up on strategies that were going nowhere.

The issue of strategic goals is critical. In al-Qaeda's case, the goal is the creation of a radical pan–Islamic caliphate. Achieving this goal will require the overthrowing of governments throughout the Islamic world. But the extreme form of Islamic governance that the jihadi terrorists seek to impose has little support in the Muslim world. This, together with the persistent failure of pan-Arabism to unite the Arab world and the often brutal effectiveness of state repression of Islamic achieved by the US-led War on Terror. These successes—in killing key al-Qaeda figures, in disrupting financial flows to terrorist organizations, etc—are not in doubt. However, as an analysis in the Washington Post noted last year:

"... many surveys show that since the U.S.-led invasions of Afghanistan and Iraq, Muslims almost universally have seen the war against terrorism as a war on Islam."[13]

The poll data suggest that the tactical successes that have been achieved in the Global War on Terror (GWOT) should be set against the increased hostility towards Washington that the GWOT has generated— hostility that translates into increased support for the violent campaigns against the US and its allies in Iraq, Afghanistan and elsewhere.



targets are justified in order to defend Islam from its enemies. Other people believe that, no matter what the reason, this kind-of-violence is never justified. Do yourpersonally feel that this kind-of-violence is often justified to defend Islam, sometimes justified, rarely-justified, or never-justified 1

\*Does-not-include-the-"rarely-justified" response-that ranged-from 5-to-18%-between-2002 and 2007------\*\*All-responders-were-muslim-and-predominantely-from-urban-areas¶

radicalism, suggest that the Islamic fundamentalist goal of using terrorism to overthrow Muslim governments and creating a global caliphate has little prospect of being realized.

The history of past terror campaigns suggests that those that fail to achieve their goals as the overwhelming majority do, are likely to be abandoned even though the terrorists may never actually be defeated.

Note that none of the above factors has anything to do with the tactical successes

#### Figure 5

#### No Room for Complacency

Despite the encouraging trend towards fewer and less deadly campaigns of armed violence, there is no room for complacency. In 2006, there were still some 56 armed conflicts being waged around the globe, plus a further 26 campaigns of violence against defenceless civilians.[14] And there is no iron law dictating that the recent downward trend in numbers of armed conflicts will be sustained.



In addition, the structural risk factors that drive conflicts to erupt in the first place are too rarely addressed in settlements that end the fighting and the risk of old wars starting again remains very real. Currently more than 30% of conflicts that stop, restart within five years.

While there is no reason for complacency, neither is there any cause for pessimism. We know far more today about the drivers of political violence than we did two decades ago. We also know that international action by donors, international agencies and NGOs can make a real difference.

#### Norway's Peace Diplomacy

A former Australian Foreign Minister once noted that even though Australia was neither rich enough to bribe other countries nor powerful enough to coerce them, it had nevertheless succeeded in 'punching above its weight' in the international community. It did so by practicing what he described as 'niche diplomacy'.

The Australian Labor government of the 1990s played a critical, and sometimes decisive, role in the creation of APEC, the Cairns Group, the ASEAN Regional Forum, the Antarctic Treaty, the peace settlement in Cambodia, the Chemical Weapons Convention (CWC) and the Comprehensive Test Ban Treaty (CTBT).

Issues were deliberately chosen in which policy options remained open and where a determined middle-power could make a difference diplomatically, primarily by marshalling foreign ministry expertise and other intellectual resources. On the CWC negotiations, for example, more than half of the Department of Foreign Affairs and Trade's experts on arms control were transferred to work on the CW file. Their efforts were closely followed by the minister. Work on the CTBTto which the US was then adamantly opposed--was relegated to the back-burner. Australia's energetic and focused diplomacy led to a new rolling text and the eventual signing of the Chemical Weapons Convention.

Norway is a much smaller country than Australia, but it too 'punches above its weight' diplomatically—particularly as a mediator. Oslo's peace diplomacy in Guatemala, Bosnia, the Middle East, Sri Lanka, Sudan, the Philippines, Haiti and Columbia has elevated Norway's reputation as a 'good international citizen', despite a mixed record of success.

Norway's overseas development assistance programs which are focused on the poorest countries—those that experience most wars can be seen as addressing the "root causes" of conflict and thus acting as a form of long-term conflict prevention.

Norway, like other major donors, the UN and the World Bank, assents to the now-prevalent slogan that "there can be no security without development". But exactly how Norwegian development assistance should change if it is to be viewed "through the conflict prevention lens" is less than clear. The Norwegian Foreign Ministry's Peacebuilding—a Development Approach had little to say about this.

Perhaps more important than any potential contribution to long-term conflict prevention, Norway's generous ODA and humanitarian programs give Oslo considerable political credibility in the nations of the global South and at the UN. This is an enormously important asset with respect to Oslo's peace diplomacy. In fact, in 2005 a Norwegian PR firm suggested that the government seek to brand Norway as the "humanitarian superpower".

Norway is one of a small number of countries widely perceived in the UN as "serious" and "punching above its weight"—with Jan Egeland doing much to strengthen that image in recent years. I offer this view as a former Director of Strategic Planning in Kofi Annan's Executive Office who continues to have strong contacts in the organization.

The UN connection is important because Norwegian peace diplomacy is also pursued indirectly through its support of the UN, via Norwegian and other NGOs working in the peacebuilding field, as well as the various "Friends" groups created to help countries that are emerging from conflict. Building coalitions of the "like-minded" (other states, international organizations and NGOs) is also a typical niche diplomacy strategy for small and medium.

357

powers and one frequently practiced by Norway.

The establishment of the Oslo Forum, a joint initiative between the Norwegian Foreign Ministry and the Centre for Humanitarian Dialogue in Geneva, is evidence of the government's commitment to strengthening the role of mediators in peacemaking and to exploring the idea of their professionalization.

There is one area in which Norway's peace diplomacy falls short, namely in the government's systematic neglect of impact evaluations of its peacemaking and peacebuilding missions.

Notwithstanding the existence of first-rate research institutions such as PRIO, NUPE, Chr. Michelsen and others, there is little work undertaken on evaluating preventive diplomacy, peacemaking or peacebuilding missions. Government agencies and NGOs do no better.

Norway is by no means unique in this respect. No government or international agency, or research institute, has ever sought to determine which is the most cost-effective policy—preventive diplomacy, peacemaking or post-conflict peacebuilding—and in terms not just of financial cost, but of lives saved.

In principle, prevention is the most costeffective. In practice, it is attempted far less frequently than peacemaking or peacebuilding.

Norwegian support for a broad-based program of systematic impact evaluations by policymakers, researchers and NGOs and of the absolute and relative efficacy of prevention, peacemaking and peacebuilding, would make a real contribution towards creating a peace diplomacy that, in being evidence-based, is also more effective.

#### Sources:

[1] The National Counterterrorism Center notes that its 2004 data are coded something differently to the data for 2005 and 2006 so the figures aren't strictly comparable. The steepness of the increase is not in doubt however.

[2] For an extreme example of terrorist threat inflation see, Norman Podhoretz, "World War IV: How It Started, What It Means, and Why We Have to Win," Commentary, September 2004.

[3] The START data have been 'filtered' to exclude attacks on the military and the police.

[4] The one major difference is that Uppsala only records cases of one-sided violence when there are more than 25 fatalities by perpetrator in a country within a calendar year.

[5] Fatality rather than incident counts are used here because definitions of incident can vary considerably; definitions of 'fatality' much less so. This is very clear in the case of countries with good statistics—Spain and Israel, for example—where there is little variation in fatality figures and trends, but considerable variation in incident counts.

[6] Raphael F. Perl, International Terrorism: Threat, Policy and Response, Congressional Research Service, January 3, 2007. http://www.fas.org/sgp/crs/terror/RL33600.pdf. Accessed August 10, 2007.

[7] Professor Schmid currently directs the Centre for the Study of Terrorism and Political Violence at the University of St Andrews.

[8] Nicolas D. Kristof, 'Listen to Iraqis', New York Times, October 8, 2006.

[9] Worldpublicopinion.org, 2007.

[10] See World Public Opinion.org. 'All Iraqi Groups Overwhelmingly Reject al Queda', October 8, 2006. http://www.worldpublicopinion.org/pipa/articles/brmiddleeastnafricara/248.php?nid=&id=&pnt=248&lb=

[11] Audrey Kurth Cronin, 'How Al–Quida Ends', International Security 31, No.1 (Summer 2006).

[12] Max Abrahams. 'Why Terrorism Doesn't Work'. International Security 31, No.2 (2006): 42-68.

[13] Karl Vick, 'Reunified Islam: Unlikely but Not Entirely Radical' In:Washington Post Foreign Service, January 14, 2006; A01. www.washingtonpost.com/wp-dyn/content/article/2006/01/13/AR2006011301816\_pf.html. Accessed , August 13, 2007. See also WorldPublicOpinion.org, 'Muslim Public Opinion on US Policy, Attacks on Civilians and al Queda', Program on International Policy Attitudes, University of Maryland, April 24, 2007. www.worldpublicopinion.org/pipa/pdf/apr07/START\_Apr07\_rpt.pdf. Accessed, August 13, 2007. [14] 25 deliberately killed civilians constitutes a campaign.

Andrew Mack is Director, Human Security Research Group c/o School for International Studies, Simon Fraser University, Vancouver



#### EU: Jihadist calls for tourist Jihad

Source: http://www.telegraaf.nl/binnenland/10277878/\_\_\_Wilders\_ideaal\_slachtoffer\_\_\_.html

Jihadist Abu Suleiman al-Nasser wrote on the Shumukh al-Islam forum that Muslims should go to Europe posing as tourists in order to murder Europeans. Al-Nasser wrote on the site that Muslims should buy a sharp knife when they're in Europe. "You could murder more than a hundred people. Walk about and choose your victims." He wrote that Geert Wilders is an ideal victim. "He looks like a fat calf." Meanwhile, the American intelligence website SITE reports that Jihadists are calling for attacks on Belgium and Belgians in retaliation for the recently enacted burqa-ban. According to one Jihadist: "If you have the freedom to make such decisions, then you must also accept our freedom to take action. I call our Muslim brothers in Belgium to do what they can: bomb them, destroy them, torture and murder them."

#### **The Third Jihad**

Source: http://www.thethirdjihad.com/about\_new.php

The Third Jihad, the newest offering from the producers of the captivating documentary film, Obsession, explores the existence of radical Islam in America and the emerging risk that this "homegrown jihad" poses to national security, western liberties and the "American



#### way of life."

The film, which is narrated by devout Muslim American Dr. M. Zuhdi Jasser, opens with the following statement: "This is not a film about Islam. It is about the threat of radical Islam. Only a small percentage of the world's 1.3

# Norway's Terrorism in Context

#### **By Daniel Pipes**

Source: http://www.meforum.org/pipes/10007/norway-terrorism-in-context

Scandinavia may look idyllic from a distance, what with royal families and prime ministers almost without security, but it has endured its fair share of violence, from the assassinations of Swedish prime minister Olof Palme and foreign minister Anna Lindh to two school massacres in one year in Finland, one killing billion Muslims are radical. This film is about



#### them."

In 72 minutes, the film reveals that radical Islamists driven by a religiously motivated rejection of western values cultures and religion are engaging in a multifaceted strategy to overcome the western world. In contrast to the use of "violent jihad" and terror to instill fear in "non-believers," The Third Jihad introduces the concept of "cultural jihad" as a means to infiltrate and undermine our society from within.

eight, the other ten. Anders Behring Breivik's rampage, in other words, was hardly unprecedented.



In the past, one had the cold comfort of knowing that deranged acts such as his were



Behring Breivik plagiarized the Unabomber, Ted Kaczynski.

carried out by individuals under the sway of extremist ideologies. Not so Behring Breivik. This terrorist lists among his favorite authors George Orwell, Thomas Hobbes, John Stuart Mill, John Locke, Adam Smith, Edmund Burke, Ayn Rand, and William James. The disconnect between Behring Breivik's mainstream political conservatism and his psychological derangement presents a shocking new dilemma and challenge.

That said, there is no reason to think that Behring Breivik has a single follower, that any other mainstream political conservative will emulate him and massacre socialists. This has never happened before and will probably never happen again. This is a gruesome, freakish exception.

And yet, this exception does tell conservatives that we have to be aware of a danger we had not thought of before. We may oppose socialists, but not vilify them.

Given how meticulously Behring Breivik planned not just his bombing attack and gun rampage but also his posting of a manifesto and a video, and given his plans to turn his trial into political theater, his terrorism appears ultimately intended primarily to bring attention to his political views. Indeed, during his initial court appearance on July 25, the Associated Press reports, he presented the violence "as 'marketing' for his manifesto," 2083 — A European Declaration of Independence.

In this way, Behring Breivik resembles the Unabomber, Ted Kaczynski, who engaged in violence as a means to market his 1995 manifesto, Industrial Society and Its Future. Indeed, the tie between these two is very close: Hans Rustad documents how extensively Behring Breivik plagiarized from Kaczynski, changing only some key words.

Add to these two Timothy McVeigh (the 1995 Oklahoma City bomber) and Baruch Goldstein (the 1994 Hebron mass killer) and one has the four outstanding exceptions to the dominant rule of Islamist mass murder. One website, TheReligionOfPeace.com. counts 17.500 terrorist incidents on behalf of Islam in the past ten years; extrapolating, that comes to some 25,000 since 1994. We are dealing with two very different orders of magnitude. As David P. Goldman notes, "there is a world of difference between the organized use of horror by terrorist movements and the depraved actions of individuals." Yes, we must worry about non-Islamist violence too, but the Islamist variety prevails and, being a vital extremist movement, will continue to do so.

Ravi Shankar, executive editor of the New Indian Express, writes that "What happened in Oslo Friday may be the early beginning of a new civil war - Europeans fighting each other, both Muslim and Christian." He could well be right. As I argued in a 2007 analysis, "Europe's Stark Options," the continent's future is likely to consist of either Islamization or protracted civil conflict. I sketched the possibility of "indigenous Europeans - who do still constitute 95 percent of the continent's population — waking up one day and asserting themselves. 'Basta!' they will say, and reclaim their historic order. This is not so remote; a chafing among Europeans, less among elites than the masses, loudly protests changes already underway."

Although he attacked socialists, not Muslims, Behring Breivik clearly fits this chafing. More broadly, he fits into a pattern of growing Christian-Muslim violence visible from Nigeria to Iraq to the Philippines.

Not surprisingly, Behring Breivik belongs to the "Islam is evil" school of thought, as he frequently signaled in his manifesto:

... a tolerant Islam is a contradiction, and the "creation" of a tolerant past for Islam to appease the position of liberal Muslims is a lie.

... to take the violence out of Islam would require it to jettison two things: the Quran as the word of Allah and Muhammad as Allah's prophet. In other words, to pacify Islam would

require its transformation into something that it is not.

Islam today is what it has been fourteen centuries: violent, intolerant, and expansionary. It is folly to think that we, in the course of a few years or decades, are going to be able to change the basic world outlook of a foreign civilisation. Islam's violent nature must be accepted as given.

Many moderate cultural conservatives have suggested that banning Sharia will solve all our problems and force the Muslims to integrate. Unfortunately, Islam is a lot more resilient than most people can comprehend. . . . Taking Sharia (and all political aspects) out of Islam is simply not possible.

This position differs fundamentally from my own, which holds that "radical Islam is the problem, moderate Islam is the solution." While sharing common opponents, these two outlooks differ on the nature of Islam, its potential for change, and the possibility of allying with Muslims.

Beyond massacring innocent Norwegians, Behring Breivik damaged conservatism, the counterjihad, and (in particular) those authors he cited in his writings, including myself. A close reading of his manifesto suggests this may have been purposeful. Noting that his former membership in Norway's conservative Progress Party would do it harm, he evinces satisfaction that this will forward his revolutionary goals:

I anticipate that the Norwegian media will persecute and undermine the Progress Party for my earlier involvement in the organisation. This is not a negative thing as an increasing amount of Norwegians will then have their "illusions of democratic change" crushed (if the Progress Party is annihilated by the multiculturalist media) and rather resorts to armed resistance.

In a similar spirit, he writes: "America as a polity is scr\*wed, and thank the gods for that." By extension, Behring Breivik may well have wanted to harm those analysts of Islam cited in the manifesto. He calls me a "moderate," which obviously is not meant as a compliment, and dismisses even the hardest-line critics of Islam as lacking in courage:

The reason why authors on the Eurabia related issues/Islamisation of Europe — Fjordman, Spencer, [Bat] Ye'or, Bostom etc. aren't actively discussing deportation is because the method is considered too extreme (and thus would damage their reputational shields).... If these authors are to [sic] scared to propagate a conservative revolution and armed resistance then other authors will have to.

Behring Breivik hopes to undermine anyone he perceives

as obstructing his dreamed-for revolution. Temporarily, at least, he has succeeded.

Daniel Pipes is president of the Middle East Forum and Taube distinguished visiting fellow at the Hoover Institution of Stanford University.

#### Norway: Lessons from a Successful Lone Wolf Attacker

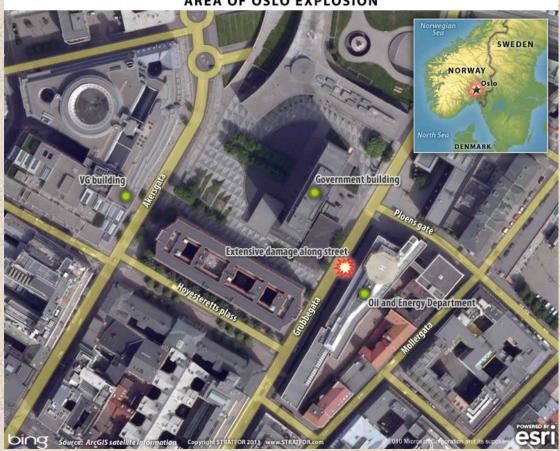
#### **By Scott Stewart**

Source:http://www.stratfor.com/weekly/20110727-norway-lessons-successful-lone-wolf-attacker?utm\_source=freelist-f&utm\_medium=email&utm\_campaign=20110728&utm\_term=sweekly&utm\_content =readmore&elg=ced8f91d62e94225a21fbc085794f348

On the afternoon of July 22, a powerful explosion ripped through the streets of Oslo, Norway, as a large improvised explosive device (IED) in a rented van detonated between the government building housing the prime minister's office and Norway's Oil and Energy Department building. According to the diary of Anders Breivik, the man arrested in the case who has confessed to fabricating and placing the device, the van had been filled with 950 kilograms (about 2,100 pounds) of homemade ammonium nitrate-based explosives.

After lighting the fuse on his IED, Breivik left the scene in a rented car and traveled to the island of Utoya, located about 32 kilometers (20 miles) outside of Oslo. The island was the site of a youth campout organized by Norway's ruling Labor Party. Before taking a boat to the island, Breivik donned body armor and tactical gear bearing police insignia (intended to afford him the element of tactical surprise). Once on the island he opened fire on the attendees at the youth camp with his firearms, a semiautomatic 5.56 mm Ruger Mini-14 rifle, and a 9 mm Glock pistol. Due to the location of the stand

camp on a remote island, Breivik had time to kill 68 people and wound another 60 before police responded to the scene.



AREA OF OSLO EXPLOSION

Shortly before the attack, Breivik posted a manifesto on the Internet that includes his lengthy operational diary. He wrote the diary in English under the Anglicized pen name Andrew Berwick, though a careful reading shows he also posted his true identity in the document. The document also shows that he was a lone wolf attacker who conducted his assault specifically against the Labor Party's current and future leadership. Breivik targeted the Labor Party because of his belief that the party is Marxist-oriented and is responsible for multiculturalism, encouraging Muslim immigration into Norway and, acting with other similar European governments, the coming destruction of European culture. Although the Labor Party members are members of his own race, he considers them traitors and holds them in more contempt than he does Muslims. In fact, in the manifesto, Breivik urged others not to target Muslims because it would elicit sympathy for them.

Breivik put most of his time and effort into the creation of the vehicle-borne IED (VBIED) that he used to attack his primary target, the current

housed government, which is in the government building. It appears that he believed the device would be sufficient to destroy that building. It was indeed a powerful device, but the explosion killed only eight people. This was because the device did not bring down the building as Breivik had planned and many of the government employees who normally work in the area were on summer break. In the end, the government building was damaged but not destroyed in the attack, and no senior government officials were killed. Most of the deaths occurred at the youth camp, which Breivik described as his secondary target.

While Breivik's manifesto indicated he planned and executed the attack as a lone wolf, it also suggests that he is part of a larger organization that he calls the "Pauperes Commilitones Christi Templique Solomonici (PCCTS, also known as the Knights Templar), which seeks to encourage other lone wolves (whom Brevik refers to as "Justiciar Knights") and small cells in other parts of Europe to carry out a plan to

"save" Europe and European culture from destruction.

Because of the possibility that there are other self-appointed Justiciar Knights in Norway or in other parts of Europe and that Breivik's actions, ideology and manifesto could spawn copycats, we thought it useful to examine the Justiciar Knights concept as Breivik explains it to see how it fits into lone wolf theory and how similar actors might be detected in the future.

#### An Opening Salvo?

From reading his manifesto, it is clear that Breivik, much like Oklahoma City bomber Timothy McVeigh, believes that his attack is the opening salvo in a wider campaign, in this case to liberate Europeans from what Breivik views as malevolent, Marxist-oriented governments. These beliefs are what drove Breivik to attack the Norwegian Labor Party. As noted above, it is also clear that Breivik planned and executed his attack alone.

However, he also discusses how he was radicalized and influenced by a Serbian living in Liberia whom he visited there. And Breivik claims to have attended a meeting in London in 2002 to "re-found the Knights Templar." This organization, PCCTS, which was founded in 2002, is not related to the much older official and public chivalric order also known as the Knights Templar. According to Breivik, the PCCTS was formed with the stated purpose of fighting back against "European Jihad" and to defend the "free indigenous peoples of Europe." To achieve this goal, the PCCTS would implement a three-phase plan designed to seize political and military power in Europe. In his manifesto Breivik outlines the plan as follows:

- Phase 1 (1999-2030): Cell-based shock attacks, sabotage attacks, etc.
- Phase 2 (2030-2070): Same as above but bigger cells/networks, armed militias.
- Phase 3 (2070-2100): Pan-European coup d'etats, deportation of Muslims and execution of traitors.

As outlined in Breivik's manifesto, the 2002 meeting was attended by seven other individuals, two from England and one each from France, Germany, the Netherlands, Greece and Russia. He also asserts that the organization has members from Serbia (his contact living in Liberia), Sweden, Belgium and the United States who were unable to attend the meeting. Brevik states that all the members of the PCCTS were given code names for security, that his code name was "Sigurd," and that he was mentored by a member with the code name "Richard the Lionhearted" (presumably a Briton). Breivik claims that after meeting these individuals via the Internet he was carefully vetted before being allowed to join the group.

The diary section of Breivik's manifesto reveals that during the planning process for the attack Breivik traveled to Prague to obtain firearms and grenades from Balkan organized-crime groups there (he had hoped to obtain a fully automatic AK-47). Breivik was not able to procure weapons in Prague and instead was forced to use weapons he was able to obtain in Norway by legal means. It is interesting that he did not contact the Serbian member of the PCCTS for assistance in making contact with Balkan arms dealers. Breivik's lawyer told the media July 26 that although Breivik acted alone in conducting his attack, he had been in contact with two terror cells in Norway and other cells abroad. Certainly, Norway and its partners in EUROPOL and the United States will try to identify these other individuals, if they do in fact exist.

In phase one of the PCCTS plan, shock attacks were to be carried out by individuals operating as lone wolves or small cells of Breivik's socalled Justiciar Knights, who are self-appointed guardians who decide to follow the PCCTS code outlined in Breivik's manifesto and who are granted the authority to act as "a judge, jury and executioner until the free, indigenous peoples of Europe are no longer threatened by cultural genocide, subject to cultural Marxist/Islamic tyranny or territorial or existential threats through Islamic demographic warfare."

Breivik's manifesto notes that he does not know how many Justiciar Knights there are in Western Europe but estimates their number to be from 15 to 80. It is unclear if this is a delusion on his part and there are no other Justiciar Knights or if Breivik has some factual basis for his belief that there are more individuals like him planning attacks.

While some observers have noted that the idea of Justiciar Knights operating as lone wolves and in small cells is similar to the calls in recent years for grassroots jihadists to adopt lone wolf tactics, it is important to understand that leaderless resistance has been a central theme of white supremacist groups in the United

States since the early 1990s. While Breivik did not express any anti-Semitism in his manifesto (something he has been heavily criticized for on U.S. anti-Semitic websites), clearly the antiimmigration and anti-Marxist ideology of the PCCTS has been influenced more by white hate groups than by al Qaeda.

Moreover, the concept of a self-identified Justiciar Knight is quite similar to the idea of a "Phineas Priest" in the leaderless resistance model propagated by some white supremacists in the United States who adhere to "Christian Identity" ideology. In this model, Phineas Priests see themselves as lone wolf militants chosen by God and set apart to be his "agents of vengeance" upon the earth. Phineas Priests also believe that their attacks will serve to ignite a wider "racial holy war" that will ultimately lead to the salvation of the white race.

Leaderless resistance has also been advocated by militant anarchists as well as animal rights and environmentalist activists who belong to such groups as the Animal Liberation Front and the Earth Liberation Front. So it is not correct to think of leaderless resistance merely as a jihadist construct — it has long been used by a variety of militant actors.

#### Lone Wolf Challenges

One of the great strengths of our enemies, the Western European cultural Marxist/multiculturalist regimes is their vast resources and their advanced investigation/forensic capabilities. There are thousands of video cameras all over European major cities and you will always risk leaving behind dna, finger prints, witnesses or other evidence that will eventually lead to your arrest. They are overwhelmingly superior in almost every aspect. But every 7 headed monster has an Achilles heel. This Achilles heel is their vulnerability against single/duo martyr cells. -Anders Breivik

As STRATFOR has long discussed, the lone wolf operational model presents a number of challenges for law enforcement, intelligence and security officers. The primary challenge is that, by definition, lone wolves are solitary actors, and it can be very difficult to determine their intentions before they act because they do not work with anyone else. When militants are operating in a cell consisting of more than one person, there is a larger chance that one of them will get cold feet and reveal the plot to authorities, that law enforcement and intelligence personnel will intercept a communication between conspirators, or that the authorities will be able to insert an informant into the group.

This ability to fly solo and under the radar of law enforcement has meant that some lone wolf militants such as Joseph Paul Franklin, Theodore Kaczynski and Eric Rudolph were able to operate for years before being identified and captured. Indeed, from Breivik's diary, we know he took several years to plan and execute his attack without detection.

As the Breivik case illustrates, lone wolves also pose problems because they can come from a variety of backgrounds with a wide range of motivations. While some lone wolves are politically motivated, others are religiously motivated and some are mentally unstable.

In addition to the wide spectrum of ideologies and motivations among lone wolves, there is also the issue of geographic dispersal. As we've seen from past cases, their plots and attacks have occurred in many different locations and are not confined just to Manhattan, London or Washington. Lone wolf attacks can occur anywhere.

Furthermore, it is extremely difficult to differentiate between those extremists who intend to commit attacks and those who simply preach hate or hold radical beliefs (things that are not in themselves illegal in many countries). Therefore, to single out likely lone wolves before they strike, authorities must spend a great deal of time and resources looking at individuals who might be moving from radical beliefs to radical actions. This is a daunting task given the large universe of potential suspects.

#### Vulnerabilities

In spite of the challenges presented by lone wolf operatives, they are vulnerable to detection at several different stages of their attack cycle. One of these vulnerabilities comes during the planning stage when weapons are acquired. From reading Breivik's diary, it is clear that he felt exposed as he tried to purchase the chemicals he needed to build his IED. Because of this vulnerability, Breivik created an extensive cover story that included renting a farm in order to explain his purchase of a large quantity of ammonium nitrate fertilizer. The farm also provided a private, spacious place for him to construct his IED.

Breivik also exposed himself to potential detection when he traveled to Prague to attempt to purchase weapons. One of the criminals he contacted could have turned him in to authorities. (In June 2011 we saw a jihadist cell in Seattle detected and arrested while attempting to buy guns from a criminal acquaintance. Another small cell was arrested in New York in May 2011, also while attempting to obtain weapons.) Even if Breivik had succeeded in purchasing weapons in Prague. he would still have been vulnerable as he smuggled the weapons back into Norway in his car (though it is important to remember that EU countries have open borders so security checks would not have been too stringent).

Breivik also exposed himself to detection as he conducted surveillance on his targets. Interestingly, in his diary, Breivik goes into excruciating detail discussing how he manufactured his device based on information he was able to obtain from the Internet, but he mentions very little about how he selected specific targets or how he conducted surveillance on them. He mentions only that he visited the sites and programmed the locations into his GPS. He also discusses using a video camera to record his attack but does not mention if he used still or video cameras in his target surveillance. How Breivik specifically chose his targets and how he conducted surveillance on them will be important for the Norwegian authorities to examine.

Finally, Breivik mentions several times in his diary that the steps he was taking would be far more difficult if he were a foreign-born Muslim instead of a Caucasian Norwegian. This underscores a problem we have discussed with profiling suspects based on their ethnicity or nationality. In an environment where potential threats are hard to identify, it is doubly important to profile individuals based on their



behavior rather than their ethnicity or nationality — what we refer to as focusing on the "how" rather than the "who."

#### Not All Lone Wolves are Equal

Finally, in the Breivik case we need to recognize that Norwegian authorities were dealing with a very capable lone wolf operator. While lone wolf theory has been propagated for many years now, there have been relatively few successful lone wolf attacks. This is because it takes a special individual to be a successful lone wolf assailant. Unlike many lone wolves, Breivik demonstrated that he possessed the intelligence and discipline to plan and carry out an attack that spanned several years of preparation. For example, he joined a pistol club in 2005 just in case he ever needed to buy a gun through legal means in Norway, and was able to rely on that alternate plan when his efforts to purchase firearms in Prague failed. Breivik was also driven, detailoriented and meticulous in his planning. His diary documents that he was also extremely patient and careful during the dangerous trialand-error process of manufacturing explosives. It is rare to find a lone wolf militant who possesses all those traits, and Breivik stands in stark contrast to other European grassroots operatives like Nick Reilly or Bilal Abdullah and Kafeel Ahmed, who made amateurish attempts at attacks. Breivik appears to have been a hard worker who claims to have amassed some 500,000 euros by working a variety of jobs and selling a communications company. After some unsuccessful speculation on the stock market he still had enough money and credit to rent the farm and the vehicles he used in the attack and to buy the required bomb components, weapons and body armor. In his diary he says that he began his two tasks - writing the manifesto and conducting the attack - with a war chest of 250,000 euros and several credit cards.

Breivik also is somewhat unique in that he did not attempt to escape after his attacks or become a martyr by his own hand or that of the authorities. Instead, as outlined in his manifesto, he sought to be tried so that he could turn his trial into a grandstand for promoting his ideology beyond what he did with his manifesto and video. He was willing to risk long prison sentence in order to a communicate his principles to the public. This means that the authorities have to be concerned not only about other existing Justiciar Knights but also anyone who may be influenced by Breivik's message and follow his example.

There is also the possibility that individuals who do not adhere to Breivik's ideology will seek to exploit the loopholes and security lapses highlighted by this incident to conduct their own attacks. Breivik's diary provides a detailed step-by-step guide to manufacturing a successful VBIED, and the authorities will be scrutinizing it carefully to address the vulnerabilities Breivik exposed before those instructions can be used again.

# The Oslo massacre in pictures

Source:ttp://www.norwaynews.com/en/~view.p hp?72Tb354LMd4823w285Bkh844UN388bPZ 76EDn353K8K8





## The 'Lone Wolf' Disconnect By Fred Burton and Scott Stewart Source: http://www.stratfor.com/weekly/lone\_wolf\_disconnect

The idea that a lone individual will appear seemingly out of nowhere to launch a horrific terrorist attack sends shivers down the spines of public security planners and law enforcement officers — not to mention average citizens. Because of their unique traits, "lone wolves" present very real challenges to the law enforcement and security professionals charged with guarding against such threats.

However, with the road from desire to actual destruction fraught with obstacles, the lone-wolf terrorist — one capable of causing mass casualties — is a rare individual indeed.

The flames of fear regarding lone wolves are fanned by the near-constant bantering about such operatives in radical circles, in movies and books and even in analyses pertaining to domestic and international terrorism. For many years now, domestic radicals such as neo-Nazi Tom Metzger and former Klansman Louis Beam have championed the "leaderless resistance" model of operation. Beam's 1992 essay, "Leaderless Resistance," has been widely embraced by many on the radical right as the definitive work on the subject and has been translated into many languages.

In his essay, Beam envisions a two-tiered approach to revolutionary struggle. One tier would be the above-ground "organs of information," who would "distribute information using newspapers, leaflets, computers, etc." The organs of information were not to conduct any illegal activities but rather to provide direction for lone wolves, as well as issue propaganda for recruitment purposes. The second tier would be made up of individual operators and small "phantom" cells that would conduct attacks. These people were to remain low-key and anonymous, with no connections to the above-ground activists. Of course, in 1992, Beam likely never imagined how the Internet would become an almost perfect medium for the organs of information to disseminate information to the detached, anonymous lone wolves.

In many ways, the radical Islamist world also has embraced this operational model and the Internet technology. Scores of Web sites dedicated to serving as jihadist organs of information aim to radicalize individual Muslims and then equip these radicalized individuals with information on how to conduct terrorist attacks. Al Qaeda franchises even have produced online magazines, such as Maaskar al-Battar (Al-Battar Training Camp), which was produced by al Qaeda's Saudi node. These magazines are designed to further support radical ideology, teach individual radicals how to train for jihad and provide guidance on how to surveil and select targets - and even how to properly employ a number of weapons systems.

However, in spite of the fact that the concept of leaderless resistance has been publicly and widely embraced in both the domestic terrorism and jihadist realms, few terrorist attacks have been perpetrated by lone-wolf operatives. In fact, we have seen more mentally disturbed lone gunmen than politically motivated lonewolf terrorists. A main reason for this lack of operatives in the political realm is the disconnect — the lack of translation from theory to action.

#### Definition of a Lone Wolf

It is important to define the term "lone wolf" because many people — both in the militant realm and in law enforcement and intelligence circles — misuse it or use it imprecisely. A lone wolf is a person who acts on his or her own without orders from — or even connections to — an organization. The theory is that this distance will prevent disclosure of attack planning to informants or technical surveillance and therefore provide superior operational security.

A lone wolf is distinct from a sleeper operative in that a sleeper is an operative who infiltrates the targeted society or organization and then remains dormant — sometimes for quite some time — until being activated, perhaps by a prearranged signal or a certain chain of events. A lone wolf is a standalone operative who by his very nature is embedded in the targeted society and is capable of self-activation at any time.

Most militant groups do not have the resources or patience to launch a true sleeper operation. While militant groups do frequently utilize covert operatives, such as the 9/11 attackers, we are unaware of any instance in which a militant group ran a true sleeper cell operation. (Most of the sleeper operations we know of involve attempts at international espionage.) Clearly, most covert militant operatives engage in some sort of operational activity and do not remain dormant. One cannot carry out operational activities and be a sleeper.

Also, it must be remembered that a sleeper or other covert operative, for that matter — is trained and dispatched by an organization. The existence of this connection to an organization means that the operative cannot, by definition, be a true lone wolf.

Al Qaeda and its jihadist cousins and progeny across the globe have used a number of different operational models, some of them quite decentralized. However, even decentralized grassroots operatives, such as the London Underground attackers, have contact with an organization and so are not, by definition, lone wolves.

Some lone wolves are ideologically motivated, some are religiously inspired, some are mentally disturbed and still others are influenced by a combination of these factors. Our focus here is on politically or religiously motivated attackers, not on mentally ill individuals motivated for other reasons (such as Virginia Tech shooter Seung-Hui Cho). Certainly such individuals create terror during their rampages, but they are not conducting politically motivated terrorist attacks. We distinguish between lone wolves and "lone nuts" because, although many politically motivated attackers do have some degree of mental illness, rational and irrational individuals operate differently. Mentally disturbed individuals are far more likely to self-radicalize in a vacuum and have less concern for their own safety than do most politically motivated attackers. This lack of concern for their own safety often helps them to overcome their lack of skill.

#### Easier Said Than Done

The rubber meets the road when potential attackers try to place lone-wolf theory into action. Like much political theory, or even business theory, it often is easier to design a system than it is to apply it to a real-world situation — one that involves fallible people.

One of the biggest problems for lone-wolf operators is acquiring the skills necessary to conduct a successful terrorist attack. Perhaps this is one reason suicide bombers rarely are lone wolves; there simply is too much involved in preparing for such an attack.

In his essay on leaderless resistance, Beam wrote, "It becomes the responsibility of the individual to acquire the necessary skills and information as to what is to be done." This, of course, is an obvious condition of leaderless resistance — and it is easy enough to write. But acquiring these skills in the real world can pose quite a daunting challenge. (As a decorated Vietnam War veteran, Beam likely did not realize how difficult it might be for someone lacking his military and combat experience to pick up those skills.)

In fact, some of the most successful lone-wolf assailants, including Olympic bomber Eric Rudolph, had served in and been trained by the military. Some people consider Oklahoma City bomber Timothy McVeigh an example of a military-trained lone wolf, but his possible association with the Aryan Resistance Army, his connections to The Covenant, the Sword and the Arm of the Lord group in Elohim City, Okla., and his connections to like-minded individuals — including Michael Fortier and Terry Nichols — suggest he was a grassroots operative and not a truly isolated lone wolf.

Military training is not a necessity for lone-wolf success. Joseph Paul Franklin carried out a series of killings (perhaps as many as 20 in several states), robberies and arsons from 1977 to 1980 in an attempt to ignite a race war in the United States. His attempts to assassinate high-profile targets Vernon Jordan and Larry Flynt failed, though he seriously wounded both of them and left Flynt paralyzed. Even though many Web sites and military manuals provide instruction on such things as making bombs and marksmanship, there is no substitute for hands-on experience in the real world. Playing the neo-Nazi video game "Ethnic Cleansing" or similar games for hours will not automatically make a person an expert tactical shooter. Gaining such expertise requires practice. Intellectual prowess also is no substitute for experience. For example, even a genius like Unabomber Theodore Kaczynski had to do much experimentation in order to improve the design of his explosive devices. Of the 16 devices Kaczynski sent, several either did not explode or did not function as designed. In the end, Kaczynski's 18-year bombing campaign killed only three people.

Because of the difficulty of successfully manufacturing (in Kaczynski's case) or even stealing (in Rudolph's case) effective explosives, many would-be lone wolves attempt to procure explosives or military weaponry. It is at this stage, when the lone wolf reaches out for assistance, that many of these individuals have come to the attention of law enforcement. One such case was Derrick Shareef, who was arrested in December 2006 while attempting to trade stereo speakers for hand grenades and a pistol he sought to use in an attack against the CherryVale shopping mall in Rockford, III. The person Shareef approached to help him obtain the weapons happened to be a police informant.

Immaturity and lack of common sense also are significant hurdles for some would-be lone-wolf attackers. For instance, a person who attempts to buy an illicit fully automatic weapon when he could easily — and legally — obtain a less expensive semiautomatic version of the same weapon clearly is influenced by Hollywood and does not understand the effectiveness of controlled, sustained fire versus the spray-andpray shooting he sees in the movies or on TV. As Franklin and several mentally disturbed shooters have demonstrated, automatic weapons are not needed to inflict carnage. Another consideration is that the process of radicalization - to the point that a person undertakes a terrorist attack - rarely occurs in a solitary setting. Many individuals require the feedback and encouragement of like-minded individuals to help them reach that point. And this group dynamic crosses ideological divides. It is seen in gangs of racist skinheads and radical Jews as much as it is in jihadists. In many cases that first appear to involve a lone wolf, further investigation shows that the person's activities were motivated and facilitated by others. Only certain types of individuals can go through this process of radicalization and indoctrination and then motivate themselves to take violent action outside of a group dynamic. Franklin, Kaczynski and Rudolph, for example, tended to be loners even before they became radicalized. Furthermore, even if someone can cross the hurdle of self-radicalization to the point that he is willing to conduct an attack, and even if he can build effective explosive devices or shoot a oun, he still must have other subtler abilities street skills - that are difficult to master without practice and actual training. Perhaps the most significant of these street skills is surveillance tradecraft.

Although radical Web sites and online training magazines provide written instruction in surveillance, mastering the complex and subtle set of skills required to be a good surveillance operative takes a great deal of training and practical experience. It is not impossible for someone to develop and hone these skills on his own, but it is extremely difficult. Even Rudolph, a lone wolf who practiced excellent operational security and had dood bombmaking and wilderness-survival skills, ultimately was captured because he lacked street skills. It was his suspicious behavior while on a street that caused a citizen to follow him back to his truck and report the vehicle's license tag to the police.

While the fictional and theoretical versions of lone-wolf operatives can be terrifying, real-life examples demonstrate that not only are such attackers fairly rare, but the constraints their isolation imposes on them (in acquiring weapons and training) usually limit the amount of damage they can do. Moreover, a lone wolf who reaches out for external assistance or training eventually finds himself interacting with other militants — and then he no longer is considered a lone wolf.

# The Wide-Ranging Psychological Impacts Of The 9/11 Tragedy -10 Years Later

Source: http://www.medicalnewstoday.com/releases/231746.php

Short-term and long-term psychological effects of the 9/11 attacks spread far beyond New York City, Washington, D.C., and Shanksville, Pa., according to research published by the American Psychological Association. A team of psychologists examine the social, political and psychological impacts of the nation's worst terrorist attack in "9/11: Ten Years Later," a special issue of APA's flagship journal, American Psychologist. With a dozen peer-reviewed articles, the issue illustrates how psychology is helping people understand and cope with 9/11's enduring impacts. It also explores how psychological science has helped us understand the roots of terrorism and how to prevent further attacks. The articles include:

- An Introduction to "9/11: Ten Years Later" Roxane Cohen Silver, PhD, University of California, Irvine
- A summary explaining the goals of the issue, which explores how the past decade was shaped by the events of 9/11 and their aftermath; lessons learned from individual, community and national responses; and new analyses of psychological research.
- The Expulsion from Disneyland: The Social Psychological Impact of 9/11 G. Scott Morgan, PhD, Daniel C. Wisneski, BA, and Linda J. Skitka, PhD, University of Illinois at Chicago
- Americans responded to the 9/11 attacks with negative social reactions, such as increased prejudice, as well as positive social reactions, including charitable donations and civic engagement. Psychological theory helps explain why people have such powerful reactions when their way of life is threatened by terrorist attacks.
- Americans Respond Politically to 9/11: Understanding the Impact of the Terrorist Attacks and Their Aftermath Leonie Huddy, PhD, and Stanley Feldman, PhD, Stony Brook University
- Research on American political reactions to 9/11 suggests that people support a strong government response to terrorism when they perceive a high risk of future terrorism and feel angry at terrorists.
- While Americans who were personally affected by the attacks were more likely to feel anxious about terrorism, they were less supportive of overseas military action.
- Posttraumatic Stress Disorder Following the September 11, 2001, Terrorist Attacks: A Review of the Literature among Highly Exposed Populations - Yuval Neria, PhD, Columbia University and New York State Psychiatric Institute; Laura DiGrande, DrPH, New York City Department of Health and Mental Hygiene; Ben G. Adams, PhD, Columbia University
- The terrorist attacks of 9/11 have brought a substantial and enduring burden of posttraumatic stress disorder on those people who lost loved ones, as well as on firefighters and recovery workers. Research over the past decade has broadened the understanding of PTSD following large-scale disasters such as terrorism.
- Growing Up in the Shadow of Terrorism: Youth in America After 9/11 Nancy Eisenberg, PhD, Arizona State University; Roxane Cohen Silver, PhD, University of California, Irvine
- For most children, the psychological consequences of 9/11 were relatively transient, particularly for those who only watched the events unfold on TV. However, 9/11 may have affected American youth in other ways, in terms of their sociopolitical attitudes and their general beliefs about the world. Parents played important roles in shaping their children's responses to 9/11.
- Post disaster Psychological Intervention Since 9/11 Patricia J. Watson, PhD, UCLA/Dartmouth; Melissa J. Brymer, PhD, UCLA; and George A. Bonanno, PhD, Teacher's College, Columbia University
- The primary focus of early interventions at disaster sites should be to promote a sense of safety and a calm atmosphere, instill hope, and connect victims and survivors with appropriate resources, according to post-9/11 research used to develop guidelines and strategies for the best post-disaster mental health care.

Other articles in the special issue include:

- Intelligence Gathering Post-9/11 Elizabeth F. Loftus, PhD, University of California, Irvine
- Communicating About the Risks of Terrorism (or Anything Else) Baruch Fischhoff, PhD, Carnegie Mellon University
- Psychology Out of the Laboratory: The Challenge of Violent Extremism Jeremy Ginges, PhD, New School for Social Research; Scott Atran, PhD, Centre National de la Recherche Scientifique-Institut; Jean Nicod, University of Michigan and John Jay College of Criminal Justice; Sonya Sachdeva, PhD, and Douglas Medin, PhD, Northwestern University
- Impacts of Psychological Science on National Security Agencies Post-9/11 Susan E. Brandon, PhD, Federal Bureau of Investigation
- Roles of Human Factors and Ergonomics in Meeting the Challenge of Terrorism Raymond S. Nickerson, PhD, Tufts University
- Intelligent Management of Intelligence Agencies: Beyond Accountability Ping-Pong Philip E. Tetlock, PhD, and Barbara A. Mellers, PhD, University of Pennsylvania
- What Should We Expect After the Next Attack? Roxane Cohen Silver, PhD, University of California, Irvine; Baruch Fischhoff, PhD, Carnegie Mellon University

# The Killing Of Bin Laden Worsened Americans' Views Of US Muslims

Source: http://www.medicalnewstoday.com/releases/231501.php

Instead of calming fears, the death of Osama bin Laden actually led more Americans to feel threatened by Muslims living in the United States, according to a new nationwide survey. In the weeks following the U.S. military campaign that killed bin Laden, the head of the terrorist organization Al Qaeda, American attitudes toward Muslim Americans took a significant negative shift, results showed.

Americans found Muslims living in the United States more threatening after bin Laden's death, positive perceptions of Muslims plummeted, and those surveyed were less likely to oppose restrictions on Muslim Americans' civil liberties. For example, in the weeks before bin Laden's death, nearly half of respondents described Muslim Americans as "trustworthy" and "peaceful." But only one-third of Americans agreed with these positive terms after the killing. Most of the changes in attitude happened among political liberals and moderates, whose views shifted to become more like those of conservatives, the survey found.

The shift in views can be explained by the fact that bin Laden's death reminded some Americans of why they may fear Muslims in the first place, said Erik Nisbet, assistant professor of communication at Ohio State University, and one of the leaders of the survey project. "The death of bin Laden was a focusing event. There was a lot of news coverage and a lot of discussion about Islam and Muslims and Muslim Americans," Nisbet said. "The frenzy of media coverage reminded people of terrorism and the Sept. 11 attacks and it primed them to think about Islam in terms of terrorism." In fact, while prior to bin Laden's death only 16 percent of respondents believed a terrorist attack in the United States was likely in the next few months, 40 percent believed an attack was likely after the killing. "That is going to have a negative effect on attitudes," Nisbet said.

The researchers' ability to find out how American attitudes changed after bin Laden's death was accidental, Nisbet said. Nisbet and Ohio State colleague Michelle Ortiz, also an assistant professor of communication, had commissioned the Survey Research Institute of Cornell University and the University of New Hampshire Survey Center to jointly conduct a national telephone poll of Americans beginning in early April. The survey focused on perceptions and attitudes about Muslim Americans. Interviews started on April 7, 2011, and 500 interviews were conducted prior to May 1, when bin Laden was killed. The remaining 341 interviews were conducted following the death. Many of the survey responses changed significantly after the killing, Nisbet said.

After bin Laden's death, 34 percent of Americans surveyed agreed that Muslims living in the United States "increased the likelihood." a terrorist attack." That was up from 27 percent prior to the killing. The percentage of respondents agreeing the Muslims in the United States are supportive of the country dropped from 62 percent to 52 percent. Americans were less likely to oppose restrictions on Muslim American civil liberties after the killing, Nisbet said. For example, public opposition to profiling individuals as potential terrorists based solely on being Muslim dropped from 71 percent to 63 percent. Likewise, opposition to requiring Muslims living in the United to register their whereabouts with the government dropped from two-thirds of respondents to about one-half.

Changes in attitudes were not related just to preventing a possible terrorist attack, but also included attitudes about religious tolerance of Muslims. For example, nearly one in three respondents surveyed after bin Laden's death agreed that "Muslims are mostly responsible for creating the religious tension that exists in the United States today." That was up from about one in five respondents before the killing. Correspondingly, opposition to a nationwide ban on mosque construction in the United States fell to 57 percent from 65 percent. The negative feelings even carried over to personal relationships. The percentage of respondents who said they were unwilling to have a Muslim as a close friend doubled after the death, going from 9 percent to 20 percent. "That's important because research has shown that the best way to reduce prejudice and improve intergroup relations is through personal contact," Nisbet said. "That won't happen if people avoid contact with Muslim Americans."

Many of the changes in attitudes after Bin Laden's death were almost entirely due to political liberals and moderates changing their opinions about the threat posed by Muslims in the United States, the survey found. The percentage of liberal respondents who agreed that Muslims in the United States "make America a more dangerous place to live" tripled after bin Laden's death, going from 8 to 24 percent. The percentage of moderates believing this increased from 10 percent to 29 percent.

In contrast, the percentage of conservatives who believed this were essentially unchanged -30 percent before bin Laden's death and 26 percent following. "Liberals and moderates essentially converged toward conservatives in their attitudes about Muslim Americans." Nisbet said. Nisbet said it is unclear whether these changes in attitudes would last long-term or not. But research suggests these negative feelings can be dangerous even if they are short-lived. "Every time these anti-Muslim feelings are activated by media coverage, it makes them that much easier to get reactivated in the future," Nisbet said. "These feelings and attitudes become more constant the more you experience them."

The telephone survey involved adults in the continental United States, including cell-phone only homes, and was designed to be representative of the U.S. population. All percentages reported here were adjusted to control for differences in the characteristics of survey respondents interviewed before and after bin Laden's death. The researchers controlled for age, gender, race, education, political ideology, whether the respondents were evangelical Christians, and their knowledge about Islam. That means any differences in attitudes between respondents polled before and after the death are not the results of any difference on these personal attributes. In addition to Nisbet and Ortiz, the survey was conducted by Yasamin Miller, director of the Survey Research Institute at Cornell and Andrew Smith, associate professor and director of the University of New Hampshire Survey Center.

# DHS unveils new Maritime security strategy

Source:http://urgentcomm.com/networks\_and\_systems/news/maritime-operations-coordination-plan-20110715/

Earlier this month DHS unveiled its Maritime Operations Coordination plan designed to more efficiently secure the nation's coastlines by increasing coordination and information sharing among agencies. "As America's maritime first responder, the Coast Guard works closely with our fellow DHS components and security partners to deter and respond to threats in our ports, along our coasts, and in waters of U.S. interest," said

Admiral Robert Papp, the commandant of the Coast Guard. "This plan will combine resources from across DHS to strengthen our ability to protect our nation's global trade and our citizens.

In particular, the new operation plans works to integrate intelligence sharing between the Coast Guard, Customs and Border Protection (CBP), and Immigration and Customs Enforcement (ICE).

John Morton, the head of ICE, echoed Admiral Papp's statements adding that the plan will help agencies to better "disrupt and dismantle criminal organizations who wish to do us harm." Federal officials say that the new plan recognizes the unique operational challenges of securing the maritime domain and the need for a multilevel approach to security that emphasizes information sharing between federal, state, local, tribal, and international partners.

The release of the strategy comes after Admiral Papp's testimony before the House Subcommittee on Border and Maritime Security. The admiral testified that the Coast Guard currently uses a layered security and communications plan to protect the nation's 350 ports and 95,000 miles of coast line.

# Growing problem in Canada: stolen passports

Source: http://www.homelandsecuritynewswire.com/growing-problem-canada-stolen-passports

Canadian passports are under siege, with more than 1,000 of them stolen across the country every month on average, Passport Canada has said. The disclosure was made in the agency's latest annual report, which says 13,077 passports were stolen in fiscal 2009-10. By comparison, only 631 were swiped overseas. Another 47,704 passports were reported lost in Canada. The Montreal Gazette

reports that before 2006, about 25,000 passports were reportedly lost or stolen annually. That number jumped to almost 43,000 in 2006-7, coinciding with a surge in demand because of new U.S. passport requirements for Canadian

and other Western travelers. By 2008-09, the number of lost or stolen passports reached 53,000, and now it is 60,781. The 60,781 lost and stolen passports in 2009-10 represent

# Full-body scanning for the shy

Source: http://www.homelandsecuritynewswire.com/full-body-scanning-shy

The Transportation and Security Administration will soon launch Full Body Scanning 2.0 at several New York area airports. Individuals who are shy about or uncomfortable with the detailed image of their bodies that appear on the screeners' computers should welcome the news. 0.3205 percent of the 18,962,745 passports in circulation as of April 2010, Beatrice Fenlon, Passport Canada's spokesperson, told the Gazette.

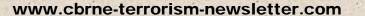
In 2008-9, the number of passports reported lost or stolen was 53,515, which represents 0.3145 percent of the 17,015,462 passports in circulation as of April 2009.

The year before that, 51,915 of the 15,515,042

passports in circulation were reported lost or stolen, representing 0.3346 percent of the total. The agency says that more than 4.8 million Canadian passports were issued in 2009, a 137 percent increase since 2000-1. Late next year, Passport

Canada will begin distributing e-Passports. The e-Passports have biometric and holographic security measures to combat tampering and fraud.

The new software, known as Automated Target Recognition (ATR), will auto-detect items that could pose a potential threat that passengers might be carrying under their clothes. The suspicious items, though, will be shown against a generic outline of a person for all passengers.





PC magazine reports that the new software will be installed at Newark, LaGuardia, and JFK airports by the end of the year. "Our top priority is the safety of the traveling public, and TSA constantly strives to explore and implement new technologies that enhance security and strengthen privacy protections for the traveling public," TSA Administrator John Pistole said in a statement.

TSA successfully tested the new software at Hartsfield-Jackson Atlanta International, Las Vegas McCarran International, and Ronald

Reagan Washington National airports. according to the agency. "This is a positive step forward to improve TSA's screening procedures at U.S. airports through increased privacy for individual travelers." said Representative Mike Rogers (R - Alabama), the chair of the House Homeland Security Subcommittee on Transportation Security.

The announcement comes in response to fierce criticism over the airport scanners which passengers and privacy groups say are too revealing. Last week, a federal appeals court rejected a lawsuit filed by the Electronic Privacy Information Center (EPIC) that argued that the scans violated the Fourth Amendment which protects against unreasonable search and seizure. The group said that the "naked" images are too graphic. Ginger McCall, EPIC's open government counsel, called TSA's recent announcement a "pretty substantial change in agency policy." The group wants TSA to go even further and publish the technical specifications of the software, but the agency has declined.

Meanwhile other privacy groups like the Association for Airline Passenger Rights want the agency to stop using the scanners all together.

Brandon Macsata, the executive director of the airline passenger association said, "We feel

there are better ways to balance security and privacy."

According to Greg Soule, a spokesman for TSA, the new software will be installed on the full body scanners in "the

coming months."

Currently there are roughly 500 body scanners deployed across seventy-eight airports in the United States. The scanners are manufactured by Rapiscan Systems, a division of L-3 Communications and OSI Systems Inc. All new scanners will already come equipped with the technology.

# Computational Models And Algorithms Cast Fresh Light On Terrorism In India

Source: http://www.medicalnewstoday.com/releases/231154.php

Recent advances in computer science at the



University of Maryland's Laboratory for Computational Cultural Dynamics cast fresh light on terrorism in India, such as the coordinated attacks in Mumbai. Some important conclusions from two forthcoming papers, accepted for publication at the 2011 European Conference on Intelligence Security Informatics and the 2011 Open Source Intelligence Conference in September 2011, suggest that reining in terror groups like Lashkar-e-Taiba (LeT), who carried out the devastating Mumbai attacks in Nov. 2008, can be done only with concurrent action by the United States and India and a reduction in US aid to Pakistan.

In order to understand how terrorism from



374

groups such as Lashkar-e-Taiba can be reduced, University of Maryland researchers led by Computer Science Professor V.S. Subrahmanian developed a number of mathematical models including stochastic opponent modeling agents and multi-player game theoretic models. The research team developed studied 5 entities - the US, India, the Pakistani military (including the Inter Services Intelligence agency), the Pakistani civilian funded by Pakistan's ISI intelligence agency", explained University of Maryland counterterrorism analyst Aaron Mannes. "The recent court trial in Chicago of two alleged LeT operatives, David Headley and Tahawwur Rana, strongly suggests an ISI hand in the deadly Mumbai terrorist attack in Nov. 2008."

"In addition to the results about trimming financial aid to Pakistan, we also found that



government (not including the military or ISI), and Lashkar-e-Taiba.

The researchers looked for Nash equilibria, named after Nobel-prize winning economist John Nash, whose life was immortalized in the Oscar-winning movie, A Beautiful Mind. Intuitively, Nash equilibria specify situations where no entity involved in the game theoretic model can ``do better" without upsetting another agency. "We did not find a single Nash equilibrium in which LeT exhibits good behavior in which the US expands financial aid to Pakistan," said Subrahmanian, who went on to remark that "This is consistent with the recent decision by the Obama administration to cut \$800M in military aid to Pakistan."

Nevertheless, "this would not be sufficient to de-fang groups like LeT that are reportedly there was not a single Nash equilibrium in which LeT exhibits good behavior in which both the US and India did not concurrently take either covert action against LeT and/or exercise coercive diplomacy toward Pakistan", said John Dickerson, a University of Maryland scientist who is also earning a doctorate at Carnegie-Mellon University. "The results do not imply that the US and India need to coordinate actions - just that the actions need to occur over an overlapping period of time that is sufficiently long to convince both the Pakistani military and the LeT that terrorist actions will not pay", said Subrahmanian.

In addition to researching Lashkar-e-Taiba, the University of Maryland team has also used their data mining algorithms to learn models of the behavior of other terrorist groups in the Indian sub-continent such as Jashar

Mohammed in Pakistan and the Indian Mujahideen - alleged by some to be responsible for the triple bombings in Mumbai that killed over 20 people. "Though it is too early to identify the perpetrators of the Mumbai attacks, computational models and algorithms can help decision makers shape improved counter-terrorism strategies and policies for threat reduction," said Subrahmanian.

#### V.S. Subrahmanian; J. Dickerson, A. Mannes, A. Sliva, J. Shakarian. University of Maryland

#### Gaping Holes in Intelligence on Overseas Terrorists

Source:http://www.foxnews.com/politics/2011/07/12/report-shows-gaping-holes-in-intel-on-overseas-terrorists/

Fox News has obtained a draft copy of a new Government Accountability Office (GAO) report that concludes, a decade after 9/11, gaping holes remain in databases of overseas terrorists as well as in passport security. "The system truly is as strong only as its weakest link," Maine Sen. Susan Collins, the senior Republican on the Senate Homeland Security Committee, told Fox News after reviewing the report. "We have spent literally billions of dollars to increase security, to make sure our watch lists are more complete, to verify documents, but in fact we have to rely to a certain extent on the systems used by other countries."

According to a year-long investigation by the GAO that included travel to Kenya, Pakistan, the Philippines and Thailand, many countries have yet to address the chronic problem of fake documents, such as birth certificates, which are a gateway to a genuine passport. Passport security is described as weak with many countries using no security features, such as biometrics, to prevent fraud.

The GAO report, first obtained by Fox News, reads in part:

"Some countries do not have their own database systems with terrorist screening information or access to other countries' terrorist screening information to keep track of biographical and biometric information about individuals who are known or suspected terrorists. Even when countries have terrorist screening information, they may not have reciprocal relationships to share such information or other travel-related information such as airline passenger lists, with other countries, thereby limiting their ability to identify and prevent travel of known or suspected terrorists."

The GAO report also notes widespread corruption means a wink and a nod at some

foreign airports will get a suspected terrorist through security.

Pakistan was problematic for investigators. Even with Usama bin Laden's death at his compound near the capital Islamabad, the country remains the base for Al Qaeda's core leadership, including Ayman al-Zawahiri, the Egyptian doctor who replaced the Al Qaeda leader. Yet, Pakistan's ability to track known and suspected terrorists is substandard.

"It is stunning, that Pakistan which is supposed to be our ally in the war against terrorism, does not even share fingerprint data within its own government," Collins told Fox News. "It doesn't share it with other Pakistani law enforcement agencies. That's a real problem."

While information sharing and passport security has improved in the U.S., the disparity overseas remains a serious problem.

"Fraudulent travel documents are the same as weapons to terrorists; they can't carry out their plots without them," Chad Sweet, co-founder of the Chertoff Group, told Fox News.

Sweet, who is a former chief of staff for the Homeland Security Department and once worked for the CIA's Directorate of Operations, says progress is being made overseas, but it has not kept pace with improvements to domestic security.

"On the defensive homeland game, we're probably at an A. If I give us a grade abroad, with our partners, again some of that is out of our control, we are probably closer to a C."

The GAO report will be officially released on Wednesday when the issue is taken up publicly by the Senate Homeland Security Committee. Sen. Joe Lieberman, who chairs the committee, called for an updated approach. "As part of our efforts to keep terrorists from entering the United States, we provide security assistance to foreign countries where terrorists are likely to begin their travels. Unfortunated

GAO has found miscommunication and overlap on the part of U.S. agencies trying to help our foreign partners," he said. "I urge the administration to update what is now a fiveyear-old strategy for preventing terrorist travel so that we can work as effectively as possible to keep terrorists out of the country and away from innocent Americans."

Collins told Fox that the issue has taken on more importance because the threat from Al Qaeda's affiliates in Somalia and Yemen is growing.

The Yemeni affiliate, which includes the American Cleric Anwar al-Awlaki among its leadership, was behind the last two major attempts on the U.S. using airplanes. It was also behind the recent threat intelligence that the group was trying to recruit a surgeon to surgically embed explosive devices in suicide bombers. The threat was not described, by U.S. officials, as imminent, but the intelligence was described as credible and another sign the Yemeni affiliate was thinking out of the box. "What this latest intelligence tells us about surgically implanting explosives is that Al Qaeda and its affiliates will continue to explore all possibilities to defeat the security that we have in place now," Collins explained. "And that is why the gaps that the GAO found are so troubling because inevitably there is going to be yet another attempt and the terrorists eventually are going to get through. We've got to do everything we can to put in place barriers to terrorists traveling to this country."

#### Securing critical infrastructure: portfolio based approach

Source:http://www.homelandsecuritynewswire.com/securing-critical-infrastructure-portfolio-based-approach

Bryan Ware, the CEO and co-founder of Digital Sandbox, a firm that provides risk analysis and management software and services to the private and public sectors, was recently interviewed by Homeland Security NewsWire's executive editor Eugene Chow; Ware discusses a portfolio based approach to securing critical infrastructure, what the government can do better to protect critical assets, and the dangers of taking a "Whack-a-Mole" tactic with national security threats

*Homeland Security NewsWire*: To start off with a broader question, what is the state of preparedness of our national critical infrastructure? Do the bulk of our nation's critical infrastructure operators have plans in place in the event of a large natural disaster or attack?

*Bryan Ware*: I think that critical infrastructure providers do have plans, but these plans are more in their business interest and may not necessarily be in the national security interest. Sometimes it may be obvious when the two interests are aligned, but I do not think that is the case all the time.

*HSNW*: The private sector controls the majority of critical infrastructure – electrical grids, financial markets, nuclear reactors – is there buy-in and support for the government's efforts to secure these resources from the private sector? Are they making moves independently or does the government need to do more to partner and incentivize them?

*BW*: I think the government definitely needs to do more, but I think the hard part is figuring out what the government should do and can do. Traditionally, or at least to date, the word partnering is thrown around a lot. I do not think we have arrived at any kind of meaningful partnership in many of the critical infrastructure sectors.

Incentivizing behavior is the direction I would like to see things go, but in general, of the threats and risks to critical infrastructure that we are concerned about, some of them are easy to see while others are hard to prove. The more emerging those threats or risks may be, the harder it is to build a business case. This is where the government needs to be able to provide incentives to help those critical infrastructure providers to develop that business case.



*HSNW*: To delve a bit deeper into that, the National Infrastructure Protection Plan (NIPP) heavily emphasizes partnering with the private sector. Is the government a good partner? What can they do to be better a partner for the private sector?

*BW:* In terms of what the government can really do, I would like to see more effective ways for information to be provided to critical infrastructure owners and operators. I would also like to see management from a portfolio standpoint where we can collaborate overall on the systems of assets. Finally, I would like to see DHS provide tools that the owners and operators could actually use to manage their risks.

HSNW: What kinds of tools are you referring to? Can you elaborate on that a bit more?

*BW*: When I say tools, I think of ways that businesses can manage all of their critical infrastructure, the information about threats to that critical infrastructure, how prepared they are, and where the gaps in their preparedness are. When I think of that, I think of software tools. This has to go from an ad-hoc meeting driven and speech driven discipline into part of day to day operations. Think of enterprise resource planning (ERP), every business and critical infrastructure operator has core systems for managing the enterprise. We need to make this critical infrastructure protection a part of that in its own way. It is like having ERP for risk management and ERP for homeland security.

There has certainly been a lot of investment that has been made at DHS with this system as a tool, but they are very much internal and they are kind of fractured. I think exposing them, trying to figure out how to leverage industry practices, and tie DHS and industry together more closely would be a very exciting development.

*HSNW*: At the Government Security conference in March, you outlined a very interesting approach to risk management and infrastructure protection, likening it to managing a shifting portfolio of risks. Can you elaborate on that?

*BW*: When you think about a big piece of critical infrastructure, it is easy to imagine sending some guys out, doing a security assessment, and having a plan for that particular asset that says what you are going to do in the case of a particular event. What is challenging though is when you have a lot of assets that you are supposed to protect. Take for instance, the chemical sector or the financial services sector as a whole or a particular business if their assets are distributed around the country or the world – that is a lot of assets and when you think about all the threats that could yield some kind a catastrophic event. These threats range from natural hazards like hurricanes, earthquakes, and tornadoes – and we are seeing plenty of those in the Mid-West – to terrorism scenarios.

When you look at all of those different threats and hazards against all those different types of assets and you look at the combinations and scenarios – which ones are more likely to happen, which assets are more vulnerable to different types of events, and which ones would drive greater consequences both from a business standpoint and from a homeland security stand point – in my mind, there is no other way to look at that than with a portfolio approach. In particular, you need a portfolio of assets that you can slice and dice by geography, critical infrastructure type, sectors, vulnerabilities, or by the ones that would produce the greatest consequences. You would also need to have a portfolio of threats with information on the likelihood of the different types of things to happen, but you also need to know the ones that may not be very likely but would have completely unacceptable consequences.

From those portfolios, and only from those portfolios, can you take a strategic risk management approach where you say, "This is where I am going to focus my priorities on, these threats I think are the most likely while these are the most likely to disrupt us, and these critical infrastructure and these key resources are most essential to maintaining the national economy, the national defense," – or whatever your goal is.



*HSNW*: It seems that this portfolio is real time and shifting where it is constantly adjusting to the threats that are emerging on the horizon. Is such an approach feasible given that there are so many decentralized elements and a finite amount of resources? Is it realistic that companies can actually shift resources and focus in time to respond to these emerging threats?

*BW*: Yes it is. We already treat properties with this portfolio idea in the same way people treat their stocks, bonds, and investments. All of these are very portfolio driven because whenever you have too many things you have to go with that kind of approach.

Everything we advocate for is software driven, so as things change you are able to immediately update your risk. Outside of cyber, risk is not changing every minute like the stock market is. Instead what we see in practice is that assets do change – they take on new missions, buildings or operations may shut down and move to a new place, or a new security assessment is done that lends some additional insight into particular vulnerabilities and some additional counter-measures are put in place. The threat dynamic and the threat environment also change – new threats emerge and there are alerts and warnings.

It is practical without a lot of manpower and resources to secure all these critical assets if you have a portfolio management system that is able to track all those variables at the same time to see how your risk is changing. The portfolio approach also helps to judge risk not just in the present, but also to see where things are going in the future so you can build a long term strategy or plan to secure your enterprise.

*HSNW*: Naturally, from the federal perspective there is going to be a certain perspective or priority that differs from local and state governments. How do you reconcile these differences to ensure that all sides are working together and have unity of effort?

*BW*: This is a really important point and I think this is a point that is lost on federal agencies and their representatives almost all the time. What is important to the federal government is not necessarily the thing that is considered important to a local government and this holds true for industries as well.

The easiest example to draw out is from the defense industrial base. There could be a manufacturer of a very specific kind of composite chemical that is needed for armor. They may not employ a whole lot of people or drive a lot of revenue for a community, but it is nationally important to the defense mission as it is a critical supplier that would have a huge impact on the DOD's abilities. To local authorities it could be one of their smaller businesses, one that they may not even know about, so making it critical to them is difficult to imagine.

The way that you balance this is you have to separate the concept, what we call the "domain model," from the things that a business, local government, or federal agency thinks are important. In other words, you have to separate individual value judgments from the facts. The facts are it has an address, a number of employees, it occupies a certain part of the infrastructure taxonomy that it lives in, and it has an annual revenue. That whole series of attributes is factual data regardless of your opinion or your belief about it.From there, you can compile this data and then apply your judgment from your perspective. In practice those same assets may look different to the DHS than they do to a city, a state, or a corporation, but we can all agree and share information on the same particular set of assets.

*HSNW*: In the wake of the massive 11 March earthquake that struck Japan, have you noticed any changes in the mindsets of critical infrastructure operators in terms of having plans in place?

*BW*: I still think it is a still a little too early to tell what is happening in terms of the fallout from those events. Companies are only starting to explore ways to understand, manage, and plan for catastrophic events in the aftermath of Japan.



But, one of the things that is very interesting from the U.S. perspective is we saw plants in the United States idling because of critical commodities or products that they could only get from Japan. I can imagine a case in which an individual auto manufacturing plant in Tennessee could have the best continuity plans with redundant power, good security, and good operational controls to make sure that the plant continues to operate, but if those supplies are not coming in the front door, the plant will idle.

These concerns are very similar to what the cyber world is about as they are many steps removed from what a business can begin to manage and plan for. In other words, like in cyber, your vulnerabilities may not be about your defenses or your critical resources, but things that are many degrees outside of your static control that may impact you.

*HSNW*: Speaking of cyber, what are your thoughts on the Obama administration's new cybersecurity plan? In particular, what are your thoughts on the proposed provision of having government oversight where DHS reviews a company's cybersecurity plan and will actually penalize them if it is found to be inadequate?

*BW*: As I read through the plan and think about it, I wonder how it is going to be implemented. I think that implementation is always a challenge with these plans. I do not know that the government feels like it is doing the best job at implementing its own cybersecurity plans and securing its own assets, so how it will look at businesses and their cybersecurity plans will be a big challenge.

This is a new frontier and I like that there is leadership. Every day you read about major intrusions into the networks of large companies that you would think are very serious and have significant capabilities. We are seeing a very hostile environment out there and we do not really have good technology, business practices, standards, or the penalties to go along with it.

I think we need to translate a lot of this stuff into business terms. Businesses are going to have business impacts and we need to separate those business impacts from national security impacts. The government needs to focus first on the things that they need to do to protect cyberspace from a national security standpoint.

*HSNW*: Of late the majority of attention seems to be focused on cybersecurity and cyber threats to critical infrastructure, but what element of critical infrastructure do you see as being overlooked that needs some attention?

*BW*: That is a hard question. I think we have a very broad economy and all of the different types of infrastructure yield different targets from a terrorism or natural catastrophe standpoint, so the focus has to be broad and holistic. This is why I am such an advocate of looking broadly at large portfolios and not trying to focus exclusively on the most critical asset or the most critical asset in a particular sector.

You have to be careful when you say "Which of the industry or sector should we be most focused on?" because if you do that you run into a game of "Whack-a-Mole" where all of a sudden something pops up and you divert your focus to the chemical sector or the nuclear sector.

What we are seeing now is threats on urban rail from the intelligence seized from the bin Laden compound. Was urban rail a critical priority before? I am not so sure it was if you look at funding and other things. Not so long ago, we became very focused on large hotels because the Mumbai attacks and the realization that we had those same kind of assets here.

So, again, my belief is we need to be prioritizing all of our threats, vulnerabilities, consequences across all of the industry sectors in a portfolio based approach so we are able to react quickly to something new and urgent, but still have a strategic program where we are constantly trying to increase the depth and breadth of our knowledge about our assets.

*HSI***W**: Finally to wrap things up, if you were responsible for NIPP and had a clichéd magic wand, what would be the first three things you would do to secure critical infrastructure?

*BW*: I come at this question from the perspective of a relatively focused company, so the way we would look at it is I would first like to see a real program to partner with industry and state and local governments to build a comprehensive library or portfolio of the critical assets that we are supposed to protect. The second thing I would do is gather that data and analyze it so we can all agree on what our national priorities are. We cannot secure everything as well as we would like to, so we need to prioritize where we want to spend our resources. From there we can develop a long term resource plan for how we are going to take care of those vulnerabilities, harden those facilities, and how we are going to deal with those threats that we face overall.

So for me, my three actions would be to set up a system where we bring everyone together, prioritize all those things that we are trying to protect, and based on those priorities set out on a real risk management program. I do not know how much of it is defenses, cyber, or counter-surveillance programs because I do not think we have put together a comprehensive look across the country of what it is we are trying to do yet.

# **Getting Bin Laden**

What happened that night in Abbottabad. By Nicholas Schmidle (The New Yorker Magazine)

Source: http://www.newyorker.com/reporting/2011/08/08/110808fa\_fact\_schmidle

No American was yet inside the residential part of the compound. The operatives had barely been on target for a minute, and the mission was already veering off course. Shortly after eleven o'clock on the night of May 1st, two MH-60 Black Hawk helicopters lifted off from Jalalabad Air Field, in eastern Afghanistan, and embarked on a covert mission into Pakistan to kill Osama bin Laden. Inside the aircraft were twenty-three Navy SEALs from Team Six, which is officially known as the Naval Special Warfare Development Group, or DEVGRU. A Pakistani-American translator, whom I will call Ahmed, and a dog named Cairo-a Belgian Malinois-were also aboard. It was a moonless evening, and the helicopters' pilots, wearing night-vision goggles, flew without lights over mountains that straddle the border with Pakistan. Radio communications were kept to a minimum, and an eerie calm settled inside the aircraft.

Fifteen minutes later, the helicopters ducked into an alpine valley and slipped, undetected, into Pakistani airspace. For more than sixty years, Pakistan's military has maintained a state of high alert against its eastern neighbor, India. Because of this obsession, Pakistan's "principal air defenses are all pointing east," Shuja Nawaz, an expert on the Pakistani Army and the author of "Crossed Swords: Pakistan, Its Army, and the Wars Within," told me. Senior defense and Administration officials concur with this assessment, but a Pakistani senior military official, whom I reached at his office, in Rawalpindi, disagreed. "No one leaves their borders unattended," he said. Though he declined to elaborate on the location or orientation of Pakistan's radars-"It's not where the radars are or aren't"-he said that the American infiltration was the result of "technological gaps we have vis-à-vis the U.S." The Black Hawks, each of which had two pilots and a crewman from the 160th Special Operations Aviation Regiment, or the Night Stalkers, had been modified to mask heat, noise, and movement; the copters' exteriors had sharp, flat angles and were covered with radar-dampening "skin."

The SEALs' destination was a house in the small city of Abbottabad, which is about a hundred and twenty miles across the Pakistan border. Situated north of Islamabad, Pakistan's capital, Abbottabad is in the foothills of the Pir Panjal Range, and is popular in the summertime with families seeking relief from the blistering heat farther south. Founded in 1853 by a British major named James Abbott, the city became the home of a prestigious military academy after the creation of Pakistan, in 1947. According to information gathered by the Central Intelligence Agency, bin Laden was holed up on the third floor of a house in a one.

acre compound just off Kakul Road in Bilal Town, a middle-class neighborhood less than a mile from the entrance to the academy. If all went according to plan, the SEALs would drop from the helicopters into the compound, overpower bin Laden's guards, shoot and kill him at close range, and then take the corpse back to Afghanistan.

The helicopters traversed Mohmand, one of Pakistan's seven tribal areas, skirted the north of Peshawar, and continued due east. The commander of DEVGRU's Red Squadron, laminated gridded map of the compound. In another pocket was a booklet with photographs and physical descriptions of the people suspected of being inside. He wore a noisecancelling headset, which blocked out nearly everything besides his heartbeat.

During the ninety-minute helicopter flight, James and his teammates rehearsed the operation in their heads. Since the autumn of 2001, they had rotated through Afghanistan, Iraq, Yemen, and the Horn of Africa, at a brutal pace. At least three of the SEALs had



whom I will call James, sat on the floor, squeezed among ten other SEALs, Ahmed, and Cairo. (The names of all the covert operators mentioned in this story have been changed.) James, a broad-chested man in his late thirties, does not have the lithe swimmer's frame that one might expect of a SEAL-he is built more like a discus thrower. That night, he wore a shirt and trousers in Desert Digital Camouflage, and carried a silenced Sig Sauer P226 pistol, along with extra ammunition; a CamelBak, for hydration; and gel shots, for endurance. He held a short-barrel, silenced M4 rifle. (Others SEALs had chosen the Heckler & Koch MP7.) A "blowout kit," for treating field trauma, was tucked into the small of James's back. Stuffed into one of his pockets was a

participated in the sniper operation off the coast of Somalia, in April, 2009, that freed Richard Phillips, the captain of the Maersk Alabama, and left three pirates dead. In October, 2010, a DEVGRU team attempted to rescue Linda Norgrove, a Scottish aid worker who had been kidnapped in eastern Afghanistan by the Taliban. During a raid of a Taliban hideout, a SEAL tossed a grenade at an insurgent, not realizing that Norgrove was nearby. She died from the blast. The mistake haunted the SEALs who had been involved; three of them were subsequently expelled from DEVGRU.

The Abbottabad raid was not DEVGRU's maiden venture into Pakistan, either. The team had surreptitiously entered the country on team.

to twelve previous occasions, according to a special-operations officer who is deeply familiar with the bin Laden raid. Most of those missions were forays into North and South Waziristan, where many military and intelligence analysts had thought that bin Laden and other Al Qaeda leaders were hiding. (Only one such operation-the September, 2008, raid of Angoor Ada, a village in South Waziristan-has been widely reported.) Abbottabad was, by far, the farthest that DEVGRU had ventured into Pakistani territory. It also represented the team's first serious attempt since late 2001 at killing "Crankshaft"-the target name that the Joint Special Operations Command, or JSOC, had given bin Laden. Since escaping that winter during a battle in the Tora Bora region of eastern Afghanistan, bin Laden had defied American efforts to trace him. Indeed, it remains unclear how he ended up living in Abbottabad.

Forty-five minutes after the Black Hawks departed, four MH-47 Chinooks launched from the same runway in Jalalabad. Two of them flew to the border, staying on the Afghan side; the other two proceeded into Pakistan. Deploying four Chinooks was a last-minute decision made after President Barack Obama said he wanted to feel assured that the Americans could "fight their way out of Pakistan." Twenty-five additional SEALs from DEVGRU, pulled from a squadron stationed in Afghanistan, sat in the Chinooks that remained at the border; this "quick-reaction force" would be called into action only if the mission went seriously wrong. The third and fourth Chinooks were each outfitted with a pair of M134 Miniguns. They followed the Black Hawks' initial flight path but landed at a predetermined point on a dry riverbed in a wide, unpopulated valley in northwest Pakistan. The nearest house was half a mile away. On the ground, the copters' rotors were kept whirring while operatives monitored the surrounding hills for encroaching Pakistani helicopters or fighter jets. One of the Chinooks was carrying fuel bladders, in case the other aircraft needed to refill their tanks.

Meanwhile, the two Black Hawks were quickly approaching Abbottabad from the northwest, hiding behind the mountains on the northernmost edge of the city. Then the pilots banked right and went south along a ridge that marks Abbottabad's eastern perimeter. When those hills tapered off, the pilots curled right again, toward the city center, and made their final approach.

During the next four minutes, the interior of the Black Hawks rustled alive with the metallic cough of rounds being chambered. Mark, a master chief petty officer and the ranking noncommissioned officer on the operation, crouched on one knee beside the open door of the lead helicopter. He and the eleven other SEALs on "helo one," who were wearing gloves and had on night-vision goggles, were preparing to fast-rope into bin Laden's yard. They waited for the crew chief to give the signal to throw the rope. But, as the pilot passed over the compound, pulled into a high hover, and began lowering the aircraft, he felt the Black Hawk getting away from him. He sensed that they were going to crash.

One month before the 2008 Presidential election, Obama, then a senator from Illinois, squared off in a debate against John McCain in an arena at Belmont University, in Nashville. A woman in the audience asked Obama if he would be willing to pursue Al Qaeda leaders inside Pakistan, even if that meant invading an ally nation. He replied, "If we have Osama bin Laden in our sights and the Pakistani government is unable, or unwilling, to take them out, then I think that we have to act and we will take them out. We will kill bin Laden. We will crush Al Qaeda. That has to be our biggest national-security priority." McCain, who often criticized Obama for his naïveté on foreign-policy matters, characterized the promise as foolish, saying, "I'm not going to telegraph my punches."

Four months after Obama entered the White House, Leon Panetta, the director of the C.I.A., briefed the President on the agency's latest programs and initiatives for tracking bin Laden. Obama was unimpressed. In June, 2009, he drafted a memo instructing Panetta to create a "detailed operation plan" for finding the Al Qaeda leader and to "ensure that we have expended every effort." Most notably, the President intensified the C.I.A.'s classified drone program; there were more missile strikes inside Pakistan during Obama's first year in office than in George W. Bush's eight. The terrorists swiftly registered the impact: that July, CBS reported that a recent Al Qaeda referred communiqué had to "brave commanders" who had been "snatched away" and to "so many hidden homes [which] have been levelled." The document blamed the "ver

grave" situation on spies who had "spread throughout the land like locusts." Nevertheless, bin Laden's trail remained cold.

In August, 2010, Panetta returned to the White House with better news. C.I.A. analysts believed that they had pinpointed bin Laden's courier, a man in his early thirties named Abu Ahmed al-Kuwaiti. Kuwaiti drove a white S.U.V. whose spare-tire cover was emblazoned with an image of a white rhino. The C.I.A. began tracking the vehicle. One day, a satellite captured images of the S.U.V. pulling into a large concrete compound in Abbottabad. Agents, determining that Kuwaiti was living there, used aerial surveillance to keep watch on the compound, which consisted of a threestory main house, a guesthouse, and a few outbuildings. They observed that residents of the compound burned their trash, instead of putting it out for collection, and concluded that the compound lacked a phone or an Internet connection. Kuwaiti and his brother came and went, but another man, living on the third floor, never left. When this third individual did venture outside, he stayed behind the compound's walls. Some analysts speculated that the third man was bin Laden, and the agency dubbed him the Pacer.

Obama, though excited, was not yet prepared to order military action. John Brennan, Obama's counterterrorism adviser, told me that the President's advisers began an "interrogation of the data, to see if, by that interrogation, you're going to disprove the theory that bin Laden was there." The C.I.A. intensified its intelligence-collection efforts, and, according to a recent report in the Guardian, a physician working for the agency conducted an immunization drive in Abbottabad, in the hope of acquiring DNA samples from bin Laden's children. (No one in the compound ultimately received any immunizations.)

In late 2010, Obama ordered Panetta to begin exploring options for a military strike on the compound. Panetta contacted Vice-Admiral Bill McRaven, the SEAL in charge of JSOC. Traditionally, the Army has dominated the special-operations community, but in recent years the SEALs have become a more prominent presence; McRaven's boss at the time of the raid, Eric Olson—the head of Special Operations Command, or SOCOM—is a Navy admiral who used to be a commander of DEVGRU. In January, 2011, McRaven asked a JSOC official named Brian, who had previously been а DEVGRU deputy commander, to present a raid plan. The next month, Brian, who has the all-American look of a high-school guarterback, moved into an unmarked office on the first floor of the C.I.A.'s printing plant, in Langley, Virginia. Brian covered the walls of the office with topographical maps and satellite images of the Abbottabad compound. He and half a dozen JSOC officers were formally attached to the Pakistan/Afghanistan department of the C.I.A.'s Counterterrorism Center, but in practice they operated on their own. A senior counterterrorism official who visited the JSOC redoubt described it as an enclave of unusual secrecy and discretion. "Everything they were working on was closely held," the official said. The relationship between special-operations units and the C.I.A. dates back to the Vietnam War. But the line between the two communities has increasingly blurred as C.I.A. officers and military personnel have encountered one another on multiple tours of Iraq and Afghanistan. "These people grew up together," a senior Defense Department official told me. "We are in each other's systems, we speak each other's languages." (Exemplifying this trend, General David H. Petraeus, the former commanding general in Irag and Afghanistan, is now the incoming head of the C.I.A., and Panetta has taken over the Department of Defense.) The bin Laden mission-plotted at C.I.A. headquarters and authorized under C.I.A. legal statutes but conducted by Navy DEVGRU operators-brought the coöperation between the agency and the Pentagon to an even higher level. John Radsan, a former assistant general counsel at the C.I.A., said that the Abbottabad raid amounted to "a complete incorporation of JSOC into a C.I.A. operation."

On March 14th, Obama called his nationalsecurity advisers into the White House Situation Room and reviewed a spreadsheet listing possible courses of action against the Abbottabad compound. Most were variations of either a JSOC raid or an airstrike. Some versions included coöperating with the Pakistani military; some did not. Obama decided against informing or working with Pakistan. "There was a real lack of confidence that the Pakistanis could keep this secret for more than a nanosecond," a senior adviser to the President told me. At the end of the meeting, Obama instructed McRaven to proceed with planning the raid.

Brian invited James, the commander of DEVGRU's Red Squadron, and Mark, the master chief petty officer, to join him at C.I.A. headquarters. They spent the next two and a half weeks considering ways to get inside bin Laden's house. One option entailed flying helicopters to a spot outside Abbottabad and letting the team sneak into the city on foot. The risk of detection was high, however, and the SEALs would be tired by a long run to the compound. The planners had contemplated tunnelling in-or, at least, the possibility that bin Laden might tunnel out. But images provided by the National Geospatial-Intelligence Agency showed that there was standing water in the vicinity, suggesting that the compound sat in a flood basin. The water table was probably just below the surface, making tunnels highly unlikely. Eventually, the planners agreed that it made the most sense to fly directly into the compound. "Special operations is about doing what's not expected, and probably the least expected thing here was that a helicopter would come in, drop guys on the roof, and land in the yard," the specialoperations officer said.

On March 29th, McRaven brought the plan to Obama. The President's military advisers were divided. Some supported a raid, some an airstrike, and others wanted to hold off until the intelligence improved. Robert Gates, the Secretary of Defense, was one of the most outspoken opponents of a helicopter assault. Gates reminded his colleagues that he had been in the Situation Room of the Carter White House when military officials presented Eagle Claw-the 1980 Delta Force operation that aimed at rescuing American hostages in Tehran but resulted in a disastrous collision in the Iranian desert, killing eight American soldiers. "They said that was a pretty good idea, too," Gates warned. He and General James Cartwright, the vice-chairman of the Joint Chiefs, favored an airstrike by B-2 Spirit bombers. That option would avoid the risk of having American boots on the ground in Pakistan. But the Air Force then calculated that a payload of thirty-two smart bombs, each weighing two thousand pounds, would be required to penetrate thirty feet below ground, insuring that any bunkers would collapse. "That much ordnance going off would be the equivalent of an earthquake," Cartwright told

me. The prospect of flattening a Pakistani city made Obama pause. He shelved the B-2 option and directed McRaven to start rehearsing the raid.

Brian, James, and Mark selected a team of two dozen SEALs from Red Squadron and told them to report to a densely forested site in North Carolina for a training exercise on April 10th. (Red Squadron is one of four squadrons in DEVGRU, which has about three hundred operators in all.) None of the SEALs, besides James and Mark, were aware of the C.I.A. intelligence on bin Laden's compound until a lieutenant commander walked into an office at the site. He found a two-star Army general from JSOC headquarters seated at a conference table with Brian, James, Mark, and several analysts from the C.I.A. This obviously wasn't a training exercise. The lieutenant commander was promptly "read in." A replica of the compound had been built at the site, with walls and chain-link fencing marking the layout of the compound. The team spent the next five days practicing maneuvers.

On April 18th, the DEVGRU squad flew to Nevada for another week of rehearsals. The practice site was a large government-owned stretch of desert with an elevation equivalent to the area surrounding Abbottabad. An extant building served as bin Laden's house. Aircrews plotted out a path that paralleled the flight from Jalalabad to Abbottabad. Each night after sundown, drills commenced. Twelve SEALs, including Mark, boarded helo one. Eleven SEALs, Ahmed, and Cairo boarded helo two. The pilots flew in the dark, arrived at the simulated compound, and settled into a hover while the SEALs fast-roped down. Not everyone on the team was accustomed to helicopter assaults. Ahmed had been pulled from a desk job for the mission and had never descended a fast rope. He quickly learned the technique.

The assault plan was now honed. Helo one was to hover over the yard, drop two fast ropes, and let all twelve SEALs slide down into the yard. Helo two would fly to the northeast corner of the compound and let out Ahmed, Cairo, and four SEALs, who would monitor the perimeter of the building. The copter would then hover over the house, and James and the remaining six SEALs would shimmy down to the roof. As long as everything was cordial, Ahmed would hold curious neighbors at bay. The SEALs and the dog could assist aggressively, if needed. Then, if bin Laden was proving difficult to find, Cairo could be sent into the house to search for false walls or hidden doors. "This wasn't a hard op," the specialoperations officer told me. "It would be like hitting a target in McLean"—the upscale Virginia suburb of Washington, D.C.

A planeload of guests arrived on the night of April 21st. Admiral Mike Mullen, the chairman of the Joint Chiefs, along with Olson and McRaven, sat with C.I.A. personnel in a hangar as Brian, James, Mark, and the pilots presented a brief on the raid, which had been named Operation Neptune's Spear. Despite JSOC's lead role in Neptune's Spear, the mission officially remained a C.I.A. covert operation. The covert approach allowed the White House to hide its involvement, if necessary. As the counterterrorism official put it recently, "If you land and everybody is out on a milk run, then you get the hell out and no one knows." After describing the operation, the briefers fielded questions: What if a mob surrounded the compound? Were the SEALs prepared to shoot civilians? Olson, who received the Silver Star for valor during the 1993 "Black Hawk Down" episode, in Mogadishu, Somalia, worried that it could be politically catastrophic if a U.S. helicopter were shot down inside Pakistani territory. After an hour or so of questioning, the senior officers intelligence analysts returned to and Washington. Two days later, the SEALs flew back to Dam Neck, their base in Virginia.

On the night of Tuesday, April 26th, the SEAL team boarded a Boeing C-17 Globemaster at Naval Air Station Oceana, a few miles from Dam Neck. After a refuelling stop at Ramstein Air Base, in Germany, the C-17 continued to Bagram Airfield, north of Kabul. The SEALs spent a night in Bagram and moved to Jalalabad on Wednesday.

That day in Washington, Panetta convened more than a dozen senior C.I.A. officials and analysts for a final preparatory meeting. Panetta asked the participants, one by one, to declare how confident they were that bin Laden was inside the Abbottabad compound. The counterterrorism official told me that the percentages "ranged from forty per cent to ninety or ninety-five per cent," and added, "This was a circumstantial case."

Panetta was mindful of the analysts' doubts, but he believed that the intelligence was better than anything that the C.I.A. had gathered on bin Laden since his flight from Tora Bora. Late on Thursday afternoon, Panetta and the rest of the national-security team met with the President. For the next few nights, there would be virtually no moonlight over Abbottabad-the ideal condition for a raid. After that, it would be another month until the lunar cycle was in its darkest phase. Several analysts from the National Counterterrorism Center were invited to critique the C.I.A.'s analysis; their confidence in the intelligence ranged between forty and sixty per cent. The center's director, Michael Leiter, said that it would be preferable to wait for stronger confirmation of bin Laden's presence in Abbottabad. Yet, as Ben Rhodes, a deputy national-security adviser, put it to me recently, the longer things dragged on, the greater the risk of a leak, "which would have upended the thing." Obama adjourned the meeting just after 7 P.M. and said that he would sleep on it.

The next morning, the President met in the Map Room with Tom Donilon, his nationalsecurity adviser, Denis McDonough, a deputy adviser, and Brennan. Obama had decided to go with a DEVGRU assault, with McRaven choosing the night. It was too late for a Friday attack, and on Saturday there was excessive cloud cover. On Saturday afternoon, McRaven and Obama spoke on the phone, and McRaven said that the raid would occur on Sunday night. "Godspeed to you and your forces," Obama told him. "Please pass on to them my personal thanks for their service and the message that I personally will be following this mission very closely."

On the morning of Sunday, May 1st, White House officials cancelled scheduled visits, ordered sandwich platters from Costco, and transformed the Situation Room into a war room. At eleven o'clock, Obama's top advisers began gathering around a large conference table. A video link connected them to Panetta, at C.I.A. headquarters, and McRaven, in Afghanistan. (There were at least two other command centers, one inside the Pentagon and one inside the American Embassy in Islamabad.)

Brigadier General Marshall Webb, an assistant commander of JSOC, took a seat at the end of a lacquered table in a small adjoining office and turned on his laptop. He opened multiple chat windows that kept him, and the White House, connected with the other command teams. The office where Webb sat had the only

video feed in the White House showing realtime footage of the target, which was being shot by an unarmed RQ 170 drone flying more than fifteen thousand feet above Abbottabad. The JSOC planners, determined to keep the operation as secret as possible, had decided against using additional fighters or bombers. "It just wasn't worth it," the special-operations officer told me. The SEALs were on their own. Obama returned to the White House at two o'clock, after playing nine holes of golf at Andrews Air Force Base. The Black Hawks departed from Jalalabad thirty minutes later. Just before four o'clock, Panetta announced to the group in the Situation Room that the helicopters were approaching Abbottabad. Obama stood up. "I need to watch this," he said, stepping across the hall into the small office and taking a seat alongside Webb. Vice-President Joseph Biden, Secretary Gates, and Secretary of State Hillary Clinton followed him, as did anyone else who could fit into the office. On the office's modestly sized LCD screen, helo one-grainy and black-and-whiteappeared above the compound, then promptly ran into trouble.

When the helicopter began getting away from the pilot, he pulled back on the cyclic, which controls the pitch of the rotor blades, only to find the aircraft unresponsive. The high walls of the compound and the warm temperatures had caused the Black Hawk to descend inside its own rotor wash-a hazardous aerodynamic situation known as "settling with power." In North Carolina, this potential problem had not become apparent, because the chain-link fencing used in rehearsals had allowed air to flow freely. A former helicopter pilot with extensive special-operations experience said of the pilot's situation, "It's pretty spooky-l've been in it myself. The only way to get out of it is to push the cyclic forward and fly out of this vertical silo you're dropping through. That solution requires altitude. If you're settling with power at two thousand feet, you've got plenty of time to recover. If you're settling with power at fifty feet, you're going to hit the ground."

The pilot scrapped the plan to fast-rope and focussed on getting the aircraft down. He aimed for an animal pen in the western section of the compound. The SEALs on board braced themselves as the tail rotor swung around, scraping the security wall. The pilot jammed the nose forward to drive it into the dirt and prevent his aircraft from rolling onto its side. Cows, chickens, and rabbits scurried. With the Black Hawk pitched at a forty-five-degree angle astride the wall, the crew sent a distress call to the idling Chinooks.

James and the SEALs in helo two watched all this while hovering over the compound's northeast corner. The second pilot, unsure whether his colleagues were taking fire or experiencing mechanical problems, ditched his plan to hover over the roof. Instead, he landed in a grassy field across the street from the house.

No American was yet inside the residential part of the compound. Mark and his team were inside a downed helicopter at one corner, while James and his team were at the opposite end. The teams had barely been on target for a minute, and the mission was already veering off course.

"Eternity is defined as the time be tween when you see something go awry and that first voice report," the special-operations officer said. The officials in Washington viewed the aerial footage and waited anxiously to hear a military communication. The senior adviser to the President compared the experience to watching "the climax of a movie."

After a few minutes, the twelve SEALs inside helo one recovered their bearings and calmly relayed on the radio that they were proceeding with the raid. They had conducted so many operations over the past nine years that few things caught them off guard. In the months after the raid, the media have frequently suggested that the Abbottabad operation was as challenging as Operation Eagle Claw and the "Black Hawk Down" incident, but the senior Defense Department official told me that "this was not one of three missions. This was one of almost two thousand missions that have been conducted over the last couple of years, night after night." He likened the routine of evening raids to "mowing the lawn." On the night of May 1st alone, special-operations forces based in Afghanistan conducted twelve other missions; according to the official, those operations captured or killed between fifteen and twenty targets. "Most of the missions take off and go left," he said. "This one took off and went right." Minutes after hitting the ground, Mark and the other team members began streaming out the side doors of helo one. Mud sucked at the

boots as they ran alongside a ten-foot-high wall that enclosed the animal pen. A three-man demolition unit hustled ahead to the pen's closed metal gate, reached into bags containing explosives, and placed C-4 charges on the hinges. After a loud bang, the door fell open. The nine other SEALs rushed forward, ending up in an alleylike driveway with their backs to the house's main entrance. They moved down the alley, silenced rifles pressed against their shoulders. Mark hung toward the rear as he established radio communications with the other team. At the end of the driveway, the Americans blew through yet another locked gate and stepped into a courtyard facing the guesthouse, where Abu Ahmed al-Kuwaiti, bin Laden's courier, lived with his wife and four children.

Three SEALs in front broke off to clear the guesthouse as the remaining nine blasted through another gate and entered an inner courtyard, which faced the main house. When the smaller unit rounded the corner to face the doors of the guesthouse, they spotted Kuwaiti running inside to warn his wife and children. The Americans' night-vision goggles cast the scene in pixellated shades of emerald green. Kuwaiti, wearing a white shalwar kameez, had grabbed a weapon and was coming back outside when the SEALs opened fire and killed him.

The nine other SEALs, including Mark, formed three-man units for clearing the inner courtyard. The Americans suspected that several more men were in the house: Kuwaiti's thirty-three-year-old brother, Abrar; bin Laden's sons Hamza and Khalid; and bin Laden himself. One SEAL unit had no sooner trod on the paved patio at the house's front entrance when Abrar—a stocky, mustachioed man in a cream-colored shalwar kameez—appeared with an AK-47. He was shot in the chest and killed, as was his wife, Bushra, who was standing, unarmed, beside him.

Outside the compound's walls, Ahmed, the translator, patrolled the dirt road in front of bin Laden's house, as if he were a plainclothes Pakistani police officer. He looked the part, wearing a shalwar kameez atop a flak jacket. He, the dog Cairo, and four SEALs were responsible for closing off the perimeter of the house while James and six other SEALs—the contingent that was supposed to have dropped onto the roof—moved inside. For the team patrolling the perimeter, the first fifteen minutes

passed without incident. Neighbors undoubtedly heard the low-flying helicopters, the sound of one crashing, and the sporadic explosions and gunfire that ensued, but nobody came outside. One local took note of the tumult in a Twitter post: "Helicopter hovering above Abbottabad at 1 AM (is a rare event)."

Eventually, a few curious Pakistanis approached to inquire about the commotion on the other side of the wall. "Go back to your houses," Ahmed said, in Pashto, as Cairo stood watch. "There is a security operation under way." The locals went home, none of them suspecting that they had talked to an American. When journalists descended on Bilal Town in the coming days, one resident told a reporter, "I saw soldiers emerging from the helicopters and advancing toward the house. Some of them instructed us in chaste Pashto to turn off the lights and stay inside."

Meanwhile, James, the squadron commander, had breached one wall, crossed a section of the yard covered with trellises, breached a second wall, and joined up with the SEALs from helo one, who were entering the ground floor of the house. What happened next is not precisely clear. "I can tell you that there was a time period of almost twenty to twenty-five minutes where we really didn't know just exactly what was going on," Panetta said later, on "PBS NewsHour."

Until this moment, the operation had been monitored by dozens of defense, intelligence, and Administration officials watching the drone's video feed. The SEALs were not wearing helmet cams, contrary to a widely cited report by CBS. None of them had any previous knowledge of the house's floor plan, and they were further jostled by the awareness that they were possibly minutes away from ending the costliest manhunt in American history; as a result, some of their recollections—on which this account is based—may be imprecise and, thus, subject to dispute.

As Abrar's children ran for cover, the SEALs began clearing the first floor of the main house, room by room. Though the Americans had thought that the house might be boobytrapped, the presence of kids at the compound suggested otherwise. "You can only be hypervigilant for so long," the special-operations officer said. "Did bin Laden go to sleep every night thinking, The next night they're coming? Of course not. Maybe for the first year or two. But not now." Nevertheless, Section

precautions were in place. A locked metal gate blocked the base of the staircase leading to the second floor, making the downstairs room feel like a cage.

After blasting through the gate with C-4 charges, three SEALs marched up the stairs. Midway up, they saw bin Laden's twenty-threeyear-old son, Khalid, craning his neck around the corner. He then appeared at the top of the staircase with an AK-47. Khalid, who wore a white T-shirt with an overstretched neckline and had short hair and a clipped beard, fired down at the Americans. (The counterterrorism official claims that Khalid was unarmed, though still a threat worth taking seriously. "You have an adult male, late at night, in the dark, coming down the stairs at you in an Al Qaeda houseyour assumption is that you're encountering a hostile.") At least two of the SEALs shot back and killed Khalid. According to the booklets that the SEALs carried, up to five adult males were living inside the compound. Three of them were now dead; the fourth, bin Laden's son Hamza, was not on the premises. The final person was bin Laden.

Before the mission commenced, the SEALs had created a checklist of code words that had a Native American theme. Each code word represented a different stage of the mission: leaving Jalalabad, entering Pakistan, approaching the compound, and so on. "Geronimo" was to signify that bin Laden had been found.

Three SEALs shuttled past Khalid's body and blew open another metal cage, which obstructed the staircase leading to the third floor. Bounding up the unlit stairs, they scanned the railed landing. On the top stair, the lead SEAL swivelled right; with his night-vision goggles, he discerned that a tall, rangy man with a fist-length beard was peeking out from behind a bedroom door, ten feet away. The SEAL instantly sensed that it was Crankshaft. (The counterterrorism official asserts that the SEAL first saw bin Laden on the landing, and fired but missed.)

The Americans hurried toward the bedroom door. The first SEAL pushed it open. Two of bin Laden's wives had placed themselves in front of him. Amal al-Fatah, bin Laden's fifth wife, was screaming in Arabic. She motioned as if she were going to charge; the SEAL lowered his sights and shot her once, in the calf. Fearing that one or both women were wearing suicide jackets, he stepped forward, wrapped them in a bear hug, and drove them aside. He would almost certainly have been killed had they blown themselves up, but by blanketing them he would have absorbed some of the blast and potentially saved the two SEALs behind him. In the end, neither woman was wearing an explosive vest.

A second SEAL stepped into the room and trained the infrared laser of his M4 on bin Laden's chest. The Al Qaeda chief, who was wearing a tan shalwar kameez and a praver cap on his head, froze; he was unarmed. "There was never any question of detaining or capturing him-it wasn't a split-second decision. No one wanted detainees," the special-operations officer told me. (The Administration maintains that had bin Laden immediately surrendered he could have been taken alive.) Nine years, seven months, and twenty days after September 11th, an American was a trigger pull from ending bin Laden's life. The first round, a 5.56-mm. bullet, struck bin Laden in the chest. As he fell backward, the SEAL fired a second round into his head, just above his left eve. On his radio, he reported, "For God and country-Geronimo, Geronimo, Geronimo." After a pause, he added, "Geronimo E.K.I.A."-"enemy killed in action."

Hearing this at the White House, Obama pursed his lips, and said solemnly, to no one in particular, "We got him."

Relaxing his hold on bin Laden's two wives, the first SEAL placed the women in flex cuffs and led them downstairs. Two of his colleagues, meanwhile, ran upstairs with a nylon body bag. They unfurled it, knelt down on either side of bin Laden, and placed the body inside the bag. Eighteen minutes had elapsed since the DEVGRU team landed. For the next twenty minutes, the mission shifted to an intelligencegathering operation.

Four men scoured the second floor, plastic bags in hand, collecting flash drives, CDs, DVDs, and computer hardware from the room, which had served, in part, as bin Laden's makeshift media studio. In the coming weeks, a C.I.A.-led task force examined the files and determined that bin Laden had remained far more involved in the operational activities of Al Qaeda than many American officials had thought. He had been developing plans to assassinate Obama and Petraeus, to pull off an extravagant September 11th anniversary attack, and to attack American trains.

SEALs also found an archive of digital pornography. "We find it on all these guys, whether they're in Somalia, Iraq, or Afghanistan," the special-operations officer said. Bin Laden's gold-threaded robes, worn during his video addresses, hung behind a curtain in the media room.

Outside, the Americans corralled the women and children-each of them bound in flex cuffs-and had them sit against an exterior wall that faced the second, undamaged Black Hawk. The lone fluent Arabic speaker on the assault team questioned them. Nearly all the children were under the age of ten. They seemed to have no idea about the tenant upstairs, other than that he was "an old guy." None of the women confirmed that the man was bin Laden, though one of them kept referring to him as "the sheikh." When the rescue Chinook eventually arrived, a medic stepped out and knelt over the corpse. He injected a needle into bin Laden's body and extracted two bone-marrow samples. More DNA was taken with swabs. One of the bonemarrow samples went into the Black Hawk. The other went into the Chinook, along with bin Laden's body.

Next, the SEALs needed to destroy the damaged Black Hawk. The pilot, armed with a hammer that he kept for such situations, smashed the instrument panel, the radio, and the other classified fixtures inside the cockpit. Then the demolition unit took over. They placed explosives near the avionics system, the communications gear, the engine, and the rotor head. "You're not going to hide the fact that it's a helicopter," the special-operations officer said. "But you want to make it unusable." The SEALs placed extra C-4 charges under the carriage, rolled thermite grenades inside the copter's body, and then backed up. Helo one burst into flames while the demolition team boarded the Chinook. The women and children, who were being left behind for the Pakistani authorities, looked puzzled, scared, and shocked as they watched the SEALs board the helicopters. Amal, bin Laden's wife, continued her harangue. Then, as a giant fire burned inside the compound walls, the Americans flew away.

In the Situation Room, Obama said, "I'm not going to be happy until those guys get out safe." After thirty-eight minutes inside the compound, the two SEAL teams had to make the long flight back to Afghanistan. The Black Hawk was low on gas, and needed to rendezvous with the Chinook at the refuelling point that was near the Afghan border—but still inside Pakistan. Filling the gas tank took twenty-five minutes. At one point, Biden, who had been fingering a rosary, turned to Mullen, the Joint Chiefs chairman. "We should all go to Mass tonight," he said.

The helicopters landed back in Jalalabad around 3 A.M.; McRaven and the C.I.A. station chief met the team on the tarmac. A pair of SEALs unloaded the body bag and unzipped it so that McRaven and the C.I.A. officer could see bin Laden's corpse with their own eyes. Photographs were taken of bin Laden's face and then of his outstretched body. Bin Laden was believed to be about six feet four, but no one had a tape measure to confirm the body's length. So one SEAL, who was six feet tall, lay beside the corpse: it measured roughly four inches longer than the American. Minutes later, McRaven appeared on the teleconference screen in the Situation Room and confirmed that bin Laden's body was in the bag. The corpse was sent to Bagram.

All along, the SEALs had planned to dump bin Laden's corpse into the sea-a blunt way of ending the bin Laden myth. They had successfully pulled off a similar scheme before. During a DEVGRU helicopter raid inside Somalia in September, 2009, SEALs had killed Saleh Ali Saleh Nabhan, one of East Africa's top Al Qaeda leaders; Nabhan's corpse was then flown to a ship in the Indian Ocean, given proper Muslim rites, and thrown overboard. Before taking that step for bin Laden, however, John Brennan made a call. Brennan, who had been a C.I.A. station chief in Rivadh, phoned a former counterpart in Saudi intelligence. Brennan told the man what had occurred in Abbottabad and informed him of the plan to deposit bin Laden's remains at sea. As Brennan knew, bin Laden's relatives were still a prominent family in the Kingdom, and Osama had once been a Saudi citizen. Did the Saudi government have any interest in taking the body? "Your plan sounds like a good one," the Saudi replied.

At dawn, bin Laden was loaded into the belly of a flip-wing V-22 Osprey, accompanied by a JSOC liaison officer and a security detail of military police. The Osprey flew south, destined for the deck of the U.S.S. Carl Vinson—a thousand-foot-long nuclear-powered aircraft carrier sailing in the Arabian Sea, off the

390

Pakistani coast. The Americans, yet again, were about to traverse Pakistani airspace without permission. Some officials worried that the Pakistanis, stung by the humiliation of the unilateral raid in Abbottabad, might restrict the Osprey's access. The airplane ultimately landed on the Vinson without incident.

Bin Laden's body was washed, wrapped in a white burial shroud, weighted, and then slipped inside a bag. The process was done "in strict conformance with Islamic precepts and practices," Brennan later told reporters. The JSOC liaison, the military-police contingent, and several sailors placed the shrouded body on an open-air elevator, and rode down with it to the lower level, which functions as a hangar for airplanes. From a height of between twenty and twenty-five feet above the waves, they heaved the corpse into the water.

Back in Abbottabad, residents of Bilal Town and dozens of journalists converged on bin Laden's compound, and the morning light clarified some of the confusion from the previous night. Black soot from the detonated Black Hawk charred the wall of the animal pen. Part of the tail hung over the wall. It was clear that a military raid had taken place there. "I'm glad no one was hurt in the crash, but, on the other hand, I'm sort of glad we left the helicopter there," the special-operations officer said. "It quiets the conspiracy mongers out there and instantly lends credibility. You believe everything else instantly, because there's a helicopter sitting there."

After the raid, Pakistan's political leadership engaged in frantic damage control. In the Washington Post, President Asif Ali Zardari wrote that bin Laden "was not anywhere we had anticipated he would be, but now he is gone," adding that "a decade of cooperation and partnership between the United States and Pakistan led up to the elimination of Osama bin Laden."

Pakistani military officials reacted more cynically. They arrested at least five Pakistanis for helping the C.I.A., including the physician who ran the immunization drive in Abbottabad. And several Pakistani media outlets, including the Nation—a jingoistic English-language newspaper that is considered a mouthpiece for Pakistan's Inter-Services Intelligence agency, or I.S.I.—published what they claimed was the name of the C.I.A.'s station chief in Islamabad. (Shireen Mazari, a former editor of the Nation, once told me, "Our interests and the Americans' interests don't coincide.") The published name was incorrect, and the C.I.A. officer opted to stay.

The proximity of bin Laden's house to the Pakistan Military Academy raised the possibility that the military, or the I.S.I., had helped protect bin Laden. How could Al Qaeda's chief live so close to the academy without at least some officers knowing about it? Suspicion grew after the Times reported that at least one cell phone recovered from bin Laden's house contained contacts for senior militants belonging to Harakat-ul-Mujahideen, a jihadi group that has had close ties to the I.S.I. Although American officials have stated that Pakistani officials must have helped bin Laden hide in Abbottabad, definitive evidence has not yet been presented.

Bin Laden's death provided the White House with the symbolic victory it needed to begin phasing troops out of Afghanistan. Seven weeks later, Obama announced a timetable for withdrawal. Even so, U.S. counterterrorism activities inside Pakistan—that is, covert operations conducted by the C.I.A. and JSOC—are not expected to diminish anytime soon. Since May 2nd, there have been more than twenty drone strikes in North and South Waziristan, including one that allegedly killed Ilyas Kashmiri, a top Al Qaeda leader, while he was sipping tea in an apple orchard.

The success of the bin Laden raid has sparked a conversation inside military and intelligence circles: Are there other terrorists worth the risk of another helicopter assault in a Pakistani city? "There are people out there that, if we could find them, we would go after them," Cartwright told me. He mentioned Ayman al-Zawahiri, the new leader of Al Qaeda, who is believed to be in Pakistan, and Anwar al-Awlaki, the American-born cleric in Yemen. Cartwright emphasized that "going after them" didn't necessarily mean another DEVGRU raid. The special-operations officer spoke more boldly. He believes that a precedent has been set for more unilateral raids in the future. "Folks now realize we can weather it," he said. The senior adviser to the President said that "penetrating other countries' sovereign airspace covertly is something that's always available for the right mission and the right gain." Brennan told me, "The confidence we have in the capabilities of the U.S. military is, without a doubt, even stronger after this operation."

On May 6th, Al Qaeda confirmed bin Laden's death and released a statement congratulating "the Islamic nation" on "the martyrdom of its good son Osama." The authors promised Americans that "their joy will turn to sorrow and their tears will mix with blood." That day, President Obama travelled to Fort Campbell, Kentucky, where the 160th is based, to meet the DEVGRU unit and the pilots who pulled off the raid. The SEALs, who had returned home from Afghanistan earlier in the week, flew in from Virginia. Biden, Tom Donilon, and a dozen other national-security advisers came along.

McRaven greeted Obama on the tarmac. (They had met at the White House a few days earlier-the President had presented McRaven with a tape measure.) McRaven led the President and his team into a one-story building on the other side of the base. They walked into a windowless room with shabby carpets, fluorescent lights, and three rows of metal folding chairs. McRaven, Brian, the pilots from the 160th, and James took turns briefing the President. They had set up a threedimensional model of bin Laden's compound on the floor and, waving a red laser pointer, traced their maneuvers inside. A satellite image of the compound was displayed on a wall, along with a map showing the flight routes into and out of Pakistan. The briefing lasted about thirty-five minutes. Obama wanted to know how Ahmed had kept locals at bay; he also inquired about the fallen Black Hawk and whether above-average temperatures in Abbottabad had contributed to the crash. (The Pentagon is conducting a formal investigation of the accident.)

When James, the squadron commander, spoke, he started by citing all the forward operating bases in eastern Afghanistan that had been named for SEALs killed in combat. "Everything we have done for the last ten years prepared us for this," he told Obama. The President was "in awe of these guys," Ben Rhodes, the deputy national-security adviser, who travelled with Obama, said. "It was an extraordinary base visit," he added. "They knew he had staked his Presidency on this. He knew they staked their lives on it."

As James talked about the raid, he mentioned Cairo's role. "There was a dog?" Obama interrupted. James nodded and said that Cairo was in an adjoining room, muzzled, at the request of the Secret Service.

"I want to meet that dog," Obama said.

"If you want to meet the dog, Mr. President, I advise you to bring treats," James joked. Obama went over to pet Cairo, but the dog's muzzle was left on.

Afterward, Obama and his advisers went into a second room, down the hall, where others involved in the raid-including logisticians, crew chiefs, and SEAL alternates-had assembled. Obama presented the team with a Presidential Unit Citation and said, "Our intelligence professionals did some amazing work. I had fifty-fifty confidence that bin Laden was there, but I had one-hundred-per-cent confidence in you guys. You are, literally, the finest small-fighting force that has ever existed in the world." The raiding team then presented the President with an American flag that had been on board the rescue Chinook. Measuring three feet by five, the flag had been stretched, ironed, and framed. The SEALs and the pilots had signed it on the back; an inscription on the front read, "From the Joint Task Force Operation Neptune's Spear, 01 May 2011: 'For God and country. Geronimo.' " Obama promised to put the gift "somewhere private and meaningful to me." Before the President returned to Washington, he posed for photographs with each team member and spoke with many of them, but he left one thing unsaid. He never asked who fired the kill shot, and the SEALs never volunteered to tell him.

# A Portrait of Abu Bakr bin Abdul Aziz al-Athri: Salafi-Jihad's Emerging Internet Ideologue

By Murad Batal al-Shishani

Source: http://www.jamestown.org

In mid-June 2010, the brother-in-law of Abu Mus'ab al-Zarqawi, the late leader of al-Qaeda in Iraq (AQI), Abu Qudama al-Hami, [1] posted a lengthy article on several jihadi web forums stating that a London-based Jordanian jihadi called Muhammad Eid al-Rifai'i (a.k.a. Abu Hammam; Abu Essa) is using the pseudonym "Abu Hammam Bakar al-Athri" to defend senior.

Salafi-jihadi ideologue Abu Muhammad al-Maqdisi. [2] Since 2008, al-Hami has launched a campaign accusing al-Maqdisi of deviating from the path of Salafi-jihadi ideology's core message. [3]

In the same article, al-Hami claimed that al-Rifai'i is the founder of the famous jihadi web forum Shmoukh al-Islam. He reminded readers of al-Rifai'i's jihadi history and described him as takfiri (empowered to excommunicate fellow Muslims) since the days when al-Rifai'i declared himself as a Caliph in Peshawar, Pakistan in the early 1990s. It is likely that al-Hami made these accusations due to his increasing enmity towards al-Magdisi and his school of jihadi thought. Additionally, it seems that al-Hami confused as al-Rifai'i's kunya (an Arabic honorific taken on from one's child) with Abu Hammam. An informed source told Jamestown that al-Athri and al-Rifai'i are indeed different men and that al-Hami targeted his rage at the wrong man.

Muhammad Eid al-Rifai'i is a Jordanian from Zarga in his early fifties. He was member of Ikhwan al-Muslimeen (the Muslim Brotherhood) until he was expelled in the late 1980s, perhaps because of his espousal of a strain of jihadi ideology out of sync with the Ikhwan. During the Second Gulf War in 1991, he was very active in mobilizing Jordanian youth to fight alongside the Iragis. When that effort failed to materialize, Rifai'i left for the greener jihadi pastures of Peshawar, Pakistan. He eventually relocated to London where he was imprisoned in Belmarsh. He was later released on health grounds. The case that resulted in his detention was unrelated to his jihadi activities but regarded a mundane immigration issue. [4]

Although his real identity remains obscured, the background of Abu Bakr bin Abdul Aziz al-Athri is not to be confused with veteran jihadi al-Rifai'i. Al-Athri's stature as a jihadi scholar is gaining momentum as his writings continue to spread across global jihadi websites. Al-Athri was recently announced as a member of the sharia committee of al-Maqdisi's Minbar al-Tawhid w'al-Jihad website. It is in this light that al-Athri appears to be a leading successor of Abu Muhammed al-Maqdisi in terms of propagating fervent jihadi ideology.

What little is known about al-Athri's background stems from an autobiographical work. [5] It suggests that he is younger than al-Rifai'i. He has a Bachelor degree in Islamic law from a university in the Levant-though he does not specify which one. He then relocated to Saudi Arabia –although he does not state that explicitly- as he became student for several Saudi sheikhs including Ibn Jbreen and the Sahwa scholar Salman al-Ouda—a moderate by comparison. Al-Athri then distanced himself from al-Ouda because he felt al-Ouda's message had grown too soft. He also became a student of many Salafi-jihadi scholars including al-Maqdisi, which suggests that al-Athri still spent a significant amount of time in Jordan.

Al-Athri describes al-Maqdisi thusly: "By Allah our sheikh al-Maqdisi is like a father [for me] among all sheikhs [who taught me] – either I mentioned them in this biography or not-the Sheikh was, after Allah, the main reason behind my steadfastness on this blessed [jihadi] way." [6] But al-Maqdisi's opinion on al-Athri suggests that the latter would be the successor of the former who wrote in an introduction of one of al-Athri's books: "if [a] Sheikh is entitled to show pride of some of his students, I am proud of this beloved brother." [7]

Perusing the books, articles, and fatwas disseminated by al-Athri, [8] one can observe that the appeal of his religious authority is widening. Most read or downloaded writings or fatwas about him as shown on the Minbar al-Tawhid w'al-jihad website indicate that his religious views on particular events and day-today minutiae appeal to more people rather than grand theorizing. He is not a jihadi strategist but a jihadi scholar in the same vein as al-Magdisi who exerts grand influence on jihadis worldwide. Al-Athri currently receives fatwarelated queries from all over the world, which he readily addresses via the pro-al-Qaeda Minbar al-Tawhid w'al-Jihad forum while al-Magdisi is imprisoned in Jordan.

Al-Athri being a central member of the sharia committee of al-Maqdisi's website and being a potential successor to al-Maqdisi arguably demonstrates that the religious expression of the Salafi-jihadi movement is becoming more institutionalized. Al-Athri, in the context of this gradual process, appears to be playing a major role in the transformation. The religious legitimization of Abu Bakr bin Abdul Aziz al-Althri will increase the recruitment capacity of the Salafi-jihadi movement to expand its ranks. The current online propaganda arm, of which al-Athri is now a primary actor, has provention

be quite effective. This combination of al-Athri's popularity and newfound legitimacy will help further promulgate the religious edicts that he and his fellow travelers are producing to influence a new generation of jihadis.

### Notes:

1. Abu Qudama al-Hami's real name is Sati Qasrawi. He is a Jordanian national who worked as Jihad Magazine's (a bi-monthly magazine founded by Abdullah Azzam in 1984) correspondent during the anti-Soviet jihad in Afghanistan where lost his leg to a landmine. He is married to al-Zarqawi's sister and currently lives in Jordan. 2. http://muslmnet.net/vb/showthread.php?t=391727, June 12, 2010.

3. Murad Batal al-Shishani, The Dangerous Ideas of the Neo-Zarqawist Movement, Sentinel, Competing Terrorism Center (West Point), September 2009, Vol 2, Issue 9, pp. 18-20.

4. http://www.alasr.ws/index.cfm?method=home.con&contentID=7463, February 16, 2006.

5. http://www.tawhed.ws/FAQ/display\_question?qid=3875, April 2011.

6. Ibid.

7. Ibid.

8. See his writings: http://www.tawhed.ws/a?a=bakraziz.

Murad Batal al-Shishani is an Islamic groups and terrorism issues analyst based in London. He is a specialist on Islamic Movements in Chechnya and in the Middle East.

# Al-Qaeda Uses Pakistani Intelligence Course to Train International Operatives By Abdul Hameed Bakier

Source: http://www.jamestown.org

Possibly recognizing that intelligence breakdowns played a major role in the elimination of Osama bin Laden and other al-Qaeda leaders, the al-Qaeda's Global Islamic Media Front (GIMF) recently released a training tool entitled "The Security and Intelligence Course." Many jihadi internet forums posted the course's download links, widespread distribution ensuring (see ansar1.info, June 15).

According to its translator and editor, jihadi activist Obaida Abdullah al-Adam, the security and intelligence training material originally consisted of Urdu language documents obtained from Pakistan's Inter-Services Intelligence (ISI), known for its close ties to various jihadi movements. Al-Adam has previously contributed other jihadi training material in various jihadi internet forums. These works include Sinaat al-Irahab ("The Making of Terrorism") and Tariq al-Tamkeen ("The Road of Enabling") (as-ansar.com, March 3; muslm.net, June 22, 2010). The training course is broken down into four main parts.

#### **Basic intelligence training**

The course starts with basic security and intelligence definitions used by the internal and external security apparatus of a given state and the different responsibilities of various state security services. To emphasize the importance of external intelligence, al-Adam claims the ISI was able to deter a joint Israeli-Indian air assault on its nuclear installations after receiving intelligence from a Pakistani agent who had succeeded in penetrating the enemy's security structure. No further details are given by al-Adam on the alleged air attack plan but the claim could be an attempt to prove the training course was taken from Pakistani intelligence.

The next training block concentrates on mujahideen group operations and the criteria used to select group members. The mujahideen group members should be Muslims, enjoy a certain degree of education and be religiously motivated and "nonmundane," the latter meaning the jihadi's pure purpose must be the elevation of the Islamic nation. Al-Adam warns that intelligence services' attempts to penetrate mujahideen cells are serious as they use the same assets they use to penetrate other state intelligence agencies. Therefore, a jihadi on a mission should be fully briefed beforehand on the area of operation. The briefing must include pictures taken of the area during earlier jihadi reconnaissance operations. The photos should indicate the security measures employed

around sensitive buildings and any other security details implemented by the enemy.

Al-Adam says the most likely cover story for a state intelligence agent is posing as a journalist. Other cover stories vary from posing as taxi drivers to shop owners. Al-Adam gives the example of the late Daniel Pearl, claiming Pearl was a U.S. intelligence agent posing as a journalist (Pearl was the South Asia bureau chief of The Wall Street Journal when he was kidnapped and killed by the mujahedeen in 2002). The personal characteristics of a cell member and the security procedures of each cell are also discussed at length in the training course. Other training includes the secure exchange of classified documents between the mujahideen. Mujahideen are cautioned not to carry their original passports when going on a mission: instead, passports with false personal information must be used by travelling mujahideen.

On communications, the course suggests the internet and mobile phones are preferred for fast and frequent connections between the mujahideen. Earlier jihadi forums have posted technical material containing more detailed mobile training on secure phone communications (see Terrorism Monitor, September 8, 2006). Any exchange of highly classified information between mujahideen leaders should be done through handwritten letters conveyed by carriers trained in concealment methods. Some concealment methods are discussed in the course, as well as the personal security steps the travelling mujahideen should implement. Methods suggested to conceal a letter include hiding it inside a pen, a toothpaste tube, a book, or a child's milk bottle.

The course recommends going to a predesignated area where the letter will be handed to the recipient after anti-surveillance procedures have been applied. The letter should be passed on through a handshake, inside a newspaper or in what is known as "brush contact" in intelligence parlance.

The course offers other basic and essential training for intelligence gathering operations such as conducting successful clandestine meetings in safe houses, different types of surveillance, communicating through dead drops and face-to-face intelligence gathering

techniques using proper elicitation, questioning and interrogation methods.

### Propaganda

Although the counter-propaganda measures suggested in the course are basic, the course seeks to raise mujahideen awareness to the existence of such operations by counterterrorism forces to reduce the effectiveness of such efforts by security forces against the mujahideen. Suggested countermeasures to propaganda include:

- Keeping the group busy with operations and training.
- Immediately informing the mujahideen of any propaganda and refuting it.
- Punishing anyone spreading the propaganda among the mujahideen.
- ☑ Increasing the mujahideen's religious awareness.
- Ensuring full obedience to the group's Amir (leader).

The effectiveness of anti-extremism campaigns such as Saudi Arabia's assakina ("tranquility from God"), launched in 2003 to refute the Salafi-Jihadi ideology and deter possible al-Qaeda recruits, would be much reduced if the mujahideen can be made to believe that any religious argument against extremism made by moderate Islamic entities or individuals is a lie (see assakina.com, July 17, 2010).

### **Deep cover operations**

Almost all training blocks in the course can be classed as conventional intelligence and security training except for the section on deep cover operations. Such operations are considered advanced intelligence and are practiced mostly by sophisticated intelligence agencies against priority targets in high risk areas. The training course implies that deep cover operations require more time and effort than conventional intelligence operations. Deep cover training enhances the ability of the mujahideen to plant sleeper cells in target countries that possess advanced intelligence and security forces. The fact that the mujahideen training course was translated from Urdu to English for the benefit of mulahideen in America and Europe, as al-Adam says at the prelude, is an indication of where the mujahideen are planning their future terror attacks.

Abdul Hameed Bakier is an intelligence expert on counter-terrorism, crisis management and terroristhostage negotiations. He is based in Jordan.

# Sovereign Citizens: A Homegrown Threat?

### By Noëlle MacKenzie

Source: http://www.wibw.com/internationalnews/headlines/125609063.html

The "sovereign citizen" extremist movement is one that many people haven't heard of, although the FBI considers its members one of the top threats to our nation. The FBI characterizes the movement as domestic terrorism: "Sovereign citizens are antigovernment extremists who believe that even though they physically reside in this country,



they are separate or 'sovereign' from the United States. As a result, they believe they don't have to answer to any government authority, including courts, taxing entities, motor vehicle departments, or law

enforcement. This causes all kinds of problems—and crimes. For example, many sovereign citizens don't pay their taxes. They hold illegal courts that issue warrants for judges and police officers. They clog up the court system with frivolous lawsuits and liens against public officials to harass them. And they use fake money orders, personal checks, and the like at government agencies, banks, and businesses."

CBS's 60 Minutes program featured the sovereign citizen movement in May and said that "there are as many as 300,000 sovereign citizens in the U.S. And with the sluggish economy

and mortgage mess, their ranks are growing." The program showed examples of many sovereign citizen sites that feature ways to beat the system, and said, "But when those efforts to beat the system fail, a sovereign citizen will often seek retribution. The weapon of choice is paper. For example, when a sovereign has a run-in with the law, they might file a lien or financial claim against the personal assets of the police officer or the judge involved. It's easy to file and you don't even need a lawyer. The sovereign never collects, but the target of the lien can have their credit ruined. The practice has been called 'paper terrorism.'"

The program also illustrated "the marked increase in violence associated with sovereign citizens, much of it directed at police and judges," reporting that "a South Carolina sovereign citizen awaits execution for killing two lawmen in a standoff; in Texas, a sovereign faces attempted capital murder charges in the shooting of three men, two of them sheriff's deputies. And an Alaska sovereign citizen and five others are charged with plotting to kill two judges, state troopers and an IRS agent."

The FBI says that "not every action taken in the name of the sovereign citizen ideology is a crime, but the list of illegal actions committed by these groups, cells, and individuals is



extensive," citing murder; physical assault; impersonating police officers and diplomats; using fake currency, passports, license plates, and driver's licenses; and white-collar scams, such as mortgage fraud and "redemption" schemes.



# **Piracy Spreads to the South**

By Ben Coetzee

Source: http://www.iss.co.za/iss\_today.php?ID=1326



# Institute for Security Studies Institut d'Etudes de Sécurité

Knowledge empowers Africa • Le savoir emancipe l'Afrique

In recent times piracy has leapt to the forefront as a threat to the world economy; impacting the prices of commodities and raising concerns about the long term impact on energy prices. Southern Africa did not experience the initial brunt of the effects of piracy when the international community identified it as a threat to world wide economic growth. This respite can be attributed to the physical distance between Somalia and Southern African waters and the continued operation of the Suez Channel.

Shipping companies preferred to use the Suez Channel trading between the west (the Americas and Europa) and the east (the Middle East and Asia) because it eliminated the need to sail around the "Cape of Storms". However



shipping companies are increasingly choosing

to follow a longer route around the southern tip of Africa in an effort to avoid running the gauntlet through the Gulf of Aden and becoming

victims of piracy. This diversion from normal practices is in effect slowly starting to starve the pirates from rich targets.



The lack of prey and the constant attention of the international fleet participating in Operation Atlanta are forcing pirates to move their operations south, towards areas outside the operational arena of the international fleet. Acts of piracy are also increasingly occurring further away from the mainland in international waters. This migration of pirate activity from Somalia is exerting pressure on coastal countries such as Tanzania to step up their efforts to protect vessels traversing their territorial waters.

Tanzanian President Jakaya Kikwete commented during his recent visit to South Africa that Tanzania has experienced almost 30 pirate attacks and that the increasing number of incidents is starting to affect the economy of Tanzania and by extension the whole of Eastern Africa. The impact is the result of ships preferring not to visit the ports in Tanzania due to the risk of becoming the victims of pirate attacks.

South Africa, in an effort to curb piracy before it reaches its doorstep, has committed its maritime resources to the fight against pirates. The main motivation for this approach seems to be to fight pirates in the waters of its neighbours whilst ensuring that the South African shipping lanes remain safe and open for business. Although the South African National Defence Force remains stoically silent.

about their strategic plan to get involved in the fight against piracy, the actions of the Government support the conceptual properties of a plan of this nature.

The agreements signed between South Africa and other Eastern African countries concerned about the impact of piracy on their economies contributes to this understanding. These countries are Mozambique, Tanzania, Kenya, the Seychelles, the Comoros, Madagascar and Reunion. Agreements of this nature increase the area of responsibility for the South African Navy but it also provides refuelling points and safe harbours in the South Indian Ocean. Allowing the South African fleet to deploy fighting vessels such as frigates and aircraft without the additional expense of support vessels to ensure continued operational capability.

The general notion is that piracy is recognised as a serious threat to Southern Africa and South Africa in particular. The South African Government is seemingly willing to commit scarce resources in an effort to prevent the further incursion of pirates into the territorial waters of SADC. This strong reaction from South Africa and its neighbours should serve as a warning to prospective pirates and robbers that these acts would not be considered lightly.

A matter of concern however, is the legal component of the fight against piracy. This concern has not attracted much attention but is vital to SADC's efforts against piracy in the future. For example if suspected pirates are apprehended, what would the legal process entail? Do African coastal countries have the legislation and capacity to prosecute the suspected pirates and where will such prosecution take place? And above all, the question remains as to who will pay for the prosecution and the incarceration of the suspected pirates upon conviction?

### Ben Coetzee is Senior Researcher, Arms Management Programme, ISS Pretoria Office

# Mumbai Outraged Once Again: India Blinks, Blames Homegrown Terror

By Animesh Roul

Source: http://www.jamestownfoundation.com

### **Executive Summary**

In the weeks following the July 13 bomb explosions in Mumbai, responsibility for the attacks has yet to be determined. Investigative agencies have not yet pinpointed a suspect nor has any terrorist group claimed the blasts as its own doing, perhaps in order to complicate the investigation or delay the process. The triple blasts, which killed 24 people and injured over one hundred, mark the first major



terrorist attack in Mumbai since the November 2008 bombings orchestrated by Pakistan's Lashkar-e-Taiba (LeT). Current indications point the finger toward the Indian Mujahedeen (IM), a terrorist group with connections to LeT, due to the use of IEDs made of ammonium nitrate and fuel oil (ANFO) as well as the remote-controlled detonation of the bombs, which were common characteristics of IM terrorist acts

across India between 2007 and 2008. While responsibility for the blasts remains unclaimed, it is the Indian intelligence agency that is bearing the brunt of guilt and scrutiny, as it is clear that stepped-up security measures that were put in place following the November 2008 attack did little to avoid another deadly situation. And while the Indian government has, in the past, been quick to blame Pakistan for harboring terrorist groups, such rhetoric has been missing in the weeks since July 13. This could be a sign of the neighboring countries' new approach to combating terrorist organizations in the region.

### Introduction

Weeks after the July 13 triple bomb blasts that stunned India's commercial capital, Mumbai, once again, investigating agencies have yet to pinpoint the terrorist group or organization behind these deadly blasts. Three bombs went off within minutes killing 24 people with over one hundred injured at Dada's Kabutarkhana, the Opera House and Zaveri Bazaar (Daily News and Analysis (Mumbai) July 25); Forensic investigation confirms the use of IEDs made of ammonium nitrate and fuel oil (ANFO) and ball bearings (Economic Times/Indo Asian News Service, July 18). And it is evidently clear that the blasts were triggered by timer devices and not by remote-controlled devices.

India's intelligence apparatus came under severe scrutiny this time as terror modules have managed to strike again in the heart of Mumbai despite stepped up security measures that were put in place following the November 2008 Mumbai siege. Pakistani based Lashkare-Taiba and Pakistan's intelligence agency, ISI, were blamed for masterminding the 2008 Mumbai attacks.

Surprisingly, no terrorist organizations have claimed responsibility so far, perhaps for the of complicating investigation purpose procedures and or to delay follow up actions by the agencies. For the first time, the Indian government and intelligence agencies have refrained from naming either any Pakistan based terror group or any homegrown groups so far. However, the direction of the ongoing investigation is moving toward Indian Mujahideen (IM), which is largely nurtured by the Pakistan based Lashkar-e-Taiba (LeT) and received explosives training from the Bangladesh based Harkat ul Jihadi Islami-Bangladesh (HuJI-B).

The Indian Mujahedeen, largely comprised of outlawed Student Islamic Movement of India (SIMI) cadres, had claimed responsibility for a number of similar terror acts across India between 2007 and 2008 in which they used mostly ANFO based IEDs and timer devices to trigger blasts in many Indian cities, a technique they learned from the HuJI-Bangladesh (Terrorism Monitor, January 21, 2010). Since the Pune Germany Bakery blast of February 2010, IM has claimed at least two terror attacks in Delhi and Varanasi. In September of last vear, bike-borne gunmen attacked a tourist bus, injuring two Taiwanese men outside Delhi's historic Jama Masjid. Again in December of that year a bomb exploded on the banks of the Holy Ganges River in Varanasi. Now the National Investigating Agency (NIA) along with Mumbai police has been connecting the dots to determine whether or not those low intensity explosions have links to the July 13 Mumbai blasts.

Arguably, ANFO can be used by any fringe group with a subversive motive, as ammonium nitrate is readily available in India and mostly used for mining purposes. For this very reason, the involvement of right wing extremist groups such as Avinav Bharat and Sanatan Sanstha is also being investigated. Past experience, however, shows that these groups have limited and low intensity capability and have only perpetrated retaliatory attacks against Islamic religious places and symbols. Their involvement, therefore, could certainly be ruled out.

### IM-LeT Handiwork?

The recent bombings have all the markings of Indian Mujahideen, as the explosives used and the tactic of synchronized bomb attacks in crowded places put the needle of suspicion squarely on the IM, whose top leadership is presently holed up in neighboring Pakistan. Two new offshoots of IM have been under intelligence radar for quite some time: 'Bullet 313 Brigade' and the Jama't Ansar-ul Muslimeen (Sakal Times (Pune) July 16; Rediff.com, July 18). These shadow organizations act as covers for IM, and more importantly, scout new talents and coordinate fund collections in Uttar Pradesh, Andhra Pradesh, Kerala and in Karnataka. If intelligence agencies are to be believed, these units are under the direct control of fugitive IM operatives in Pakistan who fled India after the countrywide crackdown on IM hideouts in 2008. Many IM operatives were arrested during that time from Gujarat, Kerala, Maharashtra, Madhya Pradesh, Delhi and Uttar Pradesh. As many as 15 top level operatives are still at large including Igbal Shahbandari, Riyaz Shahbandari, Abdus Subhan Quresi and Mohsin Chaudhary.

The arrest of Danish Rivaz, IM's treasurer and recruiter, on June 21 in connection with the 2008 Ahmadabad blasts sheds light on the Lashkar-e-Taiba, Taliban and IM's evil designs against India. The email communications of Rivaz with other arrested and absconding terrorists, including a man named Haroon, Mohammed Safikul and Abu Faisal, have revealed conspiracies hatched against India across international borders. Haroon, a suspect in the July 13 Mumbai blasts, is believed to have been in touch with Taliban leaders in Pakistan. The Gujarat crime branch police is presently investigating whether or not Haroon sent 10 new recruits, as planned, to the special Taliban training program (India Today, July 18). Another revelation came from Mohamme

Safikul, a LeT operative arrested in Malda (West Bengal) in January 2009, who told interrogators about LeT's new recruitment drives in the Eastern Indian states of West Bengal, Bihar, Assam and Tripura (Hindustan Times, July 18).

### A Possible HuJI Link

Just before the July 13 blasts, Bihar state police had detained two Harkat ul Jihadi Islami (HuJI) suspects identified as Rivazul Sarkar and Mahtab Alam, along with multiple SIM cards, cell phones and documents written in the Marathi language (spoken in Mumbai [Maharashtra]). The two men are under investigation for their possible links with the Mumbai serial blasts (Times of India, July 18). Another HuJI operative Jalaluddin Mullah (a.k.a Babu Bhai) who has emerged as key linkman between HuJI and IM earlier and now in custody, is too under interrogation. It is believed that he might have some vital clues that can solve the Mumbai mystery (Hindustan Times, July 20). According to available information, Jalaluddin was in touch with one Khurram Khayyam, a key recruiter for HuJI-B and a key linkman between various terror groups operating out of Bangladesh, for example, Lashkar-e-Taiba and Jama'atul Mujahideen Bangladesh.

Based on the investigations so far, especially following revelations from Haroon and Riaz, the Mumbai Anti-Terrorism Squad (ATS) and NIA have been working on specific leads and are now engaged in a massive search operation inside the Dangs forests on the Gujarat-Maharashtra border for six absconding IM operatives from West Bengal and Gujarat.

Reported sightings of IM's Riyaz Shahbandari, who fled to Pakistan long ago, on the outskirts of Mumbai days before the blast as well as the Nepal police arrest of a suspect named Mohammad Zaheer for alleged involvement in the July 13 Mumbai blasts added fresh leads in the ongoing investigations, but so far no definite link has been established (Mumbai Mirror, July 23).

Meanwhile, the ATS and NIA have unleashed a countrywide search and sweep operation to nab the culprit behind these deadly terrorist attacks.

### India-Pakistan Ties Amid Terror

The latest Mumbai blasts took place on the even of the scheduled July 27 talks between

the foreign ministers of the two countries in Delhi. Surprisingly, the usual blame game between India and Pakistan has been missing and war rhetoric has taken a backseat for now. India has in the past accused Pakistan of harboring violent terrorist groups and unleashing a proxy war. Following the November 2008 Mumbai siege, direct accusations emanated from India and there were talks of a surgical strike targeting terror infrastructures inside Pakistan. [1] This time, however, both political and media fraternities from each side have abstained from confrontation.

Despite this posturing, the Indian Home Minster made it clear during the fourth meeting of SAARC Home/Interior Ministers in Thimpu (Bhutan) recently that terrorist groups have flourished because of the support they have found from both state and non-state actors, and no country can escape its responsibility by blaming non-state actors for terrorist activities emanating from its soil, with an obvious reference to Pakistan (The Hindu, July 23). Raising the issue of "safe heavens" and "terror camps", he cautioned that Pakistan owes a "legal and moral responsibility to its neighbors" and to the world to suppress those non-state actors and bring them to justice.

By not blaming Pakistan for the latest terror strikes, it is amply clear that India is attempting to place psychological pressure on Pakistan to work toward dismantling terrorist infrastructures, to cooperate in solving the pending 2008 Mumbai case and, last but not least, to take serious action against those on the revised fugitive lists.

The inevitable question is now, if a LeT-IM nexus is be found to be behind the latest Mumbai blasts, then what would be India's response? Whether India should at all engage with Pakistan diplomatically in the future or go on a hot pursuit targeting Lashkar-e-Taiba and other anti-Indian terror organizations inside Pakistan is still unknown. Plausibly, India's response would remain calculated to keep the diplomatic channel open and to avoid any military confrontation at the Western borders. Looking at the latest terror investigations it

Looking at the latest terror investigations it seems that homegrown terror is thriving despite the government's repeated denial that Indian Muslims are radicalized enough to perpetrate terror on their own. The Indian Home Minster himself admitted that these "indigenous terror groups" are no locate

fledgling outfits (Times of India, July 27). However, the complicity of Lashkar-e-Taiba and Harkat ul Jihadi Islami in nurturing and

Note:

1. Read the Interview of External Affairs Minister Pranab Mukherjee, "India has right to protect its territorial integrity: Pranab," NDTV.com, December 02, 2008.

Animesh Roul is the Executive Director of Research at the New Delhi-based Society for the Study of Peace and Conflict (SSPC).

## **Report warns Amtrak vulnerable**

Source:http://www.nbclosangeles.com/news/local/Amtrak-Remains-Vulnerable-to-Terrorism-126533783 .html

A new report by the DHS Inspector General warns that Amtrak is vulnerable to terrorist



attacks, despite the \$1 billion that has already been spent to bolster security; the inspector

directing these so called homegrown terror organizations should not be overlooked.

A new report by the DHS Inspector General warns that Amtrak is vulnerable to terrorist attacks, despite the \$1 billion that has already been spent to bolster security.

Beginning in 2005 the DHS Transit Security Grant Program awarded more than \$1 billion in grant funding to help secure passenger rail lines and to protect critical transportation infrastructure. Yet the inspector general found that DHS officials did not ensure that the money was being spent efficiently securing Amtrak's most vulnerable stations. "As a result, some rail stations and the traveling public may be at a greater risk to a potential terrorist attack," the report said.

"We visited four high-risk rail stations and



general found that DHS officials did not ensure that the money was being spent efficiently securing Amtrak's most vulnerable stations resulting in security gaps observed that Amtrak did not take actions to mitigate some of the more critical vulnerabilities...identified as early as 2006," the report said. "For example, at one station, we

observed that a terrorist could access..." The rest of the sentence had been redacted.

According to Pat Jordan, the Los Angeles Sheriff's Commander who helps oversees an Amtrak and several commuter rail lines, the biggest threats to passengers are bombers or gunmen.

"The most likely one is a small improvised explosive device, or an active shooter type situation. If you look across the country, those are the challenges we face," he said.

To help protect against these threats Jordan urges passengers to report any suspicious activities they see.

"If you look at a lot of the attempts to attack the transit systems and other attacks around the country, they've been really interdicted by people who saw something and said something".

Late last month an Amtrak train was evacuated in western Kansas (photo left), after a passenger found and reported a suspicious device on board. Local law enforcement officers were called in to investigate the package, but found no threat.

The inspector general's report warns that terrorists will likely continue to target trains as they are attractive targets.

"Since 2004, bombings of the Madrid and Mumbai rail systems and the London subway have demonstrated the critical need to protect rail infrastructure from terrorist attacks," the report said. "Passenger rail stations are especially attractive to terrorist targets because of the large number of people in a concentrated area."

The report went on to say, "The largest of



America's rail stations are inter-model transportation terminals with high passenger and cargo volumes. A terrorist attack at these facilities could lead to significant loss of life and economic disruption." Each year more than twenty-seven million passengers ride Amtrak at more than 500 stations across the country.

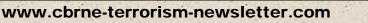
# Newly formed South Sudan joins Somalia, Pakistan, Iraq and Afghanistan at top of Maplecroft terrorism ranking – attacks up 15% globally

Top four countries sustain over 75% of world's fatalities from terrorism Source: http://maplecroft.com/about/news/terrorism\_index\_2011.html

New research has rated the fledgling state of South Sudan in the top five countries most at risk from terrorist attacks after Somalia, Pakistan, Iraq and Afghanistan, whilst data also reveals that terrorist



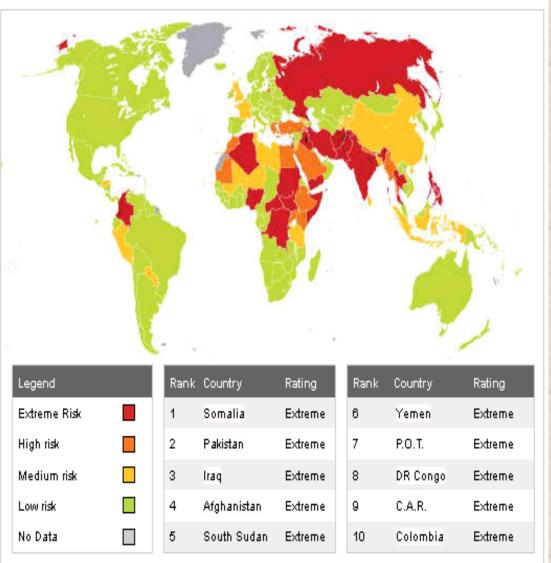
attacks are on the increase globally.



The latest Terrorism Risk Index (TRI), released by risk analysis and mapping firm Maplecroft, rates 20 countries and territories as 'extreme risk,' with Somalia (1), Pakistan (2), Iraq (3), Afghanistan (4) once again topping the ranking. The 'extreme risk' category also includes: South Sudan (5), Yemen (6), Palestinian Occupied Territories (7), DR Congo (8) Central African Republic (9), Colombia (10), Algeria (11), Thailand (12), Philippines (13), Russia (14), Sudan (15), Iran (16), Burundi (17), India (18), Nigeria (19) and Israel (20).

The TRI has been developed by Maplecroft to enable business to identify and monitor the available to calculate the frequency and lethality of terrorist incidents over the 12 month period prior to April 1st 2011. The TRI also includes a historical component assessing the number of attacks over five years and assesses risks relating to countries' geographic proximity to terrorist hotspots.

Following the country's formal secession from Sudan in July 2011, South Sudan (5) makes its first appearance in the Terrorism Risk Index. The country is rated as 'extreme risk' primarily due to the intensity of terrorist attacks, with an average of 6.59 fatalities per terrorist incident, almost three times that of Somalia at 2.23.



Terrorism Risk Index

Maplecroft, 2011

risks posed by terrorism to employees and assets in 197 countries. The index draws on the latest and most comprehensive data A number of terrorist groups operate in South Sudan including the Lord's Resistance Army, which has been responsible for mass-casualty

attacks. However, splinter groups that have broken away from the mainstream Sudan People's Liberation Army (SPLA) use terrorist methods and pose the greatest threat. One such group, led by George Athor, was responsible for 111 deaths in an attack in Jonglei province in February 2011. This one incident accounts for over 50% of the 211 fatalities sustained by South Sudan from attacks between April 2010 and March 2011.

Despite ranking 5th in the index, South Sudan's death toll of 211 from terrorist attacks pales in comparison to the top four countries. Over the same period Somalia suffered 1,385 deaths, Pakistan 2,163 deaths, Iraq 3,456 deaths and Afghanistan 3,423 deaths, which together account for over 75% of the world's 13,492 fatalities.

Looking at the year on year data, Maplecroft's research also reveals that the number of terrorist attacks rose by approximately 15% globally, with 11,954 incidents between April 2010 and March 2011, compared to 10394 from April 2009 to March 31st 2010. However, there was a decrease in fatalities falling to 13,492 from 14,478.

Significantly the TRI also reveals that the number of terrorist incidents in Afghanistan increased by over 50% over the same period, rising from 2246 attacks in 2009/10 to 3,470 in 2010/11. The growing number of attacks will be a particular concern at a time when NATO allies are seeking to reduce troop numbers and increasingly hand over security to Afghan forces.

Aside from South Sudan, the latest index sees three more countries join the 'extreme risk' category: Iran (16), Burundi (17) and Nigeria (19). Iran continues to experience a relatively small, but lethal, number of mass-casualty attacks including a twin suicide bombing in Zahedan in July 2010, which collectively killed 27 and wounded approximately 300. These attacks, launched by Jundullah, a Sunni Islamist and Baluchi ethnic group, mean that Iran has one of the highest averages of fatalities per incident at 5.71.

Security conditions in Nigeria remain fragile and a source of concern for investors. The Movement for the Emancipation of the Niger Delta (MEND) has launched attacks beyond the Delta, in the capital, Abuja. MEND is thought to be behind the 1 October 2010 car bombings in the city that killed 12. These bombings took place during celebrations for the country's 50th anniversary of independence. Somalia continues to be the highest risk country in the index, with the Islamist militant group al-Shabaab controlling much of the central and southern areas of the country. However, some of the most devastating attacks take place in the capital, Mogadishu, where al-Shabaab struggles with the Transitional Federal Government, Amonast the worst incidents in the city were armed attacks by al-Shabaab on 8 February and 15 March 2011, which killed 21 and 24 respectively. As the African Union Mission in Somalia (AMISOM) continues to be unable to dislodge al-Shabaab from Mogadishu, mass-casualty attacks are likely to persist in the city.

None of the major Western economies fall within the 'high' or 'extreme risk' bracket. However, the UK (38) is rated 'medium risk,' and ranked highest out of these countries. This is due to the deteriorating security conditions in Northern Ireland, where there was a general increase in the number of terrorist attacks. In contrast, the US is ranked 61 and 'low risk.'

Western countries meanwhile remain concerned about the continued risk posed by radical Islam and the prospect of future attacks on Western interests at home and overseas. "The killing of al-Qaeda leader Osama Bin Laden by US navy SEALs in May has helped US intelligence target senior members and affiliates of the network," said Anthony Skinner, Associate Director at Maplecroft. an "Nonetheless, al-Qaeda has in the past proven its ability to adapt and poses a continuous threat to the West."

Maplecroft's Terrorism Risk Index is accompanied by subnational mapping of all reported terrorist incidents, which are charted globally down to 100m. "Although some countries are rated as 'extreme risk', terrorism attacks can be limited to a specific region or a relatively small number of areas. Thailand is a case in point, where the majority of attacks take place in the southern states," continued Skinner. "Subnational mapping of this kind enables organisations to pinpoint these hotspots and monitor risks to staff, as well as assets, such as factories, refineries and pipelines."



# Fighting Grassroots Terrorism: How Local Vigilance Can Help

### **By Scott Stewart**

Source:http://www.stratfor.com/weekly/20110803-fighting-grassroots-terrorism-local-vigilance-help? utm\_source=freelist-f&utm\_medium=email&utm\_campaign=20110804&utm\_term=sweekly&utm\_ content=readmore&elg=cf9c83cadc8a4e80b686f0f0b896fc36

In the wake of the July 22 Oslo attacks, as I have talked with people in the United States and Europe, I have noticed two themes in the conversations. The first is the claim that the attacks came from an unexpected source and were therefore impossible to stop. The second theme is that detecting such attacks is the sole province of dedicated counterterrorism authorities.

As discussed in last week's Security Weekly, even in so-called "unexpected" attacks there are specific operational tasks that must be executed in order to conduct an operation. Such tasks can be detected, and unexpected attacks emanating from lone wolf actors can

indeed be thwarted if such indicators are beina looked for. Alleged Oslo attack perpetrator Anders Breivik reportedly conducted several actions that would have made him vulnerable to detection had the authorities been vigilant and focused on those possible actions. This is why it is critical to look at the mechanics of attacks in order to identify the steps that must be undertaken to complete them and then focus on identifying people taking such steps. Focusing on the "how" rather than the

"who" is an effective way for authorities to get on the proactive side of the action/reaction continuum.

Considering this concept of focusing on the how, one quickly reaches a convergence with the second theme, which involves the role and capabilities of dedicated counterterrorism resources. The primary agency tasked with counterterrorism in most countries tends to have limited resources that are stretched thin trying to cover known or suspected threats. These agencies simply do not have the manpower to look for attack-planning indicators — especially in a world where militant actors are increasingly adopting the leaderlessresistance model, which is designed to avoid detection by counterterrorism forces.

When these factors are combined they highlight the fact that, as the threat posed by militants adhering to the leaderless-resistance model (whom we frequently refer to as "grassroots militants") increases, so does the need for grassroots defenders.

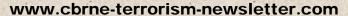
### **Grassroots Threats**

As we noted last week, Breivik's concept of self-appointed and anonymous "Justiciar Knights" (photo) who operate as lone wolves or

in small phantom cells is not a unique concept. Breivik was clearly influenced by the militantgroup case studies he outlined in his manifesto. In recent decades, governments have become fairly efficient at identifying and gathering intelligence on known groups that pose a threat to conduct violent attacks. This is especially true in the realm of intelligence, where technical dramatic increases have been made in the ability to capture and process huge amounts of data from landline, cellphone and Internet communications, but governments have also become quite adept at penetrating militant groups and recruiting informants.

Even before 9/11, government successes against militant groups had led white supremacist groups and militant animal-rights and environmentalist groups to adopt a leaderless resistance model for their violent and illegal activities.

In the post-9/11 world, intelligence and security services have dramatically increased the resources dedicated to counterterrorism, and the efforts of these services have proved very effective when focused on known organizations and individuals. Indeed, in recent years we have seen a trend where jihadist groups like al.





Qaeda and its franchises have encouraged aspiring militants to undertake lone wolf and small cell activities rather than travel to places like Pakistan and Yemen to link up with the groups and receive training in terrorist tradecraft. For several years now, STRATFOR has emphasized the nature of this decentralized threat.

We see no sign of this trend toward leaderless resistance reversing in the near future, and our forecast is that the grassroots threat will continue to grow, not only from the jihadist realm but also from far-right and far-left actors.

### **Stretched Thin**

As noted above, most counterterrorism intelligence efforts have been designed to identify and track people with links to known militant groups, and in that regard they are fairly effective. However, they have been largely ineffective in identifying grassroots militants. The focus on identifying and monitoring the activities of someone connected to a known militant group is understandable given that operatives connected to groups such as Hezbollah or al Qaeda have access to much better training and far greater resources than their grassroots counterparts. In general, militants linked to organizations pose a more severe threat than do most grassroots militants, and thus counterterrorism agencies focus much of their attention on the more potent threat.

That said, grassroots operatives can and do kill people. Although they tend to focus on softer targets than operatives connected to larger groups, some grassroots attacks have been quite deadly. The July 2005 London bombings, for example, killed 52 people, and Breivik was able to kill 77 in his twin attacks in Norway.

One problem for most counterterrorism agencies is that counterterrorism is not their sole (and in some cases even primary) mission. Often, such as the case with MI5 in United Kingdom, the the primary counterterrorism agency also has substantial foreign counterintelligence responsibilities. In the case of the FBI, it has not only counterterrorism and foreian counterintelligence missions but also a host of other responsibilities such as investigating bank robberies. kidnappings, white-collar crime, cyber crimes and public corruption.

The resources of the primary counterterrorism agencies are also quite finite. For example, the

FBI has fewer than 14,000 special agents to fulfill its many responsibilities, and while counterterrorism has become its top mission in the post-9/11 era, only a portion of its agents (estimated to be between 2,500 and 3,000) are assigned to counterterrorism investigations at any one time.

Counterterrorism investigations can also be very labor intensive. Even in a case where a subject is under electronic surveillance, it takes a great deal of manpower to file all the paperwork required for the court orders, monitor the surveillance equipment and, if necessary, translate conversations picked up from the surveillance efforts and run down and or task out additional investigative leads developed during the monitoring. Seemingly little things like conducting a "trash cover" on the subject (sifting through the trash a subject places out on the curb for evidence and intelligence) can add hours of investigative effort every week. If full physical and electronic surveillance is put in place on a subject, such a 24/7 operation can tie up as many as 100 special agents, surveillance operatives, technicians, photographers, analysts. interpreters and supervisors.

Again, given the potential threat posed by known or suspected al Qaeda, Hezbollah or, currently, Libyan government operatives, it is understandable why so many resources would be devoted to investigating and neutralizing that potential threat. However, the problem with this focus on known actors is that it leaves very little resources for proactive counterterrorism tasks such as looking for signs of potential operational activities such as preoperational surveillance or weapons acquisition conducted by previously unknown individuals. Indeed, this is a huge undertaking for agencies with limited resources.

Furthermore, in the case of a lone wolf or small cell, there simply may not be any clear-cut chain of command, a specific building to target or a communication network to compromise the specialties of Western intelligence agencies. The leaderless-resistance organization is, by design, nebulous and hard to map and quantify. This lack of structure and communication poses a problem for Western counterterrorism agencies, Breivik as accurately noted in his manifesto. Also, since this grassroots threat emanates from a large variety of actors, it is impossible to profile potential militants based on race, religion

ethnicity. Instead, their actions must be scrutinized.

### **Grassroots Defenders**

All grassroots militants engage in activities that make their plots vulnerable to detection. Due to limited number the of dedicated counterterrorism practitioners, these mistakes are far more likely to be witnessed by someone other than an FBI or MI5 agent. This fact highlights the importance of what we call grassroots defenders, that is, a decentralized network of people practicing situational awareness who notice and report possible indications of terrorist behavior such as acquiring weapons, building bombs and conducting preoperational surveillance.

Clearly, the most important pool of grassroots defenders is ordinary police officers on patrol. While there are fewer than 14,000 FBI agents in the entire United States, there are some 34,000 officers in the New York City Police Department alone and an estimated 800,000 local and state police officers across the United States. While the vast majority of these officers are not assigned primarily to investigate terrorism, they often find themselves in a position to encounter grassroots militants who make operational security errors or are in the process of committing crimes in advance of an attack, such as document fraud, illegally obtaining weapons or illegally raising funds for an attack.

In July 2005, police in Torrance, Calif., thwarted a grassroots plot that came to light during an investigation of a string of armed robberies. After arresting one suspect, Levar Haney Washington, police searching his apartment uncovered material indicating that Washington was part of a small jihadist cell that was planning to attack a number of targets. multimillion-dollar Hezbollah's cigarettesmuggling network was uncovered when a sharp North Carolina sheriff's deputy found the group's activities suspicious and tipped off the Bureau of Alcohol, Tobacco and Firearms and Explosives, thus launching the massive "Operation Smokescreen" investigation.

Traffic stops by regular cops also have identified several potential grassroots jihadists. In August 2007, two Middle Eastern men stopped by a sheriff's deputy for speeding near Goose Creek, S.C., were charged with possession of a destructive device. Likewise, a traffic stop by a police officer in September 2001 in Alexandria, Va., led to an investigation that uncovered the so-called Virginia Jihad Network. At the time of the 9/11 attacks, the operation's leader, Mohamed Atta, was the subject of an outstanding bench warrant for failing to appear in court after being stopped for driving without a license. More recently, in May 2011 we saw the New York Police Department disrupt an alleged jihadist plot. Then in June, the Seattle Police Department detected a plot that it thwarted with the cooperation of the FBI. Both of these plots were disrupted during the weapons-acquisition phase.

In some countries, networks have been established to promote this concept of heightened local-police vigilance and to provide training for officers and crime analysts. The U.S. government has established something it calls the National Suspicious Activity Reporting Initiative, which is an attempt to provide local police with training to optimize their situational awareness and to help them collect and analyze information pertaining to potential terrorist-planning activity and then to share that information with other agencies enrolled in the program. However, the initiative has only a handful of state and local law enforcement agencies participating at the present time.

But police are not the only grassroots defenders. Other people such as neighbors, store clerks, landlords and motel managers can also find themselves in a position to notice operational planning activities. Such activities can include purchasing bombmaking components and firearms, creating improvised explosive mixtures and conducting preoperational surveillance. On July 27, 2011, an alert clerk at a gun store in Killeen, Texas, called the local police after a man who came into the store to buy smokeless powder exhibited an unusual demeanor. They located the individual and after questioning him learned he was planning to detonate an improvised explosive device and conduct an armed assault against a local Killeen restaurant popular with soldiers from nearby Fort Hood. The clerk's situational awareness and his decision to call the police likely saved many lives.

And it's important to remember than an alert street vendor was the first person to sound the alarm in the failed May 2010 Times Square bombing attempt, and it was a concerned family member who provided authorities with the information to thwart a planned November

Ordinary citizens exercising situational awareness can and have saved lives. This reality has been the driving force behind programs like the New York Police Department's "If You See Something, Say Something" campaign. This program was subsequently adopted by the U.S. Department of Homeland Security as a means of encouraging citizens to report potential terrorist behavior.

zens to report potential terrorist Stat gras

# "Christian Terrorism"?

### By Raymond Ibrahim

Source: http://www.meforum.org/2999/christian-terrorism

In light of the Norway terrorist attack, and as expected, the hail of religious relativism has begun-the idea that, if a "Christian," such as Breivik, commits terrorism, then it is folly to assert that certain Muslim doctrines inspire violence and terror: all becomes relative. A recent AP report titled "Christian terrorist'? Norway case strikes debate," makes this clear: As westerners wrestle with such characterizations of the Oslo mass murder suspect, the question arises: Nearly a decade after 9/11 created a widespread suspicion of Muslims based on the actions of a fanatical few, is this what it's like to walk a mile in the shoes of stereotype? "Absolutely," said Mark Kelly Tyler, pastor of Mother Bethel African Methodist Episcopal Church in Philadelphia. "It clearly puts us in a position where we can't simply say that extreme and violent behavior

associated with a religious belief is somehow restricted to Muslim extremists." "It speaks to cultural assumptions, how we are able to understand something when it (comes from) us," Tyler said. "When one of us does something terrible, we know that's not how we all think, yet we can't see that with other people." Psychologists say stereotypes come from a deeply human impulse to categorize other people, usually into groups of "us" and "them."

The report goes on to give the opinions of an array of sociologists, anthropologists, and psychologists, who regurgitate the same aforementioned themes on "a fanatical few," "extreme and violent behavior," "cultural assumptions," and "stereotypes." Not once do any of these soft-scientists bother investigating,

There is one other factor to consider. As we have previously discussed, counterterrorism spending comes in a perceptible boom-and-bust cycle. Next month will mark the 10th anniversary of the 9/11 attacks. Since those attacks there has not been a successful large-scale terrorist attack on U.S. soil. This, along with the budget problems the United States is facing, will increase the current downward trend of counterterrorism funding in the United States and accentuate the need for more grassroots defenders.

let alone pointing out, what Christianity and Islam actually teach regarding violence.

Nor do they seem cognizant that there is a major difference between what people do in the name of religion and what the religion itself commands—just as there is a major difference between historical descriptions of war in the Bible and timeless prescriptions to wage war in the Koran.

Nor are these important differences limited to theory, but rather manifest themselves in reality: when jihadists attack in the name of Islam, such as on 9/11, high-ranking Muslim clerics praise them and Muslims celebrate in the streets; conversely, no Christian preacher has praised Breivik's terrorism, nor are Christians dancing.

The report continues:

"Breivik is not a Christian. That's impossible. No one believing in Jesus commits mass murder," Bill O'Reilly said on his Fox News show. That makes sense to Joyce Dubensky, CEO of the Tanenbaum Center for Interreligious Understanding. She said it also makes sense that "millions of Muslims say Osama bin Laden is not a Muslim, that no one who believes in the prophet Muhammad commits mass murder."

Note again how the stress is entirely on what people "believe" and "say"—not what Christian and Muslim doctrines so unequivocally teach. Worse, that "millions of Muslims say Osama bin Laden is not a Muslim" is a curious.

assertion, considering that the Obama administration saw that he was given an Islamic burial so as not to anger the Muslim world (jihadists who go down in sea receive double the brownie points that land-dying jihadists receive—which are already considerable, a la 72 celestial concubines, etc.).

The one rare mention in the report of actual teachings comes from another psychology professor: "If you're a Christian and you see this Norway murderer, you say, I have these teachings and I haven't murdered anyone, so the teachings can't be the problem. But if you're talking about the 'other,' it's different. And if you don't know what the actual Muslim

teachings are, it seems like a plausible explanation."

Quite the contrary, if you know what Islam teaches concerning the jihad and the non-Muslim—tellingly known as the "infidel" violence becomes a very "plausible explanation."

If lamentable, none of this is surprising: because Western secularists cannot fathom the importance of doctrine to believers; cannot take religion seriously—seeing all scriptures as little better than poetry to be interpreted any which way—they project their indecisive worldview onto the decisive other, much, ironically, to secularism's own detriment.

Raymond Ibrahim, an Islam specialist, is a Shillman Fellow at the David Horowitz Freedom Center and an Associate Fellow at the Middle East Forum.

# Haqqani Network Growing Stronger at the Expense of the Tehrik-e-Taliban

By Arif Jamal

Source: http://www.jamestown.org

The Tehrik-e-Taliban Pakistan (TTP) seems to disintegrating as various be slowly commanders try to pull it in different directions. A clear indication of this process came when the TTP Commander in the Kurram Agency, Fazal Saeed Haqqani, announced that his group had seceded from the TTP (for Fazal Saeed Haggani, see Militant Leadership Monitor, July 2011). Fazal Saeed Haggani also announced the formation of a new group called Tehrik-e-Taliban Islami Pakistan (TTIP) (Dawn [Karachi] June 28). Haqqani said his group was not happy with the TTP's policy of attacking civilian targets, a major reason for the split. However, Haggani and his group have been involved in the murders of innocent Shi'a Muslims. In the very first statement to dissociate his new group from the TTP, Haggani announced that his group would not carry out any attacks on the Pakistani security forces (The News [Karachi] June 28). He also announced that the United States is the TTIP's "main enemy" (Daily Times [Lahore] June 28).

The action of Fazal Saeed Haqqani has completely eliminated the TTP from the Kurram agency, as Haqqani vowed that he would not allow the TTP to operate there: "It is my area and I will ensure that no locals or outsiders oppose our policies and create problems for us in Kurram Valley" (The News, June 30). Like Maulvi Nazir and Hafiz Gul Bahadur, Fazal Saeed Haqqani is closely allied with the Haqqani Network in Afghanistan (Dawn, July 5). The Haggani Network desperately needed a foothold in the Kurram agency, which only Fazal Saeed Haggani could provide. According to Mansur Khan Mehsud of the FATA Research Center, Fazal Saeed Haggani is occupying a portion of the main road, the Thall-Parachinar road, connecting Kurram Agency with the rest of the country. While still a TTP commander, Fazal Saeed Haggani did not allow Shi'a Muslim residents to use that road. Consequently, they had to go to Afghanistan first to go to other parts of Pakistan. [1] With Fazal Saeed Haggani in charge of that road, the Haggani Network and other Taliban militants can use the Kurram Agency as their base to carry out attacks inside Afghanistan or to provide sanctuary. [2]

NATO forces in Afghanistan identified the Haqqani Network as the group responsible for a brazen attack using nine suicide bombers against Kabul's luxury Intercontinental Hotel on June 28 that killed 20 people, including the suicide bombers (AP, June 30). Shortly afterward, the Haqqani Network suffered a major blow when NATO troops and Afghan.

Special Forces mounted a raid on a Haggani Network training camp in Afghanistan's Paktika Province. The July 20-22 operation killed more than 50 insurgents in a base said to be used as a staging point for Haggani Network and foreign fighters. A large stockpile of arms was seized in the operation, which NATO sources said was based on intelligence provided by disenchanted insurgents (Daily Times, July 23; AFP July 22; Reuters July 22).

Nevertheless, Fazal Saeed Haggani's rebellion against the TTP has immensely strengthened the Haggani Network while weakening the TTP. According to one report, TTP commander Hakimullah Mehsud has become more and more isolated over the last year (Express Tribune [Karachi], July 5). On June 27, Hakimullah suffered a setback when unknown persons killed Shakirullah Shakir, a spokesman for the Fidayeen-e-Islam [suicide-bombing] wing of the TTP. Shakirullah was to replace Qari Hussain Mehsud, who was killed in an October 2010 drone strike and was known as Ustad-e-Fidayeen (master [or teacher] of the suicide bombers) (Daily Times [Lahore] June 28). Commander Tariq Afridi's Taliban group in Darra Adamkhel and Khalid Omar's Mohmand group are already operating independently of the TTP. Lashkar-e-Islam in Khyber Agency, led by Mangal Bagh, is pro-Army and does not accept TTP patronage. The TTP breakup is a great success for Pakistan's Inter-Services Intelligence (ISI), which has been working for some months to deliver Kurram Agency to the Haggani Network so that it could operate more freely in view of the emerging regional scenario

(see Terrorism Monitor, December 16, 2010). Distrust among the TTP militants seems to be According to another report, growing. Hakimullah Mehsud and his deputy Waliur Rehman rarely meet; when they do, they do not meet alone and only after making sure neither of them is carrying arms (Dawn, July 5). Fazal Saeed rebelled against the TTP on the eve of the military operation that started on July 3. Army troops moved into the central Kurram agency from the town of Sadda and Tal area in Hangu District, backed by helicopters, tanks, and artillery. The aim of the operation was to destroy the militants still loyal to Hakimullah Mehsud (The News, July 4). Although this military operation was ostensibly initiated against the militants. Shi'a Muslim residents believe it is equally directed against them. A knowledgeable Pakistani columnist, Dr. Mohammad Taqi, says that the operation is aimed at opening the Thall-Parachinar road for the Haqqani Network and other pro-Army jihadi groups (Daily Times, July 7). More importantly, it is aimed at punishing those people in the Kurram Agency who have resisted the Haggani Network and the Pakistan Army's support for the Taliban. The balance of power has shifted in favor of the Haqqani Network for the first time with Fazal Saeed Haggani openly on their side. Although several local Shi'a leaders in Upper Kurram vow to fight back, it is safe to say that they are losing the battle, at least for now. [3]

Arif Jamal is an independent security and terrorism expert and author of "Shadow War -The Untold Story of Jihad in Kashmir."

#### Notes:

1. Mansur Khan Mehsud, "TTP Divided in Kurram Agency," FATA Research Center, n.d., http://www.frc.com.pk/linkc/articlecont/41.

2. For the strategic importance of this road for the Pakistan army and the Haqqani Network, see Dr. Mohammad Taqi, "Comment: The Sham operation in Kurram," Daily Times, Lahore, July 7. Available at <u>http://www.dailytimes.com.pk/default.asp?page=2011%5C07%5C07%5Cstory\_7-7-2011\_pg3\_2</u>. 3. Telephone interviews with some local leaders through research assistant, July 2011.

## U.S. mulls terror list for Haggani network

Source:http://www.upi.com/Top\_News/US/2011/09/28/US-mulls-terror-list-for-Haggani-network/UPI-37541317185545/#ixzz1ZK5yeAPH

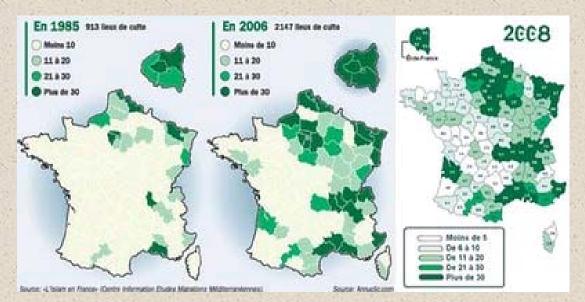
The United States is reviewing (Sept 28, 2011), whether to place the entire Haggani network on the terror list, State Department spokeswoman Victoria Nuland said.



### France: 100-150 mosques in progress

Source:http://www.20minutes.fr/article/765248/entre-100-150-mosquees-construction-france

100-150 mosques are currently being built in France, the president of the French Council of the Muslim Faith, Mohammed Moussaoui, told RTL. Moussaoui said that most are financed by the worshipers and very few from abroad. The interior minister, Claude Guéant, said three months ago that in the past decade the number of mosques increased from 1000 to 2000. Guéant wants to stop Friday prayers in



the streets. According to Moussaoui, 17-23% of French Muslims go to Friday prayers, which he says distinguishes between the practicing and non-practicing Muslims. He repeated that prayers in the streets were outrageous, but stemmed from lack of places in mosques. According to a senior official, there are 17 mosques in Paris, all filled up, and they can't accommodate more than 13,000 people, which is clearly insufficient.

### Mumbai bombings tied to homegrown group

Source: http://www.homelandsecuritynewswire.com/mumbai-bombings-tied-homegrown-group

Indian government officials have focused on domestic terror, indicating that last month's triple-bombing in Mumbai was the work of a homegrown group, the Indian Mujahideen.

The three bombs, detonated during rush hour, killed twenty-six and wounded more than 130, were the first attacks in Mumbai since the November, 2008 attack that riveted the world.

No one has claimed responsibility for the attacks three weeks ago. A police investigation is still ongoing, and according to Home minister P. Chidambaram, all indications are that a homegrown group is responsible.

Investigators' suspicion has fallen on the Indian Mujahideen, a shadowy group with ties to Lashkar-e-Taiba, the Pakistani terror group responsible for the 2008 Mumbai attacks. Those attacks resulted in accusations by India of Pakistani involvement, and the subsequent suspension of peace talks between the two sides. The peace talks were resumed earlier this year.

The Indian Mujahideen is also held responsible for three smaller attacks, including a bombing in the capital, New Delhi.

The recent coordinated triple-bombing made use of ammonium nitrate-based explosives, the same formulation used by Indian Mujahideen in its previous attacks.

The Indian Mujahideen sprouted from the outlawed Students' Islamic Movement of India, a group described in a WikiLeaks-released cable from the U.S Embassy as "a radical fringe of technically savvy disaffected Indian Muslims who embrace Islamic extremism in response to perceived injustices by the Hindu majority."

The Indian Mujahideen made contact with Lashkar-e-Taiba after 2002, and were provided by them with with weapons and <u>bomb</u>

production training. For their part, Lashkar-e-Taiba denies any links to the Indian terror group.

Indian officials are also scrupulously avoiding any mention of Pakistani influence of any kind with the Indian Mujahideen attacks, since there are continued peace talks between Indian and Pakistani officials currently underway. Pakistani officials did not comment on the attacks. The official line is that there have been no demands made or responsibility claimed in the recent attacks, that they are just general, undirected mayhem. However, the breakdown of peace talks between India and Pakistan is likely a goal shared by both Lashkar-e-Taiba and the Indian Mujahideen.

# **Conspiracy of fire - The Globalization Of Anarcho-Terrorism**

Source: http://iacsp.com/latest\_article.php

### **Origins - Ancient and Modern**

The term "anarchy" is rooted in ancient Greek; meaning "without a leader". As a philosophical worldview, "anarchism" began thousands of years ago with the founder of Stoicism: Zeno of Crete. Zeno "repudiated the omnipotence of the state, its intervention and regimentation, and proclaimed sovereignty of the moral law of the individual", according to the renown Russian anarchist Peter Kropotkin. in the arena of ideas and actions against the state. Any rebel can make brash statements, but the Greeks back it up with action, and thus have won the respect and admiration of their comrades throughout the world.

The Greek anarchists even enjoy some degree of autonomy in their urban sanctuary called Exarcheia - a neighborhood of Athens notorious for its counter-cultural and radical demographic. Even the police don't enter



Today, Greece maintains that anarchist pedigree. In the eyes of their comrades around the world, the modern Greek anarchist embodies the ideal anti-authoritarian. The Greek anarchists have become the gladiators

Exarcheia unless necessary, lest they provoke a riot.

But far from satisfied, Greek anarchists are radical as ever, incited by economic crisis and austerity measures that have followed.

Memories of state oppression when Greece was ruled by a dictatorship persist among the masses, providing an authentic backdrop to their special brand of anarchism.

The fact that Greece is currently a democracy, however, is not sufficient to pacify the wrath of Greek insurrectionary anarchists, who threaten to oppose authority in whatever form it takes, as a matter of principle.

### **Embassy Bombings: Athens**

On 1-2 November 2010, anonymous adversaries sent parcel-bombs to various targets in Athens and other cities in Europe. The targets included the embassies of Belgium, Mexico, Chile, Germany, France, Switzerland, Bulgaria, Russia; the International Court of Justice in The Hague; the offices of speculations that Al-Qaeda might have been behind the plot.

Theories of jihad however were soon replaced by the sinking realization that this was a case of domestic terrorism, as an obscure Greek anarchist group calling itself "The Conspiracy of Fire Cells" issued a communique claiming responsibility and declaring its intention to continue attacks, especially citing the ongoing social welfare austerity measures as motivation:

"Today it is imperative to launch a new phase in the development of revolutionary thought and action. A quantum leap that will bring common ends, which are hundreds of miles away, one step closer. Our goal is to create a unified anti-authoritarian international network of guerrilla groups and autonomous



President Nicholas Sarkozy of France, Italian Prime Minister Silvio Berlusconi and German Chancellor Angela Merkel; the European Law Enforcement Organization of the European Union (Europol); and Eurojust, the EU legal organization dedicated to combating organized crime.

With one exception, all these bombs were either intercepted or exploded without casualties (the bomb sent to the Mexican embassy exploded en route and injured the courier employee, causing minor injures). But the coordinated attack effectively terrorized Greece during an election week, and raised individuals.....[This will involve] coordinating subversive activities and attacks at the international level. [Such global coordination will facilitate the exchange of] knowledge in the field of sabotage [and] collective solidarity" [with] imprisoned comrades, [and] an infrastructure to support wanted rebels."

The Conspiracy of Fire's statement continued in declaring solidarity with eco-terror groups such as the Earth Liberation Front (ELF) and the Animal Liberation Front (ALF), as well the Italian anarchist group FAI (Federation Anarchy Informal), the anarchist Mexican group Praxedis G. Guerrero Autonomous Celle:

Immediate Revolution; and the armed Argentinean insurgents (the Luciano Arruga Brigades).

Furthermore, the Conspiracy of Fire's communique glorified and encouraged the terror-tactics used by these groups which include:

- The placement or delivery of explosive devices targeting politicians, security forces and police barracks, court houses, and other "symbols of power";
- Attacks on tourist offices and embassies;
- IEDs and firebombs targeting police vehicles;
- IEDs and firebombs targeting construction equipment;
- Sabotage of construction equipment;
- Arson, specifically targeting banks;
- Vandalism;
- Theft of weapons from police;
- Robbery from targeted entities

The Conspiracy of Fire then presented a timeframe for the start of its "new phase", stating that they hoped to be "presenting

including AK-47 assault rifles, semi-automatic firearms, grenades, TNT, and ammonium nitrate explosives.

But the arrests only served to empower the reputation of the Conspiracy of Fire Cells around the world. Anarchists from America to Russia carried out acts of solidarity to honor the imprisoned comrades in Greece.

### **Embassy Bombings: Rome**

On 23 December 2010, parcel-bombs were sent to the Chilean and Swiss embassies in Rome, only a month after the similar attack in Athens.

The packages exploded in the hands of the two embassy employees who opened them. Two days later, a letter-bomb arrived at the Greek embassy in Rome, but was neutralized. The claim of responsibility came from a militant anarchist group called the Federation Anarchy Informal - in Italian; Federazione Anarchica Informal (FAI):

"We attacked again and we did it in response to the appeal of Greek comrades from "Conspiracy of Fire Cells". For this reason we attacked, anew, one of the structures



integrated international calls" in coming months. This theme of internationalization would increasingly become a motivating factor for the group.

On 4 December 2010, Greek authorities responded by carrying out a major counterterrorism operation targeting the Conspiracy and other anarchist-insurgency groups such as the Revolutionary Struggle. In addition to arrests, authorities confiscated weapons representing the Greek state and its servants in support to the comrades who were arrested in Athens and for the "Conspiracy"-plan which, like ours, is based on the practices and the method of revolutionary violence. We have decided to make our voice heard again through words and actions. Destroy the system of domination. Long live FAI, long live Anarchy. Federazione Anarchica Informal revolutionary cell Lambros Fountas".

### A Shared Legacy of Terror

Modern anarchist theories spread through Greece and southern Europe in the 19th century with the influence of revolutionaries like Mikhail Bakunin.

Anarchists in Italy and Greece have long

# **Revolutionary solidarity** with all those who fight against Capitalism & State

After the young Alexis Grigoropoulos was murdered by Greek cop, riots spread throughout the whole country for several weeks. But the revolt didn't cease at the end of 2008, neither did it start on the day of the murder. The attacks against the structures of State and Capital went on and spread to several smaller towns in Greece. About 200 attacks with fire and growing artisan bomb attacks were carried out under the name of the Conspiracy of Cells of Fire (CCF). The attacks targeted banks, government institutions, police stations, offices of political parties, houses of politicians, judges, criminologists and journalists, private security firms, companies building prisons. and always accompanied by elegantly critical and nihilistic claims of anarchist responsibility.

In September 2009 extensive anti-terror raids attempted to strike the CCF, these raids became one more political tool to attack the wider anarchist-anti-authoritarian movement, a situation which intensified when two members of the CCF were captured during an operation in November 2010, Athens. Against the ongoing legalistic kidnapping of November 2010, Attens. Against the ongoing legatistic kidnapping of our comrades and for the escalation of struggle for total liberation, the Conspiracy of Cells of Fire: Illegal Sector called for an informal global project based on anarchist subversion, direct action and international solidarity. These papers document some of the many communiques, letters and legal & court updates concerning the Conspiracy of Cells of Fire, the accused comrades of the same case, here blick in university in the form the liber formation of the plus solidarity actions resulting from the call for a formation of an Informal Anarchist Federation / International Revolutionary Front.

actforfreedomnow.blogspot.com

shared close ties. The "Democrats Club", perhaps the first anarchist group in Greece, was co-founded by Italian Amilcare Cipriani

and Greek Emmanouel Dadaoglou. The two later took leading roles in the insurrection against King Otto of Greece in 1862.

This tradition of cooperation between Greek and Italian revolutionaries survives today in the relationship between the Conspiracy of Fire



# OUR LIVES OF BURNING VISION

About the Conspiracy of Cells of Fire & more

Cells and the FAI. Not only do the two groups emulate each others' tactics, but they have even named units in honor of each other.

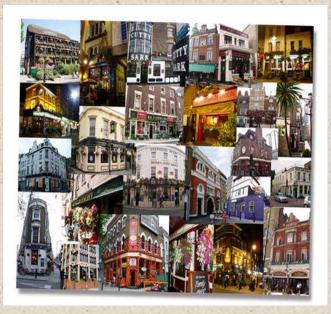
Erik Miller is an intelligence analyst and case-officer at the Institute of Terrorism Research and Response. He specializes in anti-authoritarian forms of domestic terrorism. Previously, he has fulfilled roles at organizations such as the Middle East Forum, the David Project, the Foundation for the Defense of Democracies, and the Chapel of Four Chaplains.



415

# SAS scouts shopping centres as fears of London 2012 terror attack grow

Source:http://www.mirror.co.uk/news/top-stories/2011/04/11/sas-scouts-shopping-centres-as-fears-oflondon-2012 -terror-attack-grow-115875-23052564/#ixzz1UGcSlgIT



THE SAS is secretly scouting major shopping centres amid fears of an attack by Islamic extremists during the 2012 Games.

An insider confirmed the news as a report claimed that terrorists could be planning a Mumbai-style raid during the Olympics.

Risk consultants Exclusive Analysis said "soft targets" such as pubs were most likely to be hit but singled out the Westfield Stratford City shopping centre, in East London, as being at high risk.

The group also warned against focusing on Islamists, saying Irish republican dissidents were plotting to disrupt the Olympic torch route. The Association of Chief Police Officers dismissed the study as "inaccurate".



### Westfield Stratford City shopping centre



# How to Forecast and Preempt al-Qaeda's Catastrophic Terrorist Warfare

By Joshua Sinai, Ph.D.

Source: http://www.homelandsecurity.org/journal/articles/sinaiforecast.htm

The aim of this article is to provoke consideration of a new way to conceptualize al-Qaeda's intentions and plans to conduct catastrophic warfare against the United States, its allies, and other threatened nations around the world. In response to the horrific attacks of 11 September 2001, follow-on attacks in Southeast Asia and the Middle East, and several thwarted plots in Europe, anticipating and preventing future attacks by al-Qaeda and its affiliated terrorist groupings have become first-order national security priorities for many of the world's intelligence and law enforcement communities. Such analysis is also required in nongovernmental, open-source the communities as well. Although it is difficult to predict the likelihood of every major attack by a group such as al-Qaeda, because terrorist groups have the advantage of striking at a time and location of their choosing, there already exists a wealth of diagnostically predictive indicators pointing to the next waves of catastrophic attacks by a group such as al-Qaeda and its network of terrorist allies.

This article outlines seven predictive attack indicators to forecast catastrophic terrorism. Political leaders, policy planners, and military, intelligence, and law enforcement operators at all levels will greatly improve their capabilities to respond to the terrorist challenge if they operationalize these predictive indicators against al-Qaeda's historic and potential strategies, tactics, and targeting. Such "redteaming" of a terrorist group's warfare potential is similar to the way military commanders play adversary forces (the "red teams") against their own forces (the "blue teams").

Building a robust predictive capability to anticipate and preemptively prevent attacks by groups such as al-Qaeda now is more important than ever because of their determination to inflict catastrophic damage upon their adversaries. As demonstrated by the suicide attacks against Australian and British tourists in Bali, Indonesia; Israeli tourists in Mombassa, Kenya (where an additional 250 Israeli lives could have been lost had the Arkia airliner been hit by the shoulder-fired rocket); and the large residential complex in Riyadh, Saudi Arabia, housing American and other foreign families; as well as a suicide attack by two British al-Qaeda operatives on a popular seaside bar in Tel Aviv; al-Qaeda is as determined as ever to demonstrate its viability as the world's most lethal terrorist group.

The catastrophic attacks of 11 September and the follow-on poisonous anthrax letter campaign (which reportedly was not carried out by al-Qaeda) have ushered in a new terrorist warfare paradigm in which attacks against the United States and its allies have vastly escalated in the lethality of their weaponry and targeting. The threshold from "conventional" low-impact terrorist warfare has been crossed, as demonstrated by the horrific attacks against the World Trade Center and news reports about interest in acquiring or actual experimentation by al-Qaeda in chemical, biological, radiological and nuclear devices and weapons-however crude and low tech. As a consequence of these factors, the new means of terrorist attacks we are likely to face will involve not only such weapons of mass destruction and disruption but conventional means to attack critical infrastructural targets such as nuclear and chemical plants, agricultural nodes such as livestock feeding centers, and the heart of the American and world economy-such as the New York Stock Exchange-with catastrophic human and economic consequences. Usama bin Laden's al-Qaeda terrorist network and its satellite affiliates are the most likely groups to carry out such catastrophic attacks because of their intent-a virulent hatred of their adversariescapability, and resources.

As the top leaders, members of sleeper and active cells, and other operatives of al-Qaeda and its allies are being arrested or killed in their former centers of gravity in Afghanistan, Pakistan, and other parts of the world (reportedly, some 3,000 operatives, forming one-third to one-half of the group's upper and lower echelons, have been eliminated as actives.

terrorists), there still undoubtedly remain hundreds of new leaders, operatives, and sleeper cells armed with target folders for the next waves of catastrophic terrorist operations. The U.S.-led overthrow of al-Qaeda's Taliban allies in Afghanistan and Saddam Hussein's regime in Iraq, as well as holding Taliban and al-Qaeda operatives in detention centers such as Guantanamo Bay, cumulatively are likely to serve as major triggers for their remaining operatives to seek catastrophic revenge on behalf of their fallen, retreating, or arrested comrades.

To forecast the next waves of likely catastrophic terrorist attacks, this analysis uses a methodology based on seven predictive attack indicators, generated from al-Qaeda's mindset, modus operandi, and target selection based on its training handbook (available on the Department of Justice website); public statements by bin Laden and his associates that have been broadcast on television news programs; and the extensive media reporting of the group's previous failed attacks and plots (as outlined in captured documents), which often serve as blueprints for its future targeting.

To anticipate, preempt, and deter future catastrophic attacks, the following methodology employing seven predictive attack indicators can be operationalized to forecast the next waves of al-Qaeda terrorist operations, as outlined in the following threat matrix.

## Methodology to Forecast Catastrophic Terrorism Against the U.S. Homeland

Indications and Warning Indicators and Observables Preceding the 11 September 2001 Attacks

Terrorist Group	Al-Qaeda	Armed Islamic Group (GIA)
Previous Attacks or Plots	1993 World Trade Center bombing	Dec. 1994 attempt to plunge airliner into Eiffel
	1993 plots against Holland Tunnel, Empire State Building, UN headquarters	Tower
	Mid-1990s plot to bomb CIA headquarters	
	December 1999 plot to bomb Los Angeles International Airport	
	October 2000 bombing of USS Cole	
	September 2001 plot to crash aircraft into U.S. Capitol and White House	
Modus Operandi	Meticulous planning as outlined in captured al- Qaeda training manual	
	Innovative operationally and tactically	
	<ul> <li>Training to fly commercial aircraft at U.S. and other flight schools</li> <li>Seek highly visible and symbolic targets</li> </ul>	
Weapons and Devices	Interest and training in using commercial aircraft as weapons of mass destruction	

State Sponsor Ties	Afghanistan's Taliban rulers provided safe haven and logistical support	
	State sponsor Iraq seeks vengeance against United States	
Geography	Worldwide operational cells, including cells in the United States	
Significant Historical Dates	12 September date of sentencing of African embassy bombing conspirators	
Triggers	12 September sentencing date of conspirators held in lower Manhattan triggered attack on 11 September	
= Terror Attacks	11 September simultaneous suicide bombing attacks against World Trade Center and Pentagon	

# Attack indicator #1: Previous terrorist attacks, failed attacks, or plots not yet executed, which serve as blueprints for intentions and future targeting

Al-Qaeda and its allies have carried out numerous successful attacks since the early 1990s; however, they also have experienced quite a few significant failed attacks. In other cases, some plots have never been executed. Synthesizing the lessons learned from a group's successful attacks, failed attacks, and plots can generate insight into its future intentions and capabilities. Plots, for example, can be uncovered by covertly penetrating a group, capturing its documents, or interrogating its apprehended operatives. In the case of al-Qaeda, much insight into its warfare proclivity can be gained by examining its training manual, which spells out missions that include destroying a nation's foreign embassies, critical infrastructure nodes (such as vital economic sectors and bridges), and even places of amusement (because they are considered sinful).

Underlying the first predictive indicator are some of the following historical observables and actions:

- The February 1993 bombing of the World Trade Center towers. This attack resulted in extensive property damage and some loss of life but failed to bring down the towers. The bombing was intended to be accompanied by the bombing of several other targets in New York City, such as the Empire State Building, the Holland Tunnel, and United Nations headquarters.
- In December 1994, an al-Qaeda affiliate, the Algerian Armed Islamic Group, hijacked an Air France Airbus with 171 passengers aboard, intending to plunge it into the Eiffel Tower. None of the hijackers could fly the aircraft to its intended target, so, instead, the plane landed in Marseilles, where French police stormed it.
- In the mid-1990s, Ramzi Yousef, the mastermind of the 1993 World Trade Center bombing, while in the Philippines, plotted to blow up 11 U.S. airliners and, in a separate plot, fly planes filled with explosives into the CIA headquarters in Langley, VA, and nuclear facilities elsewhere in the United States.
- In December 1999, an al-Qaeda affiliate was involved in a foiled plot to bomb Los Angeles International Airport. At the same time, al-Qaeda operatives were foiled by Jordanian security authorities in their attempt to blow up tourist sites in Jordan, and internal hurdles prevented them from bombing the U.S.S. *Sullivans* in the Yemeni port of Aden.



- On 8 September 2001, two al-Qaeda operatives pretending to be journalists assassinated Northern Alliance commander General Ahmed Shah Masoud at his Afghanistan base by detonating a bomb concealed in their video camera.
- The airplane that ultimately crashed into the Pentagon during the 11 September hijackings reportedly also targeted the U.S. Capitol and the White House. The fourth airplane, which crashed in a Pennsylvania field, reportedly was unable to crash into the U.S. Capitol or the White House, or, in another published although unconfirmed scenario, was en route to crash into a nuclear facility.
- Al-Qaeda operatives had planned to hijack airplanes in Britain and crash them into the Houses of Parliament and London's Tower Bridge.

Operationalizing attack indicator #1 yields this forecasting assessment: the 11 September bombing of the World Trade Center signifies that when al-Qaeda fails in its initial mission (in this case, the abortive 1993 attack), it is likely to return—whatever length of time is required to prepare for the next mission—to complete that objective. It can be surmised, therefore, that al-Qaeda operatives are likely to persist in their objective of attacking the following that are part of their target folder (all information is entirely speculative): the Holland Tunnel, the Empire State Building, United Nations headquarters, the Eiffel Tower, the CIA headquarters, the U.S. Capitol, the White House, and nuclear power facilities. In addition, Disney World amusement parks are likely targets. In Britain, the Houses of Parliament and the Tower Bridge, which reportedly were contemplated by al-Qaeda as part of their 11 September worldwide attack repertoire, are still likely to remain at the top of al-Qaeda's ranking of trophy targets.

In addition, the September 2001 assassination of General Masoud by operatives in disguise and several attempts since then to assassinate members of the current Afghan leadership portend continuous efforts by al-Qaeda operatives and their allies to assassinate leaders of their adversaries. Of particular concern are likely efforts by these terrorist operatives to carry out their assassination attempts in disguise or to use operatives who do not fit regular profile attributes in order to evade possible detection.

#### Attack indicator #2: A terrorist group's modus operandi, especially tactics

Al-Qaeda's modus operandi, as demonstrated by the 11 September attacks and outlined in its training manual, involves meticulous planning, training, and precisely timed simultaneous execution. Such warfare capability is attained through extensive training and operational and tactical innovations.

Based on its modus operandi, publicly announced intentions, and previous actions, al-Qaeda's future attacks will likely involve some of the following tactics:

- Truck bomb attacks on the ground or using aerial or maritime delivery means, such as miniature submarines or shipborne containers, to transport chemical, biological, radiological, or nuclear devices to a targeted site.
- Driving a truck loaded with a hazardous-material explosives against a prominent target, such as a tunnel, bridge, or busy downtown area.
- Detonating a radioactive dispersal device (a "dirty" bomb) near a nuclear power facility or a major financial center, such as the New York Stock Exchange.

# Attack indicator #3: Use of particular types of weapons and devices that a terrorist group perceives will achieve its objectives

The simultaneous suicide bombing attacks of 11 September portend that the next phase will likely involve even more catastrophic assaults, with each successive plot employing highly innovative and deadlier weapons and devices to inflict maximum casualties and physical damage.



Current news reporting is filled with discussions of possible chemical, biological, radiological, or nuclear attacks by al-Qaeda operatives. Such speculation is not without foundation. Bin Laden's Afghan training camps taught skills for using weapons of mass destruction—such as feeding poison gas through the air vents of office buildings. Other reports claimed that bin Laden's operatives tried to obtain uranium from the former Soviet republics but instead were given low-grade reactor fuel and radioactive garbage. Also possible, in this catastrophic scenario, are attacks that would use conventional or unconventional explosives against a nuclear power plant or chemical facility.

A chemical attack could be carried out by a crop-dusting plane spraying sections of a city. One of al-Qaeda's operatives who was involved in the 11 September attacks reportedly had in his possession a manual for operating crop-dusting equipment, so such an attack should not be discounted.

Another worst-case scenario might involve al-Qaeda operatives crashing a truck into the New York Stock Exchange building (which reportedly has inadequate perimeter defenses) to detonate a dirty bomb mixed with conventional and radioactive materials. Such an attack would render the stock exchange and its immediate surroundings inactive for weeks, setting off temporary worldwide economic turmoil—although this might be offset by the backup computer data storage systems located elsewhere.

The London Stock Exchange, which has already been contemplated as a target by al-Qaeda, represents another likely trophy target, also with potentially devastating economic consequences worldwide.

Based on al-Qaeda's intention to inflict maximum economic damage, another worst-case scenario involves a biological agent attack against a U.S. agricultural sector, which would produce an impact similar to that of the foot-and-mouth outbreak that devastated British agriculture. Such an attack would also severely impact the U.S. and worldwide commodities trading market. Similarly, a terrorist-induced outbreak of severe acute respiratory syndrome would devastate a region's tourism or export industries.

#### Attack indicator #4: The objectives of a group's state sponsor

State sponsors are crucial to terrorist groups engaging in catastrophic warfare because the resources of a state can be helpful in so many ways. Afghanistan's Taliban rulers provided bin Laden and al-Qaeda with a safe haven. Saddam's regime in Iraq, until its overthrow, may have provided the group with some degree of support because of the convergence of their objectives, particularly in taking revenge against the United States. According to press reports, terrorists have been trained at Iraqi camps in chemical and biological warfare and in flying commercial aircraft. Press reports also indicated that an al-Qaeda operative, Muhammad Ataf, met an Iraqi intelligence official in Prague several times. Iran now is reported to provide al-Qaeda with logistical and other forms of support, including collaboration with Iran's terrorist proxy, the Lebanese Hizballah.

Although there may be few apparent smoking guns, it is reasonable to assume that al-Qaeda is interested in obtaining the support of Iran's radical clerical leaders in mounting its catastrophic warfare against their common adversaries. Such state support would provide al-Qaeda with access to certain types of weapons of mass destruction that would be difficult for the group to obtain on its own.

#### Attack indicator #5: The geographic factor

The geographic factor is a crucial predictive indicator because it pinpoints a group's operational center of gravity and logistical capability to reach, conduct surveillance of, and attack its adversary. Al Qaeda is the umbrella organization of an international network of like-minded groups with hundreds of cells around the world. These groups operate as planets in al-Qaeda's solar system, which makes them highly dangerous because they already possess the infrastructure to carry out terrorist attacks in any part of the world, as demonstrated by their capability to carry out attacks with relative ease in dispersed countries such the Philippines, Pakistan, Kuwait, Saudi Arabia, Tunisia, Morocco, and Kenya, Mithe

reported sleeper cells in Western countries such as Britain, Spain, and the United States. Already, al-Qaeda operatives have carried out or attempted to carry out attacks against American targets in these countries, including a thwarted attempt by an al-Qaeda cell to attack American and British warships in the Strait of Gibraltar.

Moreover, al-Qaeda has expanded its geographic target folder to include Israel, as demonstrated by its successful attack in Kenya against Israeli tourists and the near-miss attack against the Israeli airliner. In fact, in May 2003, two British nationals allegedly affiliated with al-Qaeda traveled to Israel to carry out a suicide bombing of a popular bar in Tel Aviv.

Based on this predictive indicator, potential regions to be targeted by al-Qaeda are likely to range from the United States to foreign lands, especially those where the United States maintains facilities that represent significant trophy targets, such as military bases or symbols of America's economy—a fast food restaurant chain, a hotel chain, a cruise liner, or car dealerships.

#### Attack indicator #6: Historical dates of particular significance to terrorist groups

Terrorist groups, particularly religious groups, place a high premium on historical dates that are significant to their religion or their religio-ethnic community. Other types of historical dates, such as politically or militarily traumatic events, are also significant. 11 September may have been especially significant because the conspirators who carried out the 1998 African embassy bombings were to be sentenced the following day for their crimes. During that period, the conspirators were in a holding cell at a courthouse in downtown Manhattan near the World Trade Center, which fact may have propelled the terrorists to attack on the preceding day.

Other significant historical dates that are likely to trigger future al-Qaeda attacks are

- 17 January (the commencement of Operation Desert Storm)
- 19 March (Jerusalem Day proclaimed by Ayatollah Khomeini to demand the "liberation" of Jerusalem)
- 30 March (referred to by Israeli Arabs as "Land Day," it features protests against alleged expropriation of Arab property)
- 7 May (Israeli independence day)
- 31 May (the annual pilgrimage in Mecca begins)
- 5 June (the beginning of the 1967 Six Day War between Israel and her Arab neighbors)
- 4 July (U.S. Independence Day)
- 31 December–1 January (New Year's Day)

# Attack indicator #7: Triggers that propel a group to launch attacks in a revenge mode as quickly as possible ahead of a previous timeline

A spectrum of triggers propels terrorist groups to hasten the timing of terrorist attacks, usually resulting from sudden developments, such as a severe military setback. For example, al-Qaeda's conspiracy for the 11 September attacks began some two years prior to the attacks, but 12 September may have served as a trigger for the attacks to occur on the previous day.

New and devastating al-Qaeda attacks are likely to be triggered in response to its recent military defeats, particularly in Afghanistan, the detention of their captured operatives in centers at Guantanamo Bay and other areas, the overthrow of their previous state sponsors in Afghanistan and Iraq, and other factors.

### Conclusions

The 11 September attacks and follow-on operations are part of al-Qaeda's asymmetric warfare against the United States and its allies, in which small, fanatically dedicated teams are employed to inflict maximum psychological and physical damage on their much more powerful adversaries.

Terrorist attacks by groups such as al-Qaeda are intended to be catastrophic in terms of human and physical damage in order to punish and send a strong political message to the targeted adversary and to the group's constituents that the group is a world-class destroyer and political force to be reckoned with. In response, the United States, Britain, and their allies have greatly upgraded their situational intelligence, awareness, and defensive, preemptive, and deterrence postures.

Failing to anticipate the 11 September horrific attacks represented more than a failure of intelligence—it was a failure of imagination. Previously, such attacks were viewed as too grandiose and farfetched to be taken serious by intelligence and law enforcement authorities. Now these attacks, the attacks that have been thwarted, and other plots are perceived as likely blueprints for future catastrophic terrorist operations against the United States and its allies. Security and risk assessment professionals must always adopt proactive measures to anticipate, defend against, and preempt new types of terrorist threats. Moreover, one should not expect past trends to necessarily reveal future attack patterns because terrorists, especially al-Qaeda planners, always seek to exploit new vulnerabilities and new and innovative modes of warfare in order to evade detection and inflict maximum damage. Therefore, to avert catastrophic attacks that previously were considered beyond the imagination of those responsible for security, we need to begin thinking like the terrorist enemy-always anticipating and preparing to counteract new types of attacks and targeting potentialities. Continuous red-teaming is required, using outside-the-box threat and risk assessments and the most advanced (yet userfriendly) computerized predictive analytic tool kits. Such red-teaming must focus on multidimensional, not unidimensional, baskets of potential threats. Above all, emphasis must be placed on intelligence tracking of suspected terrorist networks, cells, and operatives; detection; and, above all, preemption during the earliest possible pre-attack incubatory phases.

Within this context, this threat assessment is intended to provide some of the initial conceptual means to anticipate and prevent catastrophic terrorist attacks, such as those that occurred on 11 September, from occurring again.

Joshua Sinai is a senior policy analyst in the Intelligence Division at ANSER, in Shirlington, VA. He is a specialist on international strategic and security issues; his professional work focuses on assessing terrorism in all its dimensions—the origins of terrorism, terrorist group profiles, developing indications and warning methodologies to forecast terrorist warfare (particularly the paths, links, and processes involved in the transition by terrorist groups from conventional to chemical, biological, radiological, nuclear, and cyber-warfare) and new approaches for governments to resolve terrorist insurgencies. Among his recent publications is a handbook, coauthored with his ANSER colleague Lt. Colonel Jeffrey Adams (U.S. Army, retired), Protecting Schools and Universities from Terrorism: A Guide for Administrators and Teachers, published in September 2003 by the American Society for Industrial Security. Joshua Sinai obtained his M.A. and Ph.D. from the Political Science Department at Columbia University.

## Piracy's Emerging Market: The Gulf of Guinea

## **By David Rider**

Source: http://gcaptain.com/piracys-emerging-market-gulf?29024

Despite the best efforts of the world's navies and EU NAVFOR in particular, piracy in the Indian Ocean/Gulf of Aden and Red Sea areas shows no sign of abating. Quite the contrary, according to a report released by the International Maritime Bureau's Piracy Reporting Centre in July this year. Of the incidents reported, over sixty per centre

were conducted by pirate gangs operating off the coast of Somalia and Arabian Sea. Indeed, the attacks were becoming more violent and pirates were taking much greater risks, the IMB stated.

The success of Somali pirates has not gone unnoticed by criminals in other parts of the African continent. Since May this been vear. there have increasing reports of pirate attacks in the Gulf of Guinea (GoG) and off the coast of West Africa. The incidents prompted the International Maritime Bureau's Piracy Reporting

Centre to issue a specific warning in June, citing eight attacks off Cotonou, Benin. Since then, the number of attacks has increased



significantly, although it's virtually impossible to accurately gauge the amount of pirate activity due to insufficient reporting from the region. One security analyst told Reuters that, "In Nigeria it is estimated that approximately 60 percent of pirate attacks go unreported"\*. The Gulf of Guinea is regarded as an important, emerging trade hub, spanning a

dozen countries from the tip of Northwest Africa to Angola in the South. It is a valuable source of oil, and pirates in the region are currently targeting diesel and oil tankers in particular.

According to a Reuters report\*, the Gulf of Guinea produces more than 3 million barrels of oil a day, equivalent to 4% of the global total. This oil is ultimately destined for Europe and



the USA, while some sources suggest that the USA will be receiving up to 25% of its oil supplies from the region by 2015.

With so much potentially at stake it is perhaps remarkable that little is being done on the international stage to combat piracy in the region. Local coastal defences are seen as weak, while the coastline itself is craggy and offers a variety of hiding places for potential attackers. Although thus far, only 27 or so attacks on vessels in the area have been reported by the IMB, the actual number incidents may be far higher, thanks primarily to the definition of 'piracy'.

Somali pirates operate a 'blue ocean' form of piracy, attacking vessels in international waters, which in turn means their crimes are legally recognised as "acts of piracy". The attacks in the Gulf of Guinea and off the coast of Nigeria occur in national or coastal waters, and therefore do not legally gualify as

"acts of piracy". Semantics aside, if armed men board your vessel and threaten your crew and cargo, it is hard to not call it an act of piracy. However, the law is the law.

At its most basic, piracy off the coast of Somalia can be seen as having a clear root in economics and the inevitable outcome of a failed nation state dating back 20 years. Piracy or, more correctly, criminal attacks upon vessels in the Gulf of Guinea region is simply that: maritime banditry in an area insufficiently protected by the world's navies. Intelligence sources on the ground are now seemingly acknowledging that the attacks in West Africa are very different in tone to their Somali counterparts. A report carried by the Associated Press quoted Bergen Risk Solutions, a Norway-based consultancy:

"Our investigations indicate that the organised group responsible is based in Nigeria and has high-level patronage in that country," it said, with prominent Nigerians having often been accused of involvement in the lucrative black market for oil and fuel. This cargo, Bergen suggests, has been sold in: "several West African ports, possibly including Abidjan in Cote d'Ivoire and Port Gentil in Gabon."

What the experts cannot say with any certainty, however, is why there has been such a surge in attacks in recent months. For instance, the international community has not seen a significant, proportionate fall in such incidents in Nigeria. With no international naval presence at the ready, it falls upon local agencies, such as the Benin Navy, to provide assistance. It has further been suggested that a number of shipping companies won't even call them in, for fear of increasing their insurance premiums. A report on businessday.co.za suggested that, 'insurance items due to piracy have doubled the costs of transporting goods past the Horn of Africa.' and there is no reason to believe that West Africa and the GoG should be any different in terms of insurance risk.

In response to the recent spate of activity, Bloomberg carried a report on August 5, stating that The Joint War Committee, which represents Lloyd's of London underwriters and other insurers, extended a war-risk zone for Nigeria, Africa's largest oil producer, and included waters off neighbouring Benin and listed the areas as higher-risk for shipping. The Nigerian risk zone now extends to 200 nautical miles (230 miles) offshore.

While the entire region is experiencing significant mineral wealth, it falls upon governments to ensure that this wealth is redistributed amongst the population or, to quote Reuters, "...the temptation to take a slice of the goods passing under their noses on the way to the richer world may prove irresistible for some."

It would seem clear that the world's governments, and particularly those countries whose energy usage relies upon imports from the area, could make a significant difference to piracy in this region. At present, the area to police is significantly smaller than that in the Gulf of Aden/Indian Ocean, which EU NAVFOR vessels regularly patrol, but the level of violence being used by pirates in their attacks in the GoG region is causing deep concern amongst international bodies such as the IMB. A concerted effort by the world's navies, in league with countries such as Nigeria, Cameroon and Benin could nip the problem in the bud, long before it escalates to proportions rivalling Somalia and the Gulf of Aden.

On August 5th, the International Maritime Organization (IMO) announced that plans had been tabled for maritime administrations in Togo, Republic of Benin and Nigeria to meet with relevant stakeholders to deliberate on ways of enhancing maritime safety in the region. A spokesperson for Nigerian Maritime Administration and Safety Agency (NIMASA) Lami Tumaka, stated that the Regional Maritime Awareness Capability Centre (RMAC) is equipped with the Automatic Identification System (AIS), Radar and video cameras.

The spokesperson said that the AIS identifies all vessels with the AIS transponders onboard, while those without the AIS are tracked with Radar while video cameras provide live pictures of all vessels along the Nigerian coastal waters. While the statement may reassure some ship owners, it is also true that many vessels turn their AIS transponders off to reduce the threat of attack from pirates in the Indian Ocean\*, and there is no reason to expect vessels in fear of attack by bandits in the GoG will behave differently.

An immediate solution to the problems being experienced by seafarers in the area would not appear to be on the horizon. This, however, is a work in progress. In the meantime, the job of securing cargoes, crews and corporate reputations will likely fall upon the private security provider, meaning insurance discounts and a significant sense of relief in both boardrooms and bridges.

David Rider is with Neptune Maritime Security founded by decorated, former members of Her Majesty's elite Special Boat Service (SBS) and supported by a team of international maritime legal experts, Neptune Maritime Security offers the kind of capabilities only the world's most elite commercial maritime security specialist can provide. With over 30 years of experience in the field of

amphibious counter-terrorism, Neptune Maritime Security's team of highly trained, highly motivated specialists are supremely qualified in the area that concerns shipping companies most: safeguarding crew, cargo and corporate reputations

## How Jihad Influenced the Norway Massacre

## By Raymond Ibrahim

Source: http://www.meforum.org/3007/norway-massacre-jihad

In his manifesto, Anders Breivik, the perpetrator of the Norway massacre, in which 80 people were killed and many wounded, mentioned the Crusades and aspects of it as they had been an inspirational factor to him. Predictably, Western elites—especially through the mainstream media—have begun a new round of moral, cultural, and historical relativism, some even conflating the terrorist with former President Bush, who once used the word "crusade."

The fact is, there are important parallels between the Crusades and Breivik's actions but hardly the way portrayed by the media. Ironically, this terrorist attack, like the historic Crusades, was influenced by the doctrine of jihad.

While many are aware that historically the Crusades were a retaliation to centuries of Muslim aggression (see Rodney Stark's God's Battalions: The Case for the Crusades), few are aware that the idea of Christian "holy war"—notably the use of violence in the name of Christianity and the notion that Crusaders who die are martyrs forgiven their sins—finds its ideological origins in Muslim jihad.

As historian Bernard Lewis puts it, "Even the Christian crusade, often compared with the Muslim jihad, was itself a delayed and limited response to the jihad and in part also an imitation." How? The popes offered

forgiveness for sins to those who fought in defense of the holy Church of God and the Christian religion and polity, and eternal life for those fighting the infidel. These ideas ... clearly reflect the Muslim notion of jihad, and are precursors of the Western Christian Crusade.

Still, Lewis makes clear some fundamental differences:

But unlike the jihad, it [the Crusade] was concerned primarily with the defense or reconquest of threatened or lost Christian territory. ... The Muslim jihad, in contrast, was perceived as unlimited, as a religious obligation that would continue until all the world had either adopted the Muslim faith or submitted to Muslim rule. ... The object of jihad is to bring the whole world under Islamic law.

If the Crusades arguably find their ideological origins in jihad, so too does much of modern day terrorism. The medieval Hashashin archetypal terrorists who gave us the word "assassin"—were, for example, a Muslim sect that pioneered the use of fear and terrorism for political gain during the Crusader era, around the eleventh-thirteenth centuries.

Because much of this background is missed by the media, more ironies abound. Many point, for instance, to Breivik's fascination with the Knights Templar, a Crusading order, as proof that he was motivated by the Crusades. Yet, as one AP report indicates, "The Knights Templar was a medieval order created to protect Christian pilgrims in the Holy Land after the First Crusade in the 11th century."

How exactly a military order devoted to protecting Christians inspired someone to kill innocent children in Norway is left unanswered. As one historian put it, the original Knights Templar, a "very devout people," would be "horrified" to find themselves compared to Breivik.

Even more ironic, the Knights and Crusaders in general were frequently on the receiving end of the Assassins' terror; far from being inspirations for terrorism, they bore the brunt of one of the earliest manifestations of Islamic terrorism.

In reality, Breivik's actions are more inspired by the Jihad than by the Crusades, by the Assassins rather than the Templars, and by al-Qaeda—"which he cherishes great admiration for"—than the IRA. As CNN's Fareed Zakaria correctly asserts that in Breivik's view, "the Knights Templar resembles nothing as much as al Qaeda."

The parallels are evident: Medieval Europe, in an effort to retaliate against an expansionist Islam, articulated a means influenced by jihad, or "holy war": the Crusades. Today, modern Europeans like Breivik, in an effort to retaliate against an expansionist Islam, have articulated a means influenced by al-Qaeda: jihadi-style terrorism. Some may argue that there are non-Muslim terror groups from which Breivik can draw inspiration. Even so, in a globalized world where Islam has by far the lion's share of terrorism—where nonstop images of jihadi terror have metastasized in the media, and thus the culture—it is not hard to see from where Breivik got his inspiration.

Raymond Ibrahim, a widely published Islam-specialist, is a Shillman Fellow at the David Horowitz Freedom Center and an Associate Fellow at the Middle East Forum.

## Fort Hood Plots: Answering the Call of Individual Jihad

#### By Clare M. Lopez

Source: http://www.radicalislam.org/content/fthood-jihad

"Muslims are being commanded...to strike out against the U.S, Israel, and "corrupt" Muslim rulers and take up the cause of jihad as an



#### individual responsibility."

The recent arrest of Pfc. Naser Jason Abdo for plotting to attack Fort Hood should be a real wake-up call to all Americans. As we know, Pfc. Abdo is the second Muslim member of the U.S. Armed Forces to target Ft. Hood; Major Nidal Hassan, tragically, was not stopped before he opened fire on his fellow soldiers at Ft. Hood in November 2009, killing 13.

The lessons to be learned from the actions of these two men are, or should be, plainly visible for all of us to see. Both of them announced their violent intentions openly and clearly long before they moved to actually carry out their threats. And both of them grounded their beliefs and their attack plans firmly on citations from the Qur'an.

Maj. Hasan told his colleagues that he considered himself "a Muslim first and an American second." He also gave a graphic Power-Point presentation ("The Koranic World View as it Relates to Muslims in the U.S.

Military") on his jihadist beliefs many times in front of U.S. military audiences. In this presentation, Maj. Hasan quoted the

Qur'an with verses on fighting the infidel and included many slides about the rewards of Paradise for those who fight and kill and die in the way of Allah.

He also foreshadowed the later actions of Pfc. Abdo when he concluded his Power-Point with this warning to the U.S. military:

"[The] Department of Defense should allow Muslim soldiers the option of being released as 'conscientious objectors' to increase troop morale and decrease adverse events."

#### [Hasan's whole slide show can be seen here.]

So, it can be seen from these two examples that the jihadist leaderships of both al-Qa'eda and the Muslim Brotherhood have called for Muslims everywhere to turn the page as it were from the more moderate Meccan period to the more violent Medinan period. Muslims are being commanded by both of them to strike out against the U.S, Israel, and "corrupt" Muslim rulers and take up the cause of jihad as an individual responsibility.

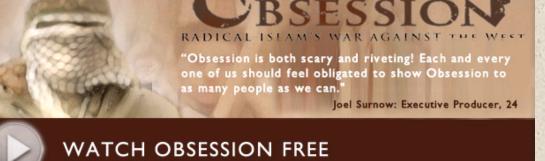
We should note that those Muslims who obey and follow the call of jihad as stipulated in the sharia (Islamic law) do not hide their intentions but rather speak out openly about them - for this, too, is a command of Islamic law, that warning be given before an attack. It is for us to heed the warnings, and as our national security forces did in the case of Pfc. Abdo, take steps to stop their attack plans before they can be carried out.



Clare M. Lopez, a senior fellow at the Clarion Fund, is a strategic policy and intelligence expert with a focus on Middle East, national defense, and counterterrorism issues.

## **Obsession - The movie**

30,000,000 HAVE ALREADY SEEN OBSESSION. HAVE YOU?



Using images from Arab TV, rarely seen in the West, Obsession reveals an 'insider's view' of the hatred the Radicals are teaching domination.

#### Bin Laden movie has King worried

Source: http://www.homelandsecuritynewswire.com/bin-laden-movie-has-king-worried

Representative King, the chairman of the House Homeland Security Committee, requested the Pentagon and the CIA to determine whether the Obama administration had leaked any classified information about the raid to Kathryn Bigelow and Mark Boal, the creative team behind the Oscar-winning movie "The Hurt Locker".



Director Katheryn Bigelow // Source: womenandhollywood.com

The clandestine Navy SEAL raid that killed Osama bin Laden is a compelling story that movie makers have been clamoring to try to obtain more details, which has Representative Pete King (R – New York) worried.



On Wednesday, Representative King, the chairman of the House Homeland Security Committee, requested the Pentagon and the CIA to determine if the Obama administration had leaked any classified information about the raid to Kathryn Bigelow and Mark Boal, the

428

creative team behind the Oscar-winning movie "The Hurt Locker."

The two are currently working on making a move about the military's Special Forces who have sought for to capture or kill bin Laden for the past decade. "The Administration's first duty in declassifying material is to provide full reporting to Congress and the American people in an effort to build public trust through transparency of government," Representative King said in a statement. "In contrast, this alleged collaboration belies a desire of transparency in favor of a cinematographic view of history."

Tommy Vietor, a spokesman for the National Security Council, said King's claims were "ridiculous." "When people working on articles, books, documentaries or movies that involve the president ask to speak to administration officials, we do our best to accommodate them to make sure the facts are correct. That's hardly a novel approach to the media," Vietor said. "We do not discuss classified information. I'd hope that as we face a continued threat from terrorism, the House Committee on Homeland Security would have more important topics to discuss."

King's comments come after a series of several high-profile reports detailing the raid on bin Laden. Most recently, the New Yorker published a highly detailed account of the raid. The military and intelligence officials have tried to keep details of the raid confidential, but King says that the administration has not had a good

record of maintaining confidentiality. "To find there's a movie coming out and there's been cooperation with Hollywood ... considering the track record of the last 90 days, I'm concerned," King said.

Work on the bin Laden movie was scheduled to begin later this summer and is expected to hit theaters before the November 2012 elections.



# 10 Years and a Diagnosis Later, 9/11 Demons Haunt Thousands

#### By Anemona Hartocollis

Source:http://www.nytimes.com/2011/08/10/nyregion/post-traumatic-stress-disorder-from-911still-haunts.html?\_r=1

Dr. Margaret Dessau heard the crash of a plane into the World Trade Center from her apartment; the things she saw out her window changed her life.



In the safety of her therapist's office in late 2001, Dr. Margaret Dessau made a tape reliving what it was like to look out her living room window after she heard the boom of a hijacked plane eight blocks away.

Running naked from her bath, she saw pigeons and paper flying through the air. "It's kind of beautiful in a way," she recalls on the recording she made and listened to over and over as part of her treatment. "There's these silver pieces

just floating in the air." Her gaze met the hole in the tower. "The flames get worse, and then I start seeing all these people hanging out there. The guy with this white towel, and he's waving it." He jumps. Children at a nearby school scream. "How are you feeling?" her therapist, David Bricker, is heard asking on the tape. "I start crying," she replies. Dr. Dessau's husband yells at her, "Stop looking at it, stop looking at it." But, she says, "I can't tear myself away from it."

One measure of the psychological impact of 9/11 is this: At least 10,000 firefighters, police officers and civilians exposed to the terrorist attack on the World Trade Center have been found to have posttraumatic stress disorder, and in a kind of mass grieving, many of them have yet to recover, according to figures compiled by New York City's three 9/11 health programs.

In interviews over the last several

months, Dr. Dessau and others revealed a wide-ranging but consistent body of symptoms. They cannot sleep. They replay the disaster in their minds, or in their nightmares. They have trouble concentrating. They are jittery and overreact to alarms or loud noises. They feel helpless, hopeless, guilty and cut off from the people who are close to them. They avoid anything that reminds them of that terrible day. Millions of dollars will be spent treating them over the next few years through the James Zadroga 9/11 Health and Compensation Act, passed by Congress in December, which provides \$4.3 billion to compensate and treat people with 9/11-related illnesses.

Some are emergency responders and others who vainly searched the debris for survivors. But some were residents, commuters and office workers caught in the dust cloud. And others were passive witnesses with no direct connection to the attack other than proximity. Because of lingering questions about the bounds of the PTSD diagnosis, which is only three decades old, people with mental problems are eligible only for treatment assistance, whereas people with physical ailments, in most cases breathing difficulties, qualify for both treatment and compensation. And money available to treat patients with the



stress disorder might decline if the government concludes there is a link between certain cancers and 9/11, which would give cancer patients access to the same pool of money. Doctors are expecting a surge in PTSD patients with the coming 10th anniversary, as they have on each Sept. 11.

Charles Figley, professor of disaster mental health at Tulane University's School of Social Work and a former Marine, advanced the concept of PTSD in a 1978 book on Vietnam War veterans. He said one reason the trauma had been so hard to shake was that it ripped at the most ordinary fabric of daily life.

The landmark is not a distant hill in Afghanistan that one will never see again. "It's the places you see every day, where you proposed to your wife, where you remember getting the news that you got promoted, where your young children played," Dr. Figley said.

"You go into a combat zone and then you leave," he added. "You don't leave home. You return all the time."

#### Ancient but Evolving Illness

"The Iliad" described warriors consumed by feelings of guilt, rage and grief. World War I had "shell shock," and World War II had "combat fatigue." PTSD has been found in survivors of Nazi concentration camps, fires and railway accidents. But it was not until 1980, after the Vietnam War, that post-traumatic stress disorder was added to the psychiatric bible, the Diagnostic and Statistical Manual of Mental Disorders.

The current manual, the DSM-IV, says PTSD can develop through a range of exposures to death or injury: direct personal involvement, witnessing it or, if it concerns someone close, just learning about it. Almost no other psychiatric diagnosis has generated as much controversy, according to Dr. Robert L. Spitzer, a retired psychiatry professor from Columbia University and an expert in mental disorder classifications. It has become so vague that stressed-out college students and people who watched horror movies could fit the profile, he and two other experts wrote in a professional journal article.

"It's a way of saying something terrible has happened to me and I've been damaged in some way, but that doesn't necessarily mean it's an illness," Dr. Spitzer, who advocates tightening the criteria, said in an interview.

Some experts have been skeptical of studies finding that people suffered the disorder from watching television coverage of the Sept. 11 attacks. (Congress effectively excluded TV watchers from its treatment program by requiring that victims had lived or worked within certain geographic boundaries.)

Amy Cushing-Savvi, a social worker at Mount Sinai Medical Center, which runs the largest program, said a frequent topic at staff meetings was, "What's 9/11 and what isn't?" — in other words, the exquisitely vexing question of how to separate the effects of 9/11 from the traumas of everyday life.

"Taxpayers could end up paying for psychotherapy for Woody Allen and half of Manhattan," Theodore H. Frank, a fellow at the Manhattan Institute, testified before the House Judiciary Committee in April 2008, when he was a fellow at the conservative American Enterprise Institute. Ultimately, federal financing for PTSD treatment was limited to firefighters, police officers, employees of the New York City medical examiner's office who handled body parts, and other rescue, recovery, cleanup and support workers at ground zero, on the barges that carried debris and at the Staten Island landfill where the twin towers rubble was entombed; responders at the attack sites at the Pentagon and Shanksville, Pa.; and people exposed to 9/11 dust when the buildings collapsed or who lived, worked or attended school south of Houston Street in Manhattan and in parts of Downtown Brooklyn where the dust may have extended.

Family members of New York City firefighters who died are covered as a continuation of an existing Fire Department counseling program, but family members of other victims are not. Representative Carolyn B. Maloney, Democrat of New York and the lead sponsor of the Zadroga Act in the House, said that since victims' families had been covered by the original 9/11 compensation fund, which paid an average of \$2.1 million to each family, the goal was to look after others who suffered. "We were focusing on covering the people who did not die on 9/11, but those who were dying and sick because of 9/11," she said.

The law was named after a New York police detective who took part in the rescue efforts and later developed breathing complications. The cause of his death in 2006 became a source of debate.

Dr. John Howard, who oversees 9/11 programs as the director of the National Institute for Occupational Safety and Health, said in an interview that he was willing to give people the benefit of the doubt about PTSD, even if they had other stresses. "Collapsing 220 stories of a lot of material in one of the most densely populated cities in the world is a very unique event," Dr. Howard said. "In mental health you have to treat the whole person, and you can't really separate out some of these other influences, personal stressors, economic issues. People are living their lives." "It sounds squishy," he added, "but it really isn't squishy." **Her World Collapses** 

For Dr. Dessau, who is now 64, listening to the tapes she made during therapy conquered her fears for a while, "like cod liver oil," she said. But in 2009, her sense of tragedy was compounded when her husband, Bob Wheeler,

died just four months after being told he had lung cancer.

Dr. Dessau, a youthful, athletic blonde with blue-rimmed green eyes, still lives in the same airy loft on Greenwich Street, decorated with souvenirs of 35 years of travel with Mr. Wheeler — shells arranged in bowls, a childsize winged Hermes, a many-limb stone goddess, a terra cotta Chinese statue of a man. There is also a green plastic box containing her husband's ashes.

Mr. Wheeler, a lawyer, never smoked, so Dr. Dessau, a pulmonologist, suspected that his disease was related to his exposure to the falling buildings. His quick death revived the sense of helplessness she had felt watching people jump from the towers. "As a doctor you always think you can fix it," she said.

She lost 20 pounds. She stopped seeing friends. She was "on red alert," sure that something bad would happen at any second. She avoids looking at the skyline outside her

to cover her out-of-pocket expenses, but she prefers her own therapist.

She sees 9/11 and her husband's death as part of a continuum, along with her parents' escape from Nazi Germany, the suicide of a close relative and her time preparing bandages as a student in Israel during the 1967 Arab-Israeli war. "It confirms my sense of pessimism," she said. "It's corroboration of the evil of human beings."

That sense of 9/11 as a catalyst is common. In June, Stanley Mieses, 58, a freelance writer and editor, lined up with other psychiatric patients at the city-run Elmhurst Hospital Center under a sign that said, as if atient Registrati n. testing his sanity: New

During a screening, he circled the maximum, "nearly every day," to a question about how often he had been "feeling bad about yourself — or that you are a failure or have let yourself or your family down."

Mr. Mieses, who is receiving treatment under



window, though her reaction is not as bad since buildings have begun to fill in the space where the World Trade Center used to be.

A city fund set up before the Zadroga Act was enacted provided \$9,000 to Dr. Dessau to cover therapy expenses not handled by her insurance. The city sent a letter encouraging her to seek further treatment through a public program that would allow the Zadroga money the Zadroga Act, lived six and a half blocks from the trade center and watched the buildings collapse. The police evacuated him, but he returned every few days to feed his cats. "Dead people were blowing into my apartment off the windowsills," he said, remembering the ash, "because the landlord was too cheap to clean it."

For a while he sublimated his anxiety, filing reports for NPR from his stunded

neighborhood. But in short order, his mother, a World War II German refugee with what he said were her own PTSD issues, died; his girlfriend left him; work dried up; and he was forced by his finances to move to Jackson Heights, Queens.

These psychic blows led, he said, to "a change in my attitude, a change in my - 1 don't know

3,000 of the 10,000 patients were treated by the public hospitals, whose statistics do not differentiate among PTSD, depression and anxiety. The Zadroga program covers all three, along with panic disorder, substance abuse and a few other conditions.

Extrapolating from a registry of people exposed to the attack, the city's health department has



## - joie de vivre."

His pulmonologist at Elmhurst says his shortness of breath could be from the dust, or the 20 years he smoked. The origins of his mental wounds are also ambiguous. "I tend to think of 9/11 as the trapdoor that opened up," Mr. Mieses said. "Whatever else I'm doing past that, is climbing back up."

#### A Number Unknown

It is impossible to say how many people have 9/11-related PTSD. The city's three official programs do not count people, like Dr. Dessau, who use private physicians — or those who have not been treated at all.

According to figures provided by the programs, run by the Fire Department, which treats its own employees; a consortium of hospitals led by Mount Sinai Medical Center, which treats police officers and other rescue and recovery workers; and the city's public hospital system, which treats civilians, at least 10,000 patients have met the criteria over the last decade, and at least 3,600 of them still have symptoms. But even those rounded numbers have an asterisk: estimated that 61,000 of the 409,000 in the disaster area experienced "probable" PTSD within six years of 9/11. But these numbers were produced by institutions and a city government with two main goals: to make as many people as possible feel better, and to try to persuade Congress to provide a steady stream of treatment money. The city's 9/11 health programs have created a huge intake system that screens every patient for mental as well as physical illness, and the public hospitals reached out to New Yorkers with subway advertisements that said: "Lived there? Worked there? You deserve care."

No one can say exactly how many people were exposed to the attack, and how many will eventually become physically or mentally sick. The federal government will allow the Mount Sinai and public hospitals programs to grow by 25,000 patients each over the next five years. It will be up to each program to decide who qualifies for treatment, but they will have to use uniform criteria approved by the government. Therapy can cost \$135 for a 45-minute week

434

session with a psychologist or \$165 with a psychiatrist.

If the government finds a link between 9/11 dust and cancer, there is some concern about

running out of money, though the Zadroga fund is to be a secondary payment source, covering what insurance and workers' compensation do not.

Dr. Howard, the federal 9/11 health administrator, said the government "will treat people as they come in to the extent possible."

#### Alarms, Over and Over

Patients at Mount Sinai find a busy warren of rooms where they are divided into three categories: green (no further assessment needed), yellow (potentially symptomatic) and red (symptoms so severe that they might be

suicidal). They begin the screening at home, filling out an 11-page questionnaire that asks about their level of energy, how often they feel "calm and peaceful," and about recent life experiences like losing a job or having a relationship break up. In a section called "Reminders of 9/11," they are asked whether they have recurring thoughts of the disaster and whether they feel emotionally cut off from those close to them.

In an interview with a clinician, they are asked whether "you often believe it would be better if you were dead," "you feel worthless" or "you feel guilty even though you didn't deserve to feel that way."

If they have PTSD, patients are usually given a combination of psychotherapy and pills, typically antidepressants, and sometimes sleeping pills. Many patients are encouraged to make recordings of their memories, as Dr. Dessau did, or to write about them until the memories lose their power. This is called exposure therapy.

Alain Delaquérière contributed research.



Once a month, Earl Holland drives from his home in Flatlands, Brooklyn, to Mount Sinai for meditation classes. "You get in a room, the chimes are going, it's fantastic," Mr. Holland

> said. He also takes Wellbutrin. an antidepressant. and Ambien, a sleeping pill. Mr. Holland, 48, was a paramedic supervisor for North Shore-Long Island Jewish Health System when he responded to the disaster after the second tower collapsed. In his dreams, he still hears the alarms — attached to each firefighter's mask - that signal that a firefighter has stopped moving. "There were hundreds of alarms going off," he said, grabbing a tissue to wipe away the tears as he sat in his kitchen,

remembering.

"I kept the list" of the missing, he said.

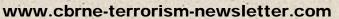
Two months after the attacks, he responded to the crash of American Airlines Flight 587 in Belle Harbor, Queens.

He started shutting himself in his bedroom, refusing to talk to his wife and children. He spent hours staring at photographs of the burning rubble and had flashbacks of responding to murders during the 1980s crack epidemic.

"Toward the end, I didn't want to do my calls," he said. "It was like, enough. I actually thought it was burnout, but it wasn't burnout."

Mr. Holland's diagnosis of PTSD was made in 2009 through a Mount Sinai outreach program, and his costs will be covered by the Zadroga Act.

He has recovered enough that he hopes to return to work, but not on the front lines. "I don't know if I'll go to the memorial any time soon," he said. "I look at that kind of as closure, if I'm able to do that."



# Indonesia's "Ghost Birds" Tackle Islamist Terrorists: A Profile of Densus 88

**By Jacob Zenn** Source: http://www.jamestown.org

After the 2002 Bali bombings, Indonesia

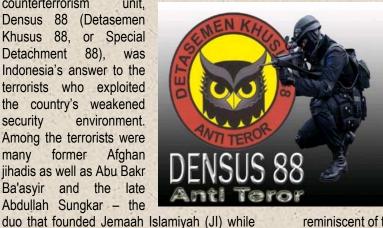
Densus 88 is an all-Indonesian force with 400-500 personnel led by Brigadier General M.



recognized that the main threat to national security came from regional terrorist networks whose leaders returned to Indonesia after Suharto fell from power in 1998. An elite

in exile in Malaysia between 1985 and 1998.

counterterrorism unit. Densus 88 (Detasemen Khusus 88, or Special Detachment 88), was Indonesia's answer to the terrorists who exploited the country's weakened security environment. Among the terrorists were many former Afghan jihadis as well as Abu Bakr Ba'asyir and the late Abdullah Sungkar - the



Syafii. The unit is equipped primarily with U.S.made Colt M4 carbines (which were effectively employed in the siege of Dr. Azahari Husin's hideout in Batu in 2005), Armalite AR-10 sniper

rifles. Reminaton 870 shotguns, and Austrian-made Steyr AUG assault rifles. Training is provided by American security services and Australian Special There is some Forces. debate about the origin of the "88" designation, though most likely it represents the number of Australians who died in the Bali bombings and the image "88" is

reminiscent of two handcuffs [1].





From 1999 until 2002 - the year Densus 88 was created - JI attacks included a bombing at the Istiglal Mosque in Jakarta, an assassination attempt on the Philippine ambassador in Jakarta, and church bombings in Jakarta, Sumatra, Lombok, Java, and Batam. The JIaffiliated Lashkar Jihad also sent thousands of students from five JI-linked pesantren (Islamic boarding schools) in Java to the Moluccas, Sulawesi, and Papua to fight against Christians (see Terrorism Monitor, May 5, 2005). JI's terror offensive culminated with the bombings at Kuta Beach in Bali, which killed eight Americans, 88 Australians and more than 100 others.

Following the Bali attack, the U.S. State Department's Diplomatic Security Services identified Indonesia as a frontline in the global war on terror and provided funds under the Anti-Terror Assistance Program to establish

Densus 88 and pay for salaries, weapons, highlevel training in communications interception. close combat warfare and forensic sciences, and surveillance and intelligence gathering analysis. The and budget included start-up costs of \$130 million in the second half of 2003. followed by annual funding which increased from \$1.3 million in 2004. to more than \$13 million in 2005, to more than \$40 million in 2006 [2].

Currently, Australia funds Densus 88 with \$16 million annually and 2004 Australia in pledged \$35 million over five years to build a training center at the Jakarta Centre for Law Enforcement Cooperation, where the Australian Federal runs Police (AFP) seminars for Densus 88. [3] In

November 2005.

Densus 88 turned the tide in Indonesia's war against JI. A Densus 88 sniper shot Dr. Azahari Husin, the JI mastermind behind the 2002 and 2005 Bali bombings and the JW Marriot and Australian Embassy bombings, during a raid on Husin's hideout in Batu, East Java. An accomplice set off a suicide explosive killing himself and a third man who had joined Husin in engaging the counterterrorism force in an intense gun battle. After Husin, Densus 88 eliminated JI's other top operatives in near succession:

> In 2007 Densus 88 captured Abu Duiana in Central Java with the help of U.S satellites operated by Australian Police which tracked his cellphone activites.(Tempo Interaktif [Jakarta], June 20, 2007; for a profile of Abu Dujana, see Terrorism Monitor, April 4, 2006).

- In 2009 Densus 88, acting on tips and surveillance, surrounded a house that Noordin Mohammed Top was renting in Solo. Noordin blew himself up along with his wife and two children to save himself from being killed or captured by Densus 88 (for a profile of Noordin Top, see *Terrorism Monitor*, July 25, 2006).
- In 2010, Densus 88 tracked down and killed Dulmatin, who had a \$10 million bounty on his head, in an internet café in Jakarta. Indonesian President Yudhoyono confirmed Dulamtin's death while giving a speech to the Australian Parliament (for a profile of Dulmatin, see *Terrorism Monitor*, July 9, 2006).
- In May 2011 Abu Bakr Ba'asyir received a 15-year sentence after his conviction for sponsoring a terrorist camp in Aceh that Densus 88 raided in 2010.

Densus 88's collaboration with the U.S. and Australia has not gone unnoticed by the terrorists it hunts down. Abu Bakar Ba'asyir

said during his trial that allegations of terrorism were "deliberately spread by God's enemy - the Zionists and their allies America and Australia, and followed by Densus 88" (The Age [Melbourne], February 23). Radical Islamic groups in the country, such as the Islamic Peoples' Forums (FUI) and Islamic Defenders Front (FPI), see Densus 88 as a U.S. and Australian-backed paramilitary unitthat systematically arrests and kills Islamic activists under the pretense of terrorism. They cite Densus 88's start-up and operational funding as proof (Jakarta Globe, August 31, 2010).

Densus 88 has also come under scrutiny from human rights groups because of its reputation for torture, especially when it comes to suppressing separatists, and its use of American and Australian wire-tapping technologies to track suspects. In 2007, Densus 88 tortured many of the 22 people responsible for unfurling the South Mouccan independence movement flag in front of President Susilo Bambang Yudhoyono during his visit to Ambon. In 2010, their leader died in prison three years into his 12-year sentence for treason after having been denied medical access for kidney problems he attributed to beatings and being forced to drink hot water infused with carbon paper (Sydney Morning Herald, September 13, 2010). In August 2010 Densus 88 allegedly tortured 12 Mouccan separatist suspects for a week, suffocating them with plastic bags, stabbing them with nails, and forcing them to eat raw chili peppers.

Densus 88's reputation was tainted again in October 2010 one month before President Obama's visit to Indonesia when a video showed Indonesian security forces pressing a stick smoldering from fire against a Papuan separatist suspect's genitals, a plastic bag wrapped around the suspect's head, and one officer holding a large knife next to the suspect as he pleads, "I'm just an ordinary civilian." [3] This was only months after the Obama administration announced it would resume aid to Kopassus in July 2010. Congress had prohibited relations with Kopassus in 1999 due to allegations that Kopassus aided militias in East Timor that carried committed human



Members of Densus 88, an elite anti-terrorist unit of the Indonesian police

#### rights abuses.

Cutting off funds to Densus 88 is still unlikely since Densus 88's record of more than 500 militant arrests and decapitating the JI leadership has drawn as much, if not more, international attention and praise. Since its last major attack in July 2009 – the bombings of the JW Marriot and Ritz-Carlton hotels in Jakarta, allegedly planned by Noordin – JI has not been able to orchestrate sophisticated large-scale attacks.



Although Densus 88 has dismantled and decapitated the JI network, small cells of former JI fighters and other separatist movements have attacked Ahmadiyah Muslims, churches, moderate mosques and various Islamic organizations to create religious divides in the normally tolerant country. [3] These terrorists have employed letter bombs, suicide-bombings, and drive-by shootings in their campaign, which typically targets Indonesians rather than Westerners.

A look at Densus 88's recent operations shows the effectiveness of Densus 88 in detecting new cells, connecting suspects from one cell to related cells and tracking down long-time terrorists:

 On June 9, Densus 88 arrested Heri Kuncoro, a brother-in-law of Dulmatin, and Sugeng Setiaji, in Central Java. Interrogation of Heri and Sugeng led to the arrest of two of the 18 suspects in police shootings in Palu, Sulawesi in May 2011 (Antara News [Jakarta], June 16).

 On June 10, acting on reports from local residents, Densus 88

found three bombs tied with yellow tape behind a church in Poso, Central Sulawesi (*Jakarta Post*, June 10).

On June 11, the police Muhammad arrested Sibghotulloh and Yuwardi East in Kalimantan Province. The pair supplied weapons from the Philippines that were used in drive-by shootings that killed two police officers in Palu,

Central Sulawesi, in May. They were also suspected of being involved in planning last April's suicide-bombing of the Adz Zikra mosque in Cirebon, West Java (Antara News, June 16; Reuters, June 15).

 On June 15, Densus 88 confiscated bomb components, detonators, and notes on bomb-making and arrested a terror suspect at a sports store in Pemalang, Central Java. The 42-year old suspect, Sudirman, was believed to have been involved in the 2002 and 2005 Bali bombings as Dulmatin's right-hand man (*Jakarta Post*, June 17, 2011).

 On July 19, Densus 88 arrested seven people in Yogyakarta and 5 people in Central Java allegedly linked with the network of Upik Lawanga (a.k.a. Taufik Bulaga). Lawanga was a student of Azahari Husin and is now JI's bomb making expert (*Tempo Interaktif*, July 20).

Densus 88 is living up to the local reputation of its emblem, the *burung hantu* ("ghost bird," or owl). Having come into its own since 2005, Densus 88 has turned JI into the prey, disrupted the terrorist infrastructure in Indonesia, and protected its citizens as well as the facilities and citizens of its American and Australian allies.

Densus 88's operational capabilities are



proven, but Densus 88's leadership still has to find a way to eliminate rogue members from the unit and abolish the heavy-handed tactics that provide a source of propaganda for Islamist and separatist groups as well as justification for unsympathetic members in the U.S. Congress and Australian parliament calling for a reduction or halt in funding.

#### Note:

 See "Indonesia's Elite Forces Detasemen 88," http://indonesiaeliteforces.tripod.com/id37.html
 See Muradi Clark, Densus 88 AT: "Peran dan Koordinasi Dalam Pemberantasan Terorisme di Indonesia" [Densus 88 AT: The Role and Coordination in Counter-Terrorism in Indonesia], May 12, 2009.

http://muradi.wordpress.com/2009/05/12/densus-88-at-peran-dan-koordinasi-dalam-pemberantasan-terorisme-di-indonesia/.

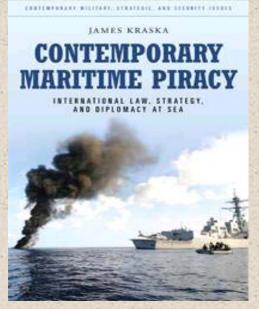
3. See http://video.ahrchk.net/AHRC-VID-012-2010-Indonesia.html

4. The Ahmadiyah are a Muslim movement founded in India by Mirza Ghulam Ahmad (1835–1908), who declared himself the expected Mahdi. The movement is considered unorthodox by orthodox Muslims and heretical by Salafists.

Jacob Zenn graduated from Georgetown Law as a Global Law Scholar in 2011 and works as an international security consultant. He is currently based in East Java, Indonesia.

## **Contemporary Maritime Piracy**

International Law, Strategy, and Diplomacy at Sea By James Kraska (Author) Source: http://www.bokklubben.no/SamboWeb/produkt.do?produktId=5915530



The threat of maritime piracy has exploded in the last decade, causing insurance costs to skyrocket and incurring losses estimated to be in the billions of dollars each year. Pirates operating off the Horn of Africa repeatedly disrupt the oil supply from the Persian Gulf as well as shipping traffic through the Suez Canal and the western Indian Ocean. The problem of piracy is a common topic of discussion within the shipping industry as well as among insurance companies, government officials, media, and academia. "Contemporary Maritime Piracy: International Law, Strategy, and Diplomacy at Sea" comprises three sections, the first of which contains chapters on historical and contemporary piracy, international law and diplomacy, and coalition strategies for combating future piracy. The second and third parts provide collections of historic profiles and relevant documents.

"James Kraska is a brilliant and forthright commentator on maritime security and legal issues relating to oceans governance. He brings to the subject an acute legal brain and clarity of exposition rare in both fields. These qualities are exemplified in this fine book in which he elucidates the detail surrounding emerging counter-piracy practices. It is a model exposition which will benefit anyone from the interested amateur to the pressured professional. It is a book that will never be far from my desk."

Martin M. Murphy, Visiting Fellow Corbett Centre for Maritime Policy Studies, King's College London and author of Somalia, the New Barbary? Piracy and Islam in the Horn of Africa

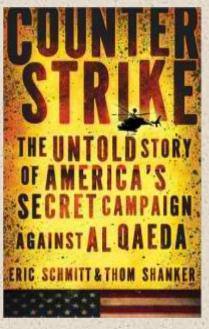
James Kraska, JSD, is Howard S. Levie Professor of Operational Law and Senior Associate in the Center for Irregular Warfare and Armed Group at the U.S. Naval War College, in Newport, RI. Kraska also serves as guest investigator at the Marine Policy Center, Woods Hole Oceanographic Institution and as senior fellow at the Foreign Policy Research Institute. A commander and judge advocate in the U.S. Navy, Kraska served as the Oceans Policy Adviser for the Director of Strategic Plans & Policy, Joint Chiefs of Staff, where he developed global counter-piracy policy for the U.S. armed forces and represented the Pentagon in counter-piracy policy at the National Security Council and the International Maritime Organization. Kraska earned a professional doctorate in law from Indiana University, Bloomington, IN; a research doctorate in law from the University of Virginia, Charlottesville, VA; and a master's degree in foreign affairs from the School of Politics & Economics at Claremont Colleges, Claremont, CA. His published works include Maritime Power and the Law of the Sea and numerous scholarly articles.



# Counterstrike: The Untold Story Of America's Secret Campaign Against Al Qaeda

Authors: Thom Shanker & Eric Schmitt

In the years following the 9/11 attacks, the United States waged a "war on terror" that sought to defeat Al Qaeda through brute force. But it soon became clear that this strategy was not working, and by 2005 the Pentagon began looking for a new way.



In Counterstrike, a Henry Holt and Company book, former CNAS Writers in Residence, Eric Schmitt and Thom Shanker of The New York Times, tell the story of how a group of analysts within the military, at spy agencies, and in law enforcement has fashioned an innovative and effective new strategy to fight terrorism, unbeknownst to most Americans and in sharp contrast to the cowboy slogans that characterized the U.S. government's public posture.

Eric Schmitt is a terrorism correspondent for The New York Times and has embedded with troops in Iraq, Somalia, and Pakistan. Schmitt has twice been a member of Times reporting teams that were awarded the Pulitzer Prize.

Thom Shanker, a Pentagon correspondent for The New York Times, routinely spends time embedded with troops in Iraq and Afghanistan. Shanker was formerly a foreign editor and correspondent for the Chicago Tribune, based in Moscow, Berlin, and Sarajevo.

#### Review

"A remarkable detective story by two of the nation's best reporters. With meticulous research and fine storytelling, Counterstrike reveals who, what, when, where, and why in describing the long campaign by the United States government to demolish Al Qaeda and ultimately to kill Osama bin Laden."--Rick Atkinson, Pulitzer Prize-winning author of An Army at Dawn

"Counterstrike lays bare the provocative new ideas that are driving the war on terrorism. Generals often talk about changing the hearts and minds of people in faraway lands, but Eric Schmitt and Thom Shanker reveal the importance of changing the hearts and minds of America's defense strategists. This is a groundbreaking intellectual history that is also a great read."--Jessica Stern, author of Terror in the Name of God: Why Religious Militants Kill "Eric Schmitt and Thom Shanker dig deep to tell the story of the covert campaign to defeat Al Qaeda, from the CIA to the Pentagon. Counterstrike is a richly reported work that is a seminal account of the battle between America and Al Qaeda since 9/11."--Peter Bergen, author of The Longest War: The Enduring Conflict Between America and Al-Qaeda

"Filled with amazing characters and details, Counterstrike traces the evolution of America's strategy for stopping the next attack. It's a fascinating story and a great read, too."--Dexter Filkins, author of The Forever War

"Counterstrike scores a direct hit. Eric Schmitt and Thom Shanker, two of America's most respected national security correspondents, provide pathbreaking reporting on and incisive analysis of the secret war against Al Qaeda after 9/11. This cogent history of America's elusive search for a strategy – essential reading for specialists and concerned citizens alike – should inform our national debate on how best to counter this most urgent threat."-- Lee H. Hamilton, former congressman and co-chair of the 9/11 Commission



"Eric Schmitt and Thom Shanker have written a brilliant and important account of America's battle with Al Qaeda. It is an exceptional work in that it truly addresses strategic issues and not just the tactical fight. There are critical insights and recommendations provided in this book that make it a must-read for all those who want to understand how we must deal with this complex threat."--General Anthony C. Zinni, USMC (retired)

## How to Hijack an Airplane in 3 Seconds

## By Abraham Tekippe

Source:http://www.theatlantic.com/national/archive/2011/08/how-to-hijack-an-airplane-in-3-seconds/243 631/

Ten years after 9/11, airline cockpits are vulnerable every time a pilot takes a bathroom break. So why isn't the FAA making secondary barriers a requirement?

One-one thousand. Two-one thousand. Three-one thousand.

And just like that, it can happen: From the front row of a passenger airplane, a group of hijackers leap from their seats and race toward the cockpit, leaving flight attendants, galley carts, and other improvisational means of defense in their wake. The reinforced cockpit door, opened just a few moments earlier to allow one of the pilots to use the lavatory, slams shut behind them, sealing off all hopes of regaining control of the aircraft.

All in a matter of three seconds.

It's a scenario the Federal Aviation Administration has been aware of for years and one that has prompted many in the airline industry to push for installed physical secondary barriers (IPSBs) -- retractable, fence-like devices set up between the cabin and the cockpit -- as well as more comprehensive, industry-wide security procedures on all passenger aircraft.

"We're in a race against time, frankly, because there is going to be another attack," said Capt. Ed Folsom, a United Airlines pilot who has played an active role in the development of the secondary barrier system since 2002. "I'm no rocket scientist, so if I can see the vulnerability, so can everyone else."

The primary concern: door transitions, or times when the cockpit door is opened and closed during a flight. Although most transitions are over before passengers even realize they're happening, Folsom and others, including Capt. Rob Powers, said they believe airplanes are not as secure as they can and should be during these brief exchanges. "Just like in medieval times, the castle is secure until you open the drawbridge," said Powers, a commercial airline pilot and former chairman of the Air Line Pilots Association's National Security Committee. "If you don't have



a moat or something else around to add a second layer of security, then you have some vulnerabilities. When the door's open, it's just a hole."

Post-9/11 FAA regulations do permit flight crews to open and close cockpit doors during flights, but only when it is necessary to do so. Typically, this means meeting pilots' physiological needs -- for example, lavatory use and food and beverage service -- though airline officials said pilots may need to exit the cockpit if mechanical problems arise during a flight.

Currently, each airline has its own FAAapproved procedures that specify how crews should go about opening and closing the cockpit door mid-flight. While the FAA doesn't specify how long or how many times the door can be opened per flight, FAA officials said it is assumed crews will do it as quickly and minimally as possible, usually for under five seconds.

But numerous passenger complaints, obtained from the Transportation Security Administration through a Freedom of Information Act request, suggest this isn't always the case.

On April 28, 2007, a passenger flying from. Dallas/Fort Worth International Airport to Sa Diego filed a complaint saying that the cockpit door was open for five minutes mid-flight, according to TSA records.

More recently, on May 3, 2010, a passenger flying between Columbus, Ohio, and St. Louis said the cockpit door was opened a minimum of five times during the flight.

"Once that door comes open, you're vulnerable to another attack like 9/11," said Capt. Paul Onorato, a commercial airline pilot and former president of the Coalition of Airline Pilots Associations.

In recent years, according to Onorato, the coalition has set up scenarios where a handful of would-be terrorists are seated in the first few rows of an airplane. These scenarios have shown that terrorists are able to "blow past" both a flight attendant and galley cart and get into the cockpit within three seconds.

What's more, Folsom added that the drills, while grim, likely offer a best-case scenario.

"We looked at some highly trained individuals playing the role of flight attendants and crew members and even they couldn't prevent a breach of the flight deck," Folsom said. "If they can't do it, then little 57-year-old, 40 percent body fat Susie isn't going to do it."

Secondary barriers, supporters say, would give crews more time -- approximately five seconds -- to react to threats. Prior to opening the cockpit door, flight crews would deploy the barrier, temporarily securing the space directly in front of the cockpit door.

"It's not an impenetrable barrier," Powers said of the device. "If somebody attempted to breach it, that would, one, give everyone an indication of that individual's intent and, two, delay them long enough so one of the flight attendants could shut the flight deck door."

Despite the barriers' perceived benefits, the FAA has yet to mandate them, largely because of the cost of the devices -- about \$5,000 to \$10,000 per barrier.

"Right now, we don't see a need for it," FAA spokeswoman Alison Duquette said, adding that the post-9/11 security measures the FAA and TSA currently have in place, such as improved screening technologies and increased air marshals, have been sufficient.

This doesn't mean the FAA has dismissed the barriers altogether. In 2008, the administration petitioned to establish a committee that includes representatives from the FAA, airlines, and airline trade associations. Folsom, a cochairman of the committee, said the group is currently working on a report that will outline minimum performance criteria, installation instructions, and other issues for secondary barriers. Folsom said the committee is on track to complete the report this September, around the 10th anniversary of 9/11.

Although a federal mandate for secondary barriers is nowhere in sight, United Airlines, which designed the devices in-house in 2002, has continued to develop and install them on its fleet voluntarily, a move Duquette says the FAA fully supports.

Meanwhile, in 2007, Northwest (now Delta) began a one-year test program of the barriers on the airline's 747s. But after receiving negative feedback from crews, the airline decided not to move forward with widespread installation. According to Wolfgang Koch, a Northwest pilot at the time, the barriers created noise in pilots' sleeping quarters and made meal and beverage service to the cockpit difficult, as flight attendants were expected to close the barrier while their hands were full. Additionally, the airline estimated that the cost of the barrier would be closer to \$100,000 over the life of the airplane.

As a result, Northwest decided not to move forward with the barriers. But Koch maintains that while that particular design wasn't ideal for the 747, the value of the device was clear.

"Some things are feel-good products and other things are substantial products. A secondary barrier is a substantial product," he said, adding that he believes Northwest gave up on the devices too quickly.

In the meantime, U.S. Rep. Steve Israel (D-NY), a longtime advocate of secondary barriers, reintroduced a bill in April calling for mandatory installation of the devices on commercial aircraft.

"Ten years ago terrorists exploited airline security vulnerabilities to murder thousands of people on 9/11. Since then we've made significant improvements, but there is still more we must do," Israel said in an e-mail. "Without secondary cockpit barriers, the door is literally wide-open whenever the crew members leave the cockpit to use the restroom, change positions during a long flight, or conduct visual inspections. A secondary barrier protects pilots and passengers for a fraction of the installation costs of an in-flight entertainment center," which costs around \$1 million.

While Folsom said he supports Israel's bill, he stressed that he is not pushing for mandated

barriers -- at least not yet. He said it is far more important that airlines see the necessity of the barriers, opting to install them voluntarily as United has done.

Also important, Folsom said, is getting airlines to understand that the secondary barrier devices themselves are only a part of the larger combination of equipment, people, and procedures that, collectively, protect the cockpit.

"If we put the barriers on and the companies are reluctant, you're not going to have ongoing training, and without proper training, it's not going to be effective," Folsom said. "This system requires active participation, so it's really important that we lead and educate and sell the industry on the value of this."

Eventually, Folsom said he hopes to show airlines that barriers, while more expensive initially, are actually more cost effective than other equivalent means of protecting the cockpit, such as extensive defense training for flight crews.

Currently, the FAA does not mandate flight attendants' defense training. Instead, the training is optional, and flight attendants must go to training facilities on their own time, paying all of the expenses incurred, said Candace Kolander of the Association of Flight Attendants.

A 2007 survey revealed that, on average, flight attendants receive between five minutes and one hour of defense training per year, according to Kolander.

"We don't believe that we're at a level yet that is sufficient for us," she said.

Folsom said that after 9/11, defending the plane essentially became part of flight crews' job description. But he stressed that training alone won't protect the cockpit.

"It's absurd to think that flight attendants are going to be able to defend against multiple highly trained attackers," he said. "They're going to roll right past them into the flight deck. There is no level of training they could receive that's going to be effective in and of itself."

If terrorists do get inside the flight deck, the reinforced cockpit door, which Folsom called a "kneejerk reaction" on the part of the government after 9/11, could end up working against the flight crew, making it impossible to regain control of the aircraft.

Despite the threats, not everyone in the aviation industry believes secondary barriers are essential to airline security.

The International Air Transport Association (IATA), an industry trade group representing 230 airlines in 115 countries, said it is confident in current security measures but supports further research on the topic of airline security.

"What we don't want to do is rush toward any measure based on a 'one size fits all' paradigm," said Anthony Concil, IATA's director of corporate communications. "Aircraft differ in type, construction, and use and to suggest that any single measure is the answer would be incorrect."

Recently, IATA has drawn criticism from some members of the secondary barrier committee. From the beginning, said Folsom, IATA "has made it clear to us that they do not think secondary barriers are a necessary enhancement to aviation sector security." Folsom called IATA's support of further research on the barriers "a politically correct way to say they want to kill the initiative." At a recent meeting, says Folsom, IATA pulled out of the committee altogether and asked that all reference to its participation be deleted. (IATA declined to comment when asked about its withdrawal from the committee.)

Ultimately, Folsom said he believes any pushback on secondary barriers stems from denial. "People don't want to admit that there's a threat out there. They have forgotten the horror of 9/11. It's like a coping mechanism," he said.

## Has Al-Qaeda Opened A New Chapter In The Sinai Peninsula?

## By Andrew McGregor

Source: http://www.jamestown.org

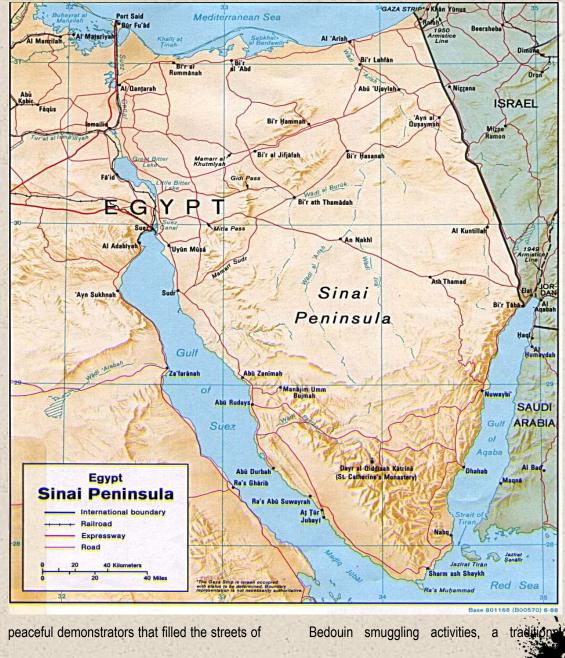
#### **Executive Summary:**

In the absence of police and government security forces, al-Qaeda-sympathetic movements, including al-Shabaab al-Islam (The Youth of Islam), have formed in the Sinai Peninsula. The demands of these Salafi-Jihadist groups reflect both local and regional concerns. Among their demands are calls for a full implementation of Shari'a, the revocation of Egypt's treaties with Israel, the establishment of an Islamic. Emirate in the Sinai and Egyptian military intervention against Israel on behalf of the Palestine.

Gaza. Despite a statement proclaiming the establishment of al-Qaeda in the Sinai Peninsula, core al-Qaeda has not yet acknowledged this new chapter of the movement. Sinai-based militants have repeatedly targeted a natural gas pipeline to Israel in a show of distaste for Arab-Israeli relations and to strike a symbol of the corruption of Mubarak's regime. These attacks and the recent storming of a police station by armed militants in the regional capital of al-Arish have alarmed Cairo, which has lost control of the region since security forces fled Bedouin attacks in the January revolution. In response to these developments, Egyptian security forces have returned to the Sinai, though there are conflicting accounts of whether their mission will be solely defensive or directed at eliminating the militant threat. The size and armament of the deployment is limited by restrictions imposed by the Camp David Accords signed with Israel. The long standing alienation of the Sinai Bedouin from the rest of Egypt and the growth of a radical Salafist movement influenced by like-minded groups in Gaza have combined to pose a serious challenge to a regime that is handcuffed in its response.

#### Introduction

The one area of Egypt that appeared ready to explode into violence during last January's revolution was the Sinai. Unlike the unarmed, Cairo and Alexandria, the Bedouin tribesmen of the Sinai were well armed and already engaged in a low-level conflict with Egyptian authorities over a number of issues, including



occupation that has lately become politicized through Bedouin interaction with radical Islamists in Gaza, the end-user of the weapons the desert dwellers are shipping to Sinai's eastern border. Possibly the only reason a large-scale conflict did not break out in Sinai at the time was the flight or desertion of nearly all the police and security forces based in Sinai after a number of attacks on police stations. Now, however, after a growing number of acts of militancy and the release of an alarming video allegedly depicting the formation of an al-Qaeda-sympathetic movement in Sinai known as al-Shabaab al-Islam (The Youth of Islam),

Egypt's security forces are back, this time accompanied by a significant military presence. [1] The release of the video and a subsequent statement followed an attack on an al-Arish police station in northeast Sinai and the fifth attack this year on a pipeline supplying natural gas to Israel.

#### Al-Qaeda in the Sinai Peninsula

An August 2 pamphlet distributed in al-Arish entitled "A Statement from al-Qaeda in the Sinai Peninsula" displayed a mix of local and regional concerns, demanding an Islamic Emirate in the Sinai, an end to the exploitation of Sinai's wealth by nonresidents, the full implementation of Shari'a, an end to discrimination against the Bedouin, the revocation of Egypt's treaties with Israel and Egyptian military intervention on behalf of the Palestinians in Gaza. It also questioned the military government's efforts to halt drugsmuggling in the region (Youm7.com [Cairo], August 2; Bikya Masr [Cairo], August 2). Though the video was carried on jihadi websites before

being taken down by its host, the declaration of a new branch of al-Qaeda in this highly sensitive and strategic region has yet to be supported by a statement from any of al-Qaeda's known media outlets.

Despite the influx of Egyptian security forces into the Sinai, the military-run interim government is reluctant to acknowledge the emergence of an al-Qaeda chapter in the Sinai. One state-controlled Egyptian daily described the group's declaration as "a fabrication" (*al-Jumhuriyah* [Cairo], August 4).

The latest disturbances began on July 29 when tribesmen in Land Cruisers or on motorcycles attacked a police station in al-Arish, killing three civilians and two security officers as well as wounding 19 others (MENA Online, July 30). The attack occurred the same day as an estimated one million Islamists gathered in Cairo's Tahrir Square to demand an Islamic state in Egypt. Tribal sources indicated that most of the attackers came from a single village that had become a stronghold of Salafi-Jihadis who "raise the black flags of al-Qaeda"



(*al-Ahram* [Cairo], August 1). A later statement by police said that 15 suspects had been arrested in connection with the attack, ten of them Palestinians (*al-Ahram*, July 31).

On July 30, an Egyptian National Gas Company (Gasco) pipeline carrying natural gas to Israel was attacked for the third time in a month, and the fifth time this year. The attackers punched a hole through the pipeline with rocket-propelled grenades. The pipeline was still out of operation following an application

attack on July 12 (*Jerusalem Post*, July 31). Israeli sources indicate that a second attack on the pipeline in the early hours of July 30 was beaten off by private security forces working for Israel's East Mediterranean Gas Company (Globes Online [Rishon LeZion], July 31).

Beside the militants' distaste for Israel, the pipeline also symbolizes the corruption of the Hosni Mubarak regime, which is believed to have offered a contract at below-market prices to Israel in return for kickbacks. The loss in revenue to the Egyptian state is estimated at roughly \$700 million. One tribal leader insisted that locals viewed such attacks by militants as little more than a nuisance: "The most they do is torch the pipeline that transfers gas to Israel and we couldn't care less about whether Israel has gas or not" (Daily News Egypt, August 12). The steady series of attacks on the \$500 million al-Arish to Ashkelon pipeline have placed the future of the project in jeopardy and Israel is already looking for alternative supplies. Further unrest spread to the main border crossing with Gaza at Rafah, a key smuggling site, where Egyptian police turned back hundreds of people (Ma'an News Agency [Bethlehem], July 31).

## The Bedouin Struggle with the State

As the meeting point of Asia and Africa, the Sinai has always been important to Egypt's security. Though the Sinai has been, with brief interruptions, a part of Egypt in one form or another since the time of the First Egyptian Dynasty (c. 3100 - 2890 B.C.E.), it has also been regarded as something apart from the Egypt of the Nile and Delta, a remote wasteland useful for mineral exploitation and strategic reasons but otherwise best left (outside of Egyptian security outposts) to the unruly Semitic and Bedouin tribes (left) that have called the Sinai home since ancient times. The effect of these policies is that the Sinai Bedouin form only a tiny minority of Egypt's total population, but retain an absolute majority in the Sinai.

In recent decades, however, Cairo has attempted to impose the deeply infiltrated security regime that existed in the rest of the country up until last January's revolution. Many Bedouin involved in traditional smuggling activities found themselves in Egyptian prisons serving long sentences in often brutal conditions. The attempt to impose a security regime on the freedom-minded Bedouin led to a greater alienation of the tribesmen from the state, and the Egyptian uprising presented an opportunity to quickly roll back decades of attempts to impose state control on life in the Sinai. Most importantly, it opened the door for those influenced by the Salafist movements of neighboring Gaza to begin operations.

There are roughly 15 Bedouin tribes in the Sinai. In the politically sensitive northeast region (including al-Arish and the border area) the most important are the Sawarka and Rumaylat. There are also significant Palestinian populations in al-Arish and the border towns of Rafah and Zuwaid.

Local Bedouin took the opportunity of storming the Sinai's prisons, freeing an unknown number of Bedouin smugalers and Palestinian militants. In nearly all cases they were unopposed by prison staff. One of the escapees was Ali Abu Faris, who was convicted for involvement in the Sharm al-Shaykh bombings that killed 88 people in 2005. Others freed included Lebanese and Palestinian prisoners convicted more recently of planning terrorist operations in Eqypt (see Terrorism Monitor, June 12, 2009). Since emptying the prisons the tribesmen have warned the police to stay out of the main smuggling centers on penalty of death and the region has been effectively operating without any type of government. Police stationed in the north Sinai have tended to be drawn from Egypt's Nile and Delta population rather than local sources, giving the impression of an occupation force to some of the Sinai's moreindependent minded Bedouin.

One unintended consequence of sealing the border between Gaza and Egypt has been growing cooperation between Bedouin and Gazan smugglers. While goods and arms have passed into Gaza, Salafi-Jihadi ideology has crossed into Sinai in return. A new and volatile of Bedouin combination dissatisfaction. Palestinian radicalism and Salafist-Jihadi ideology erupted in 2004 with the emergence of the Tawhid wa'l-Jihad (Monotheism and Struggle) – a mixed Bedouin-Palestinian group that opposed the presence of Egyptian security forces and sought to end tourism in the region. especially visits to historical or archaeological sites, which the group regarded as idolatry. The new group carried out a series of bombings in 2004-2005 that targeted tourist resorts in Sinai (well used by Israelis), and international peacekeepers belonging to the

446

Multinational Force and Observers (MFO) (see *Terrorism Monitor*, May 2, 2006). The government security operations that followed cast a very wide net, killing dozens of suspects and sweeping thousands of Bedouin into detention, creating an ever more hostile relationship between the Bedouin and Egyptian administrators and security forces.

### **Cairo's Military Response**

Cairo addressed the emerging threat on August 12 by sending over 2000 troops from the Egyptian Second Division backed by police and border guards to al-Arish, along with a number of armored vehicles stripped of their main armaments to meet security obligations under Egypt's treaty with Israel. Authorities were emphatic that the deployment was for defensive purposes only and that none of the troops would be "chasing anyone in Sinai's mountains" (*al-Masry al-Youm*, August 12). The deployment marks the largest Egyptian military presence in the Sinai since the signing of the 1979 Camp David Accords.

The military response is hampered by Camp David Accord restrictions on the deployment of Egyptian military forces in parts of the Sinai, especially in the sensitive "Zone C" near the Israeli border, where only international peacekeepers and Egyptian civilian police were allowed to carry arms before a 2005 agreement with Israel permitted the deployment of 750 soldiers to secure the border. Al-Arish is located in Zone B, where Egypt is permitted to maintain four border security battalions, but Rafah and Zuwaid are within Zone C.

Despite attempts to downplay the extent of the deployment in Sinai, the inclusion of two brigades of Special Forces (1,000 men) would indicate significant operations are planned. Security sources claim the deployment is called "Operation Eagle" and is designed to restore security in the Sinai in three phases:

- Supported by armored vehicles and warplanes, the troops will restore security in northern Sinai and crack down on organized crime and smuggling rings in al-Arish.
- Security forces will then deploy in the border towns of Rafah and Zuwaid, where they anticipate strong resistance. Salafists have already destroyed the shrine of Shaykh Zuwaid in the town that bears his name, an action typical of Salafist ideology.

• The last phase of the operation will be a coordinated ground-air offensive in the mountains of central Sinai, particularly the Mount Halal area, which is believed to be a haven for militants (*al-Masry al-Youm* [Cairo], August 13; *Egyptian Gazette*, August 13).

So far, the deployment has not impressed many tribesmen. Of the disarmed armored vehicles, tribal leader Shaykh Hassan Khalaf remarked: "They look stupid and are completely useless in facing Islamist groups who carry machine guns and heavy artillery. Israel has tied the army's hands." North Sinai governor al-Sa'id Abd al-Wahab Mabruk has denied the existence of "Operation Eagle," insisting that the newly arrived security forces will be limited to protecting individuals and buildings (Daily News Egypt, August 12).

The return of the Egyptian military to sensitive areas of the Sinai has been encouraged in some quarters of Egypt as a necessary step to allay fears of Israeli military action designed to protect Israel's security in the border region (*al-Ahram* [Cairo], August 12). Typical of the suspicion regarding Israeli intentions is a report in a Saudi-owned pan-Arab daily that said Egyptian security sources claimed to have intelligence regarding contacts between the militants and Israel's Mossad in relation to obtaining material support for further terrorist operations that would give Israel an excuse to stop the opening of the Rafah border crossing with Gaza (*al-Sharq al-Awsat*, August 12).

#### The Salafist Denial

Reports are circulating that claim Sinai's Salafist community intends to replace traditional Bedouin councils with courts run by Salafist shaykhs, their writ enforced by 6,000 armed men. According to a leading local Salafist, Shaykh Sulayman Abu Ayyub, the Salafists "will work to serve justice between people, even if we have to use force through youth members" (*al-Misri al-Youm* [Cairo], August 10). Local Salafist leader Shaykh As'ad al-Beek has denied the reports, however, maintaining that the Salafists do not conduct any armed activities (Daily News Egypt, August 12).

The leader of the Salafist movement in al-Arish, As'as Bey al-Arish, denied that the Salafis had entered into any confrontations with police in Sinai, claiming that such rumors originate with Israel's Mossad,

"propagates such rumors to foster instability in Sinai" (Youm7.com [Cairo], August 12; *Bikya Masr* [Cairo], August 12). Other Salafist leaders have denied that the movement had any part in the attack on the al-Arish police station (MENA Online, August 2).

#### Conclusion

The near collapse of Egypt's internal security forces has opened Egypt to a resurgence of Islamist violence that would have been inconceivable a year ago. There are now concerns within Egypt that the nation's sizeable but divided Islamist community intends to usurp the secular revolution to impose an Islamic state in Egypt.

Aside from suspicions of Israeli involvement in instigating the unrest, some Egyptian commentators see the hand of HAMAS behind the disturbances in the Sinai (*al-Akhbar* [Cairo], August 10). However, there seems to be a general reluctance to discuss the specific grievances of the Sinai Bedouin or their place in Egyptian society. Thousands of years of Egyptian occupation have failed to integrate

the native peoples of the Sinai Peninsula into Egypt, whether socially, politically or even economically. The persisting sense of alienation provides fertile ground for the growth of militancy, conditions easily exploited by Salafist-Jihadi groups that see themselves as fighting two enemies in the region – the apostate regime in Cairo and the Zionist regime in Israel. While the enhanced security force now in the Sinai may be able to restore some semblance of security in the urban areas of the northeast, it will almost certainly be insufficient to tackle the militants should they decamp to the wild, cave-ridden mountain region of central Sinai.

#### Note:

1. The video was posted to YouTube (www.youtube.com/watch?v=OYuKeeIVFzM) on July 27, but has since been removed "as a violation of YouTube's policy on depiction of harmful activities."

Andrew McGregor is Director of Aberfoyle International Security, a Toronto-based agency specializing in security issues related to the Islamic world.

## Egypt's 5,000 troops take on 2,000 al Qaeda in Sinai

Source: http://www.debka.com/article/21209/

Egyptian troops enter Sinai in force

Egyptian forces descended on the Sinai



Peninsula Sunday, Aug. 14, for their first post-Mubarak operation to retake control of the territory from lawless and terrorist elements rampant there since the Egyptian revolution and responsible for sabotaging the Egyptian gas pipeline to Israel, Jordan and Syria.

Monday, three Egyptian army brigades of 1,700 men backed by tanks, an equal number of special policemen and 3,400 security personnel drove into the northern towns of El Arish, Sheikh Zuweid and Rafah, which is divided between Egypt and the Gaza Strip. In their first clashes with Islamic Liberation Army gunmen, they killed one and detained 11, four of them Palestinians, he Egyptian military communiqué reported.

debkafile's military sources add that three Egyptian officers were kidnapped in the clash – whether they were killed or held as hostages is unknown.



For two years, debkafile's counter-terror sources have been reporting on the burgeoning concentration of al Qaeda cells and affiliates in Sinai and the Hamas-ruled Gaza Strip. The 2,200 Egyptian troops maintained there after Feb. 14 to maintain order and guard the Egyptian natural gas pipeline to Israel, Jordan and Syria were easily overpowered The facility was sabotaged five times and supplies remain cut off. Restoring a semblance of law and order to northern Sinai will be the easy part of the Egyptian military mission – for which Cairo obtained prior Israeli permission as mandated under their peace accord. The hard part is



ahead when in the coming weeks the units head south to flush out the Islamist invaders holed up in the central Sinai Mountains to which they withdrew last week after being tipped off that large-scale Egyptian forces were coming.

On the narrow mountain trails, the soldiers will have their work cut out to contend with 2,000 well-organized and heavily armed Islamist gunmen. The forbidding central Sinai range of precipitous peaks, from 1,000 to 2,642 meters tall, covers 21,000 square kilometers. The terrain has deep wadis, dense shrubbery, abundant natural water and plenty of animals for food. Judged in terms of the war in Afghanistan, a Taliban force this size in control of a region twice the area of the Taliban stronghold of North Waziristan would pose a prohibitive challenge even to a full-scale NATO army. Egyptian forces have fought for control of these mountains several times but failed, ending up with accommodations of sorts with the 350,000 Bedouin tribes sheltering the Islamists and sharing in their smuggling trade. The tribes always came out of these deals in control of the region.

Our military sources therefore expect this first wave of Egyptian armored forces into Sinai to be followed by more - if Cairo's rulers seriously intend to recapture the strategic peninsula and expunge the al Qaeda presence. There is no way this can be accomplished, according to our military experts, without air might. The terrorists' hideouts will have to be bombed from the air and combat helicopters provide cover for armored units moving along the isolated Sinai trails; drones will be needed to gather intelligence on enemy movements.

Cairo will have to apply to Jerusalem for permission to deploy air might in Sinai for the first time since the territory was demilitarized under their peace accord. debkafile's military sources report that the Islamic Liberation Army - which has declared its objective as the seizure of all of Sinai and its transformation into a Muslim Caliphate - is a conglomerate of five terrorist groups:

- ☑ Indigenous Bedouin tribes who have a score to settle with the Egyptian army;
- Palestinians from the Gaza Strip drawn into extremist Salafi sects which are integral parts of al Qaeda.
- Hundreds of adherents of the Egyptian Islamic Jihad and the murderous Jamaa al-Islamiya who escaped Egyptian prisons on January 29 at the peak of the popular revolution which overthrew Hosni Mubarak. The former jailbirds made a beeline for Sinai and today constitute the hard operational core of the movement.
- Al Qaeda adherents, who made their way to Sinai after violent careers in Afghanistan and Pakistan in the late 1990s and early 2000s.
- Followers of various Egyptian Sufi and dervish orders.

## Innovative disaster communication tech developed

Source: http://www.gatech.edu/newsroom/release.html?nid=69356

Communication networks typically collapse when they are needed most -- during and in the

immediate aftermath of massive disasters; researchers have developed a -- an innovative.

wireless system called LifeNet designed to help first responders communicate after disasters; LifeNet is a mobile ad-hoc network designed for use in highly transient environments that requires no infrastructure such as Internet, cell towers or traditional landlines.



LifeNet ad-hoc network will work with cellphones and laptops // Source: smartphonewell.com

In the aftermath of most disasters — from the terrorist attacks of 9/11 to this year's earthquake in Japan — communication systems have been overwhelmed, leaving people without phones and Internet when they need these tools the most.

Georgia Tech College of Computing researchers have developed a possible solution. It is an innovative wireless system called LifeNet designed to help first responders communicate after disasters. LifeNet is a mobile ad-hoc network designed for use in highly transient environments that requires no infrastructure such as Internet, cell towers or traditional landlines.

"It's an independent network you can join," said Santosh Vempala, Georgia Tech distinguished professor of computer science in the College of Computing.

"It doesn't need wires, antennas, cell towers and so on, and it works across platforms like laptops and smart phones. We imagine relief agencies would be able to set up a network right away and communicate about what's needed."

A Georgia Tech release reports that Vempala and his graduate student, Hrushikesh Mehendale, demonstrated the LifeNet system at the ACM SIGCOM conference in Toronto, Canada, on Monday. The standard for post-disaster communications is the satellite phone, which, at \$600 or more per unit, can be expensive to own, and, at 50 cents per text, costly to use.

LifeNet, however, bridges connectivity between a satellite phone or other Internet gateway and a WiFi-based network on the ground. It extends the coverage of a satellite phone or a service such as SMS from one computer with access to the entire independent network in the field. Essentially, that means several people in the field who may not have satellite phones but have smart phones or laptops with WiFi capability can connect to the LifeNet network, communicate with each other with no other infrastructure and use the Internet as long as any one of them has access.

"Currently available options such as satellite communication are expensive and have limited functionality," Mehendale said. "If you use LifeNet, the cost savings per text message is 100 times less than a satellite phone."

LifeNet is also easy to set up. The network starts as soon as a node is put in place. Each LifeNet-enabled computer acts as both a host client and a router, able to directly route data to and from any other available wireless device. Nodes can be moved from location to location as needed, and the network remains intact.

The software developed by Vempala and Mehendale for LifeNet provides basic communications that are low bandwidth and reliable. It does not allow users to stream video, for example, but it can send text messages for basic communication needs.

"It's a trade-off of performance for reliability," Vempala said. "Reliability is really what you need the most in these situations."

During the demo at SIGCOMM, conference attendees could see the Atlanta-based LifeNet network via a Web-based interface in Toronto. They were able to log into the network, send messages, move nodes, and see how communication is affected.

Georgia Tech researchers are currently ready to deploy LifeNet for field testing and are looking to expand beyond crisis communications.

The release notes that Vempala's team recently partnered with Tata Institute of Social Sciences India, which has a disaster management center. Together, the researchers identified cyclone-affected areas without communications infrastructure that could benefit most from LifeNet. As a

researchers will be deploying LifeNet in the Mohali region of India over the next several months.

"In an area without any other connectivity, we will establish a set up that could be used daily and could also be specifically helpful during a disaster," Mehendale said. "We need to make the solution a part of their daily lives since people cannot afford costly equipment like satellite phones in third-world regions." The researchers also hope to pitch LifeNet as a package to FEMA, the Red Cross, and other U.S. relief agencies soon.

"There are many recent situations, like the Mississippi floods this summer, where this would have been valuable," Vempala said. "People were trapped. Cell phones were not working, the Internet is down and people don't have a way to communicate.... LifeNet can be the solution."

# The Lone Wolf Jihad

## By Raymond Ibrahim

Source: http://www.meforum.org/3017/lone-wolf-jihad

As we near the ten-year anniversary of the September 11, 2001 strikes, the Obama administration is stressing that the threat remains, but in a different form. In a speech at a Chamber of Commerce event yesterday, Homeland Security Secretary Janet Napolitano said:

[T]he U.S. has a "layered system of security that would give us multiple ways to deter" an attack like the one a decade ago in which airplanes were weaponized. "What we see now is smaller plots," she said. "We are also seeing a rise of activities by individuals who are actually in the country, and they are acting by themselves and that kind of attack is the most difficult to prevent because there is nothing to intercept." Napolitano's comments echoed what President Obama said in an interview Tuesday in discussing the 10-year anniversary of Sept. 11.... With the nation preparing to observe the 10th anniversary of hijacked airliners crashing in New York and Washington and in the Pennsylvania countryside, Obama said the government is in a state of heightened awareness. "The biggest concern we have right now is not the launching of a major terrorist operation, although that risk is always there," the president said. "The risk that we're especially concerned over right now is the lone wolf terrorist, somebody with a single weapon being able to carry out wide-scale massacres of the sort that we saw in Norway recently," he said. "You know, when you've got one person who is deranged or driven by a hateful ideology, they can do a lot of damage, and it's a lot harder to trace those lone wolf operators."

While it is nice that the administration is able to acknowledge that jihadis are going lone wolf that the jihad has metastasized—this report is a reminder of the administration's failed policies, policies which in many ways led to the current situation, where it is no surprise that, a decade after the strikes of 9/11, "the government is [still] in a state of heightened awareness."

For starters, rather than once attempting to understand the ideology of jihad itself and its place in Islamic history and tradition—not to malign, but for proper context, to understand what one is up against—the administration, like the one before it, preferred to take the easy, politically-correct, way out: focus on formal organizations and people—al-Qaeda and Osama bin Laden, as the root source of the problem—while ignoring the jihadi elephant in the room.

Indeed, all evidence indicates that the focus remains on the tangible, the quantifiable—al-Qaeda—without wanting to look at the surrounding context which produces groups like it and even jihadi lone wolfs. In the CNN interview, "Obama said the government continues to monitor and gather information about potential terror plots, even though Al Qaeda's capabilities have been degraded," Note the ingrained "even though," as if the

very demise of al-Qaeda, its total eradication, is naturally supposed to equate the demise of jihad, which is some 1400 years older than al-Qaeda.

And if ever there was talk on the context that fuels the jihad, it was always the idea that U.S. foreign policy in the Middle East was to blame

(regurgitating what the jihadis themselves were saying). Likewise, it was believed that terrorism was a "foreign" problem that could never infect American Muslims, as it has nothing to do with Islam.

Yet here is Napolitano saying that "We are also seeing a rise of activities by individuals who are actually in the country." More to the point, months earlier, Attorney General Eric Holder

said that "the threat has changed ... to worrying about people in the United States, American citizens — raised here, born here, and who for whatever reason, have decided that they are going to become radicalized and take up arms against the nation in which they were born."

None of this is surprising, considering that the Obama administration went out of its way to ban the use of accurate words—such as jihad and Islam from national security documents thereby epistemologically undermining



American discourse on the nature of the threat. In short, Fort Hood style attacks—both the successful one of 2009 and the unsuccessful one from weeks ago—should have been expected. Expect more to come as the lone wolf jihad runs loose.

Raymond Ibrahim, an Islam-specialist, is a Shillman Fellow at the David Horowitz Freedom Center and an Associate Fellow at the Middle East Forum.

## Implication of the Negev terrorist incident

By Jeffrey White and Ehud Yaari Source: http://www.washingtoninstitute.org/templateC05.php?CID=3394

The August 18 Palestinian terrorist attack in Israel's southern Negev Desert is the most serious such incident since 2008. The Israeli casualty toll was nearly forty, including eight dead. Seven of the terrorists were killed as the Israel Defense Forces (IDF) responded and the fighting extended into the night.



The violence represents a major break in the relative calm on Israel's southern border, with major implications for both the situation in Gaza and Israel's relationship with Egypt. The focus of military action has now shifted to the improvised explosive devices (IEDs), explosive vests, and a mortar. Their targets included two civilian buses and several cars, and they used IEDs against IDF units responding to the action. The scope and complexity of the



Gaza area, and another Gaza escalation cycle may be underway, with an uncertain outcome. Furthermore, the incident is seriously aggravating Israeli-Egyptian relations, with Cairo claiming Israel killed and wounded Egyptian soldiers in the course of the incident.

#### THE INCIDENT

The terrorist attack was conducted by elements of the Gaza-based Popular Resistance Committees (PRC), an organization with close operational ties to Hamas. It was controlled from Gaza and mounted via the so-called "Uroute," by which Palestinian operatives attempt to move from Gaza to the Sinai and then into Israel. The attack itself was carried out along a strip of the Israel-Egypt border north of Eilat along Israeli Route 12, where the road runs very close to the boundary in an area frequently used for illegal immigration and smuggling.

As many as twenty terrorists were involved, apparently divided into several groups acting in concert. They used various weapons, including at least one rocket-propelled grenade, operation suggests careful planning and intelligence collection, significant logistics preparation, and determined execution.

The Israeli death toll included one IDF soldier and one counterterrorism police commando. Six Egyptian soldiers were also reportedly killed, and although the circumstances of their deaths are unclear, Egypt is claiming that some of them were killed by Israeli fire.

#### **IDF RESPONSE**

The IDF reportedly had general warning of a potential Sinai-based terrorist attack some days before the event, but not specifics regarding time and place. Special combat forces from the Golani Infantry Brigade and the police counterterrorism unit were deployed as a result of the warning and responded quickly to the incident. Some Israeli troops reportedly crossed the border briefly and shallowly to engage terrorists there.

After identifying the PRC as the group responsible, Israel retaliated directly against its leadership in Rafah with airstrikes. PRC leader Kamal Nairab (alias Abu Awad) and four of bir lieutenants were killed, including military commander Imad Hamad, who Israeli intelligence believes planned the attack.

More broadly, the incident highlights the challenge Israel faces in responding to threats from the Sinai. Because of the peace treaty with Egypt, Israeli forces cannot operate in the area and must rely on Egyptian authorities to control criminal and terrorist activity there. Even if the IDF has warning of an attack, it cannot do much more than increase its state of alert, reinforce its side of the border, and pass the warning to Egypt. In 2010, Israel began construction of a security barrier along the Sinai border and is reportedly about 20 percent finished. Completion of this project will help but not eliminate the problem.

#### THE EGYPTIAN DIMENSION

The attack also highlights Cairo's growing Sinai problem. The vast Sinai Peninsula and 170mile border with Israel have always proven difficult for Egyptian governments to control, including the Mubarak regime. But the situation has become more chaotic since the revolution, with smuggling, crime, and violence increasing significantly, including several attacks on gas pipelines and a recent assault by some 200 jihadists and Bedouins on an Egyptian police station at al-Arish in the northern Sinai.

Indeed, conditions in the area have been exacerbated by the government's traditionally poor relationship with the Bedouin population. Cairo has put most of its effort into policing the Sinai's northeast corner, where its ongoing "Operation Eagle" aims to disrupt criminal and jihadist activity. Yet this focus has left the central area more vulnerable to such problems.

#### WHY NOW?

The attack was most likely spurred by internal pressures among Gaza-based Palestinian terrorist groups to strike at Israel. Some group leaders may have believed that such an operation could relieve the pressure while avoiding full-scale Israeli retaliation, given that the attack was not conducted directly from Gaza.

Israeli sources indicate that the operation was also intended as a kidnapping action based on the Hizballah model: that is, a border attack coupled with the seizure of military personnel or civilians. Israeli civilian vehicles using this road are certainly vulnerable to such tactics, though no Israelis were taken in this instance. Moreover, Hamas has never really given up on kidnapping as a strategy, and the PRC aided the group in the 2006 seizure of Israeli soldier Gilad Shalit.

#### IMPLICATIONS

The incident, which became a prolonged engagement, has very serious implications. Most immediate is the potential for escalation. Rocket fire from Gaza has already resumed in earnest, with more than twenty launches into southern Israel, several of them hitting populated areas. For its part, the Israeli Air Force has struck multiple PRC and other terrorist-associated facilities in Gaza, in response to both yesterday's attack and the rocket strikes.

Israel did not immediately strike Hamasassociated targets, however, and the group has not joined directly in the attacks on Israel. Should those conditions change, the cycle of retaliation could expand in intensity and scope.

In addition, the incident has seriously aggravated Israeli-Egyptian tensions. Cairo has officially protested what it claims was the killing of its forces by Israeli troops, demanded an investigation of the incident, and closed the Nitzana cargo border crossing with Israel. The Egyptian chief of staff has gone to the Sinai, and anti-Israel demonstrations have occurred in Cairo and Alexandria. Contacts between the IDF and the Egyptian military continue, however.

Looking ahead, the IDF will need to focus more attention on the Sinai. This is not to say that Israel has done nothing up to now: the barrier project, changes in southern force structure, the issuing of periodic Sinai terrorist warnings, and the agreement to allow Egypt to deploy 2,000 additional troops into the peninsula for Operation Eagle all show that Israel has not been ignoring the problems. But it will now likely devote even more attention to the area. That means more money, more intelligence assets, more rapid construction of the barrier, and probably more forces in the south.

#### CONCLUSION

Yesterday's attack has triggered a strong reaction from Israel, as its perpetrators undoubtedly expected. The situation now threatens to escalate into both a wider Israel-Gaza conflict and an Egyptian-Israeli diplomatic crisis. Controlling this escalation will

require careful responses from Hamas, Egypt, and Israel.

Specifically, Hamas must curb any surge in rocket fire by its own military wing and other armed elements. This will not be easy even if the organization actually wishes to do so. Egypt needs to prevent the emotions of the

moment from producing a breach in relations with Israel and demonstrate that it is capable of maintaining security in the Sinai. And Israel must weigh carefully the scope and nature of its response. An overly harsh or broad Israeli retaliation could spur further escalation both in Gaza and in tensions with Egypt.

Jeffrey White is a defense fellow at The Washington Institute, specializing in military and security affairs. Ehud Yaari, a distinguished Israeli journalist and author, is a Lafer international fellow with the Institute.

## Attacks in Israel and New Militant Opportunities in Egypt

Source: http://www.stratfor.com/regions/middle\_east

A series of coordinated attacks took place on Thursday (Aug 18, 2011) along Israel's border with Egypt. While each attack was relatively small, the incidents indicate some degree of coordination among the attackers. Israeli Defense Minister Ehud Barak attributed the attacks to elements emanating from the Gaza Strip, while Israel Defense Forces (IDF) tactical



reports stated that the attacks had been launched from across Israel's border with Egypt along the Sinai peninsula. No one has yet claimed responsibility.

Israel has plenty of experience in dealing with threats from militants in Gaza. In response, Israel often conducts preemptive as well as retaliatory airstrikes using real-time intelligence. In addition, whenever things appear to be getting out of control, the IDF conducts a major ground offensive.

Attacks inside Israel have become a rare occurrence. Weakened capability and shifting strategic imperatives have caused Hamas and other militant groups to largely refrain from such attacks. Most attacks usually consist of the firing of rockets from Gaza, a practice Hamas has an interest in both limiting as well as calibrating to enhance its control over the Strip.

In light of recent unrest in the Arab world and the new political and security reality in Egypt, these latest attacks in Israel potentially represent a new kind of threat — one posed by transnational jihadists who have long wanted to undermine Egypt without operational success.

It is quite possible that al Qaeda is trying to exploit the post-Mubarak political environment to mobilize its Sinai- and Gaza-based assets in order to create an Egyptian-Israeli crisis that can (potentially) undermine Cairo's stability.

#### Egypt After Mubarak

Under the police state run by ousted President Hosni

Mubarak, Egypt successfully kept political Islamists restrained, neutralizing the threat from jihadist groups. The unrest that broke out in the Arab world earlier this year has altered the domestic political reality in Egypt. Mubarak's fall from power in the wake of popular agitation and the Egyptian military regime's obligated engagement in political reforms have created a new environment one in which autocratic measures have become largely obsolete.

Egypt's rolling back of the police state and subsequent political reforms have made it difficult to maintain domestic security and keep militants under control. Indeed, militants are already taking advantage of the political opening. They have stepped up their operations, as evidenced by attacks against energy infrastructure and other targets in the Sinai Peninsula.

The new era of Egyptian multiparty politics has also allowed a variety of Islamist actors to emerge as legitimate political entities. At the same time, Egyptian national sentiment is emerging as a major factor in the foreign policymaking process. This change alone constitutes a threat to Israel's national security, though it is a more of a long-term issue.

The rise of different types of Islamist actors (Muslim Brotherhood, Salafists and Sufists, among others) as legitimate political entities who pursue constitutional means to come to power makes it difficult for jihadists to directly threaten the stability of the Egyptian regime. With even Salafists and former jihadist groups such as Gamaah al-Islamiyah and Tandheem al-Jihad embracing the political mainstream. the jihadists will have a hard time gaining support for an armed insurrection against the Egyptian state. Realizing that they are not able to directly confront the Egyptian state (despite the Arab unrest), the jihadists are trying to indirectly undermine the regime by exploiting the Israeli-Gaza situation and the renewed militancy in the Sinai.

#### A New Threat To Israel?

Even before today's attacks, the Israelis responded to increasing attacks in the Sinai by allowing Cairo to deploy an additional 1,000 troops to the peninsula. That concession indicated that Israel is likely skeptical of the Egyptian military's ability to effectively deal with this problem, considering current political and security circumstances. Cairo is under a lot of stress domestically and regionally. Egypt is in the early stages of trying to manage political and militant opposition in a tense political climate and it is unable to maintain internal security as effectively as it once did.

Israel, therefore, will likely see today's attacks as a new kind of threat. The Israeli leadership realizes that the problem is no longer strictly confined to Gaza but has now spread to Egypt itself. However, Israel doesn't have any good way to control the situation unfolding within the borders of its Arab neighbor. That said, Israeli officials have already begun pointing fingers at the deteriorating security situation in Egypt, a response which likely going to cause tensions between Jerusalem and Cairo — exactly what the jihadists hope to achieve.

The latest video statement from al Qaeda chief Ayman al-Zawahiri, in which he speaks of an "intellectual" effort in addition to the armed one, is noteworthy. Al-Zawahiri's comments are part of al Qaeda's response to the so-called "Arab Spring" — a development in which the jihadists have largely been marginalized. Al-Zawahiri has long been frustrated by the fact that many former jihadists in Egypt (his home country) have renounced violence, attacking al Qaeda and him personally.

For decades, the al Qaeda leader has longed to be capable of undermining the Egyptian state, and now the Arab unrest provides an opportunity (albeit not without challenges of its own). Al-Zawahiri's status as al Qaeda chief after the death of Osama bin Laden boosts the viability of this endeavor. In this new role, he is more or less free to steer the movement toward his preferred direction. His ascension to the top of the jihadist hierarchy also signals a rise of Egyptians (who have long held а disproportionate amount of influence) within the global jihadist network.

The result is that al Qaeda can be expected to focus heavily on the Egyptian-Gaza-Israeli fault line. This fixation will not only complicate matters for Israel and its efforts to deal with the Gaza Strip, it could also begin to unravel the Egyptian-Israeli relationship that has existed since the signing of the 1978 Camp David Peace Accords.

# New training facility features simulated bus, air, and rail stations

Source: http://www.homelandsecuritynewswire.com/new-training-facility-features-simulated-bus-air-and-rail-stations

On Tuesday DHS Secretary Janet Napolitano was in Brunswick, Georgia for the grand opening of a sophisticated new \$5.3 million counter-terrorism training center for law enforcement officials; the 22,000 square-foot facility features several simulation areas including a mock bus terminal, subway station, and an airport terminal

Training in simulated airliner // Source: publicradio.org

respond in real-life situations.

FLETC's new facility is the latest component of DHS's counter-terrorism training program for

law enforcement officials and Secretary Napolitano said the facility played a critical role in preventing another 9/11.

"The whole idea is to make sure that we have the best training bar for those who are charged with the mission of protecting the American homeland and all which that entails," said Napolitano. "I'm confident in saying now, almost 10 years later, we're a stronger nation, a better prepared nation when it comes to detecting and preventing terrorism and a better

The new Federal Law Enforcement Training Center (FLETC) site is designed to give local, state, and federal law enforcement officials an opportunity to conduct realistic handson training. The 22,000 square-foot facility features several simulation areas including a mock bus terminal, subway station, and an airport terminal replete with security checkpoints, baggage claim, food court, and even a boarding bridge to a 727 jet.

"Anything they can find out there, they can find in here," said Jennifer Ranger, the branch chief of FLETC's Counterterrorism Division. "This facility is designed to create real-world training

not just for counterterrorism but for all law enforcement."

Ranger added that the simulated environments will better teach officers what to look for and



how to



trained law enforcement nation."

On her tour of the facility, Napolitano watched a hazardous materials team conduct a demonstration at the facility's rail yard.

"The American public is increasingly going to be satisfied that they have and will maintain the safest transportation systems in the world and that we will not have another 9/11 on our watch," Napolitano said. "It's not going to happen."

The new center is dedicated in memory of Christine Lee Hanson (photo), who at two years-old, was the youngest victim killed in the 9/11 attacks when United Flight 175 crashed into the South Tower of the World Trade Center. Her photo hangs in the new facility, and Lee Hanson, Christine's grandfather who was on hand for the ceremony, said the portrait is a reminder of the innocent lives lost that day.

## An Emerging Threat: Al-Qaeda In The Sinai Peninsula

By Robin Simcox (The Henry Jackson Society)

Source:http://www.eurasiareview.com/an-emerging-threat-al-qaeda-in-the-sinai-peninsula-analysis-31082011/

This month's attacks in Israel were staged from the Sinai Peninsula, Egypt. Recent terrorist acts there have led the US to conclude that an al-Qaeda presence has emerged. This will the Sinai Peninsula (AQSP), has been identified as a potential key participant in the attacks on Israel.



have a significant impact on the entire region, and could further strain relations between Egypt and Israel.

At 12pm on 18 August, twelve militants launched a series of attacks near Eilat, Israel. Automatic weapons, roadside bombs, rocket propelled grenades and suicide belts were used to target passing civilian vehicles, military transport and personnel, killing six civilians and two Israeli soldiers.

The attacks were launched from the Sinai Peninsula in Egypt, after the militants tunnelled from Gaza into the Sinai, travelled down the Peninsula and entered Israeli territory. While it is still unclear which group they are aligned to, Israel's military response has largely been focused on Gaza's Popular Resistance Committees (PRC) (who praised the attacks but denied involvement).

However, US intelligence officials believe the PRC only scouted locations, and are increasingly focused on the development of terrorist groups loosely aligned to al-Qaeda (AQ) in the region. A new group, al-Qaeda in Background: The Sinai Peninsula

The Sinai Peninsula borders both Israel and Gaza, bridging Africa and Asia. The region was previously under Israeli control following the Six Day War of 1967, but was returned to Egypt as part of the 1978 Camp David accords.

The Sinai is divided into north and south governorates, and comprises four military zones. Zone A (territory to the east of the Suez Canal running northsouth) is Egyptian, and possesses a 22,000 man infantry division. Zone B (central Sinai) has four

battalions in support of the Egyptian police. Zone C (to the west of the border with Gaza and Israel) is a demilitarised zone under joint control between the Egyptian police and Multinational Force Observers. Zone D (a narrow strip on the east side of the Egypt-Israel border) has four Israeli infantry battalions, including along the Gaza border.

Historically, the Sinai has been beset by tribal disputes. It possesses a large native Bedouin population of approximately 360,000. The Bedouin are a mainly desert based, ethnically Arab group which have long term grievances with the government. The Bedouins have not shared in the economic windfall brought about in the region from tourism and mineral resources, with the tourist industry in the Sinai mainly run by Egyptians from Cairo and other major cities. According to Dr Ely Karmon, a Senior Research Scholar at the International Institute for Counter-Terrorism in Herzlyia, the Bedouins have taken to smuggling in response. This has including weapons to Hamas, narcotics, foreign workers and prostitutes, and has especially increased since 2006.

#### An increasingly lawless region

Since the popular uprisings against Hosni Mubarak began, the Sinai has become an increasingly lawless area. Dr Karmon told HJS that he believes the security situation has 'collapsed' and the Sinai is 'on the way to becoming a failed region'.

The US assessed that 200-300 prisoners were freed from Egyptian jails opened or abandoned in the wake of the uprisings, some of whom subsequently settled in the Sinai, bolstering extremist movements. Joint Palestinian-Egyptian terrorist cells went to the Sinai, seemingly assisted by local Bedouins. Salafist groups have now formed armed committees to settle tribal disputes and police stations have been attacked on multiple occasions. One attack involved militants armed with rocket propelled grenades. Another led to a fire fight in which three civilians died. In response, the Egyptian government - with Israeli consent deployed military forces into previously demilitarised zones in the Northern governorate.

The situation remains unstable. A Bedouin sheikh told the BBC that the area could be exploited by external actors such as Iran, Hezbollah and AQ. It is possible that such actors (along with Somalia) have now begun to establish training centres and hide weapons caches in the Sinai. Dr Karmon goes as far as to say that the Sinai could become 'a breeding ground for future al-Qaeda activity'.

#### The emergence of a new AQ franchise?

Following a recent attack on a police station in the Sinai, a pamphlet and video were produced containing a 'Statement from Al Qaeda in the Sinai Peninsula.' The statement called for:

- An Islamic emirate in the Sinai
- The introduction of Sharia law

• The abolition of the Egypt-Israel peace treaty

• Egyptian military intervention on behalf of Hamas in Gaza

• An end to discrimination against the Bedouin population

This mix of jihadist ambitions and Bedouin grievances suggests that either segments of

the Bedouin population have either been radicalised by AQ or sympathise with their goals; or, alternatively, AQ activists are deliberately courting the Bedouin, and highlighting issues that concern them for strategic reasons. Either way, following the operation against the police station, a US official commented that there is 'no longer any doubt that AQ had some kind of potent presence in the peninsula.' The US believes they have begun to establish basic training facilities and gain strategic control of some towns.

Recently, there have also been bombings on the pipeline that transports gas to Israel, Jordan and Syria. Bruce Riedel, a former CIA officer and current Senior Fellow in foreign policy at the Saban Center for Middle East Policy of the Brookings Institution, told HJS that it was possible that these were the 'first steps' of a group (possibly working with Bedouins) aspiring to become part of the AQ franchise and wanting to display their terrorist credentials. This assessment is shared by US officials in relation to the Eilat attacks.

If this is the case, such acts are not going unnoticed. The pipeline bombings were publicly praised by Ayman al-Zawahiri, the new head of AQ, who called for further operations against Israel to take place. (However, there is no consensus that these attacks were linked to AQ. For example, Dr Karmon believes that they were carried out by Palestinians financed by Hizbullah and Iran.)

AQ's central shura, or committee, has yet to give their formal approval of a franchise operating in the Sinai Peninsula. Yet this does not mean that such a situation could not occur in the coming months. As Riedel explains, negotiations between AQ central and aspirant groups can be protracted as there are certain criteria such aspirant cells must meet. There must be consensus on their enemies; for example, AQ does not want groups focussed solely on local issues at the expense of global goals. More importantly, according to Riedel, they must be operationally capable of violence. He states that there have been many groups in Gaza, for example, that have aspired to be part of the AQ network but have not been approved because they lacked the capacity.

US counterterrorism officials recently briefed the Washington Post that the core AQ leadership was on the verge of collapse. As such, it is possible that AQ may lower the back in how effective groups have to be in order to get their official branding. Furthermore, their weakness highlights their need to show they are still a relevant organisation. As Riedel asks, 'what better way is there of doing so than announcing that they have a new franchise, and it is in the heart of the Arab world?' This being the case, the core leadership may want to officially endorse AQSP sooner rather than later.

## What strategic impact could AQ in the Sinai Peninsula have?

The development of an official AQ branch in the Sinai Peninsula threatens the stability of an already chaotic region.

Attacks against Israel and Israeli interests could become commonplace. However, bombing gas pipelines affects not only Israel but also Syria and Jordan, both of whom import gas from Egypt. AQ could also target the Multinational Force Organization present in the Sinai as part of the Camp David accords.

Relations between Egypt and Israel would likely become fractured by AQ militancy in the Sinai. A glimpse of this came in the aftermath of the Eilat attacks. After the terrorists launched their operations, Israeli troops pursued them into the Sinai. One Egyptian officer and two policemen died in the crossfire, as did two Egyptian soldiers in a later incident.

Israel was forced to issue an apology – which may have placated the Egyptian government but has had little effect on the general Egyptian population. Riedel believes popular opinion in Egypt supports renegotiating the current peace treaty with Israel and regards the restrictions placed on their movement in the Sinai as humiliating.

Israel feared such a scenario following Mubarak's departure. Retention of peace with Egypt is a key goal in Tel Aviv, yet there is uncertainty within the Israeli government over the extent that a post-Mubarak Egypt will be willing to commit to its treaty obligations.

#### Conclusion

While the situation is bleak in the Sinai, it is not irretrievable. It is too early to describe the Sinai as a failed region in the way parts of Yemen and Somalia are. It will be virtually impossible for AQ to coordinate a takeover in the Sinai. The group does not have the manpower; it has been weakened by bin Laden's assassination; and they are pinned back in the face of sustained US drone attacks in Pakistan.

There is a risk that the lawless situation could deteriorate further if Israel and Egypt do not work together to prevent it. If AQ was to launch a sustained bombing campaign, it could push Israeli-Egyptian relations to breaking point. Israel would increasingly doubt the willingness of Egypt to restore law and order in Sinai and rein in militant groups, a perception which would only increase were the Muslim Brotherhood to strengthen its presence in the Egyptian Parliament following the upcoming elections.

In order to restore order and achieve their strategic objectives, the three main actors must establish their short and long term goals.

#### Egypt

A fledgling democratic Egypt cannot allow the Sinai Peninsula to descend into further chaos analogous to Somalia or Yemen. Failure to do so will only allow AQ to embed itself deeper in the region. It should therefore:

- Seek permission from Israel to increase its military presence in particularly lawless areas in the Northern governorate.
- Make steps to resolve the grievances of the Bedouins. The mistrust between the state and the Bedouins cannot be resolved overnight, but the state needs to foster the support of tribal elements in order to isolate terrorist groups.

#### Israel

Israel's immediate concern is the threat that an AQ presence on its border poses. It is also reticent about the direction that a post-Mubarak Egypt will take: allowing Egypt to break the terms of the 1979 treaty gives an insight to the strategic importance with which it views the Sinai Peninsula. Israel should therefore:

- Allow Egypt access to the lawless parts of the Sinai which terrorists are seeking refuge in, while seeking assurances concerning their dedication to the Camp of David accords.
- Ensure it hits its target of completing the Israel-Egypt security fence by next year.

#### US

The US is currently making significant progress against the AQ core in Pakistan. However, it is struggling to contain AQ in Yemen and other, affiliates, and does not want a new frances

develop in the Sinai. To this end, Riedel believes that the CIA has almost certainly already established an intelligence gathering presence in the Sinai. Separately, good Egypt-Israeli relations are a pre-requisite to furthering the Middle East peace process. The US should therefore:

- Encourage Egypt behind the scenes to crack down on terrorist groups in the Sinai.
- Stress to Israel the importance of temporarily accepting an increased Egyptian military presence in the region.
- Lead a concerted international effort to ensure Egypt agrees to respect the Camp of David accords
- The CIA should continue intelligencegathering on the ground. It needs a flexible approach: as extremist groups grow more entrenched, it will be more dangerous to collect sound data.

The Henry Jackson Society: Project for Democratic Geopolitics is a cross-partisan, British-based think-tank. Its founders and supporters are united by a common interest in fostering a strong British and European commitment towards freedom, liberty, constitutional democracy, human rights, governmental and institutional reform and a robust foreign, security and defence policy and transatlantic alliance.

## Iran's Quds Force: Supporting Terrorism Worldwide

Source:http://www.realite-eu.org/site/apps/nlnet/content3.aspx?c=9dJBLLNkGiF&b=2315291&ct= 1203021

Recently the European Union announced that it was introducing sanctions against Iran's elite

Iraq, declared that Iranian-backed militias represent the greatest threat to Iraq's security,



Quds Force on the grounds of its technical and material support to President Bashar al-Assad of Syria in his repression of the five-month-old uprising against his regime. [1]

On the same day, Maj. Gen. Jeffrey S. Buchanan, the top US military spokesman in

outpacing al-Qaida-linked terrorists. Maj. Gen. Buchanan pointed out that the Quds Force "is providing direct support to the militias in terms of manning, equipping, provision of intelligence." [2]

#### **Global reach**

According to the US State Department, the Quds Force, "the external operations branch of the Islamic Revolutionary Guard Corps (IRGC), is the regime's primary mechanism for



cultivating and supporting terrorists abroad." [3] On October 25, 2007, the US Department of the Treasury named the Quds Force a "specially

designated global terrorist organization," freezing its assets under US jurisdiction and prohibiting transactions with US parties. Measures were also taken against several senior Quds officers, including the force's commander Qassem Suleimani. [4]

The Quds Force's activities are global: it has directorates for Iraq, Lebanon, Palestine and Jordan; Afghanistan, Pakistan and India; Turkey and the Arabian Peninsula; Asian countries of the former USSR, Western nations (Europe and North America), and North Africa (Egypt, Tunisia, Algeria, Sudan, and

Morocco). [5]

Its global reach was clearly stated by the unit's commander Suleimani, who reportedly said in early 2008: "General Petraeus (then the top US commander in Iraq), you should know that I, Qassem Suleimani, control the policy for Iran with respect to Iraq, Lebanon, Gaza, and Afghanistan. And indeed, the ambassador in Baghdad is a Quds Force member. The individual who's going to replace him is a Quds Force member." [6]

## The Middle-East

### Iraq

In January 2007, Iran's Supreme National Security Council decided to place all Iranian operations in Iraq under the command of the Quds Force. At the same time, it increased its personnel strength to 15,000. [7] The last eight years have witnessed a proxy war between the Quds Force and the US military. In 2007, Gen. David Petraeus testified to the US Congress on the growing role of the Quds Force. He noted that the US had found Quds operatives in Iraq and seized computers with hard drives that included a 22-page document that had details about the planning and conduct of an attack that killed five US soldiers in Karbala. [8] The same year, Brig. Gen. Kevin J. Bergner, a US military spokesman, asserted that Iran's Quds Force was providing armor-piercing weapons to extremist groups in Iraq, funneling as much as \$3 million a month and training Iraqi militiamen at three camps near Tehran. [9] In June 2011, 15 US servicemen died in Iraq, the highest monthly casualty figure there in more than two years. The US attributed these attacks to Shiite militias trained and armed by the Quds Force. [10] Recent evidence indicates that these militias are using Iranian materials in "Improvised Rocket-Assisted Munitions" attacks against US troops. The munitions, or IRAMS, are metal canisters packed with explosives and propelled by rockets. IRAMS along with armor-piercing grenades are believed responsible for the majority of US deaths in recent months, an American official said. [11]

#### Afghanistan

According to the US Department of the Treasury, the Quds Force "provides select



members of the Taliban with weapons, funding, logistics and training." [12] In December 2010, a member of the Quds Force was captured supplying weapons to the Taliban in Afghanistan for attacks on British and American troops. [13] In recent months, the Pentagon has traced to Iran the Taliban's acquisition of rockets that give its fighters roughly double the range to attack NATO and US targets. [14]

Syria



462

The European Union sanctions announced last Wednesday against the Quds Force represent a direct international accusation that Iran is helping Syria in carrying out a brutal crackdown, which the United Nations says has killed 2,200 since March. [15] The European Union said in a statement published in its official journal that the Quds Force "provided technical assistance, equipment and support to the Syrian security services to repress civilian According to a US Department of Defense report released in April 2010, recent years have witnessed an increased presence of the Quds Force in Latin America, particularly in Venezuela. [18] "If US involvement in conflicts in these regions deepens, contact with the IRGC-QF (Quds Force), directly or through extremist groups it supports, will be more frequent and consequential," the report said. Iran's terrorist infrastructure in Latin America



protest movements." [16]

#### **Hezbollah and Hamas**

The US Treasury has stated that the Quds Force "continues to support designated terrorist groups such as Hizballah and Hamas. Hizballah is the largest recipient of Iranian financial aid, training, and weaponry; and Iran's senior leadership has cited Hizballah as a model for other militant groups. Iran also provides training, weapons, and money to Hamas, bolstering the group's ability to maintain its armed resistance and opposition to Israeli-Palestinian peace negotiations." [17]

#### Latin America

#### **References:**

[1] "Europe Accuses Iranian Force of Aiding Syrian Crackdown", The New York Times, August 24, 2011, http://www.nytimes.com/2011/08/25/world/middleeast/25syria.html

[2] "US general: Iran-backed groups biggest Iraq threat", AP, August 17, 2011 http://www.iranfocus.com/en/index.php?option=com\_content&view=article&id=23608:us-general-iran-backedgroups-biggest-iraq-threat&catid=7:iraq&Itemid=29

[3] State Sponsors of Terrorism: http://www.state.gov/s/ct/rls/crt/2010/170260.htm

has already been used in the past to launch terrorist attacks, such as the 1992 Israeli Embassy attack and the 1994 bombing of the Jewish community center in Buenos Aires (Amia). According to the Argentinian prosecutor, Iran's Defense Minister Ahmad Vahidi, then the head of the Quds Force, "participated in and approved of the decision to attack Amia during a

meeting in Iran on August 14, 1993". [19] Vahidi is wanted by the Interpol for his involvement in the bombing that killed 85 people and wounded hundreds.

#### Africa

In October 2010, Nigerian security forces seized an Iranian weapons shipment in the port of Lagos. The arms seizure led to the arrest of a Quds Force officer in Nigeria suspected of facilitating the shipment. [20] Nigeria reported the incident to the UN last November, as Iran is barred from shipping weapons internationally. [21] Gambia [22] and Senegal [23] cut ties with Tehran over the incident.

[4] Fact Sheet: Designation of Iranian Entities and Individuals for Proliferation Activities and Support for Terrorism, October 25, 2007, http://www.treasury.gov/press-center/press-releases/Pages/hp644.aspx

[5] "Iran's Revolutionary Guards, the Al Quds Force, and Other Intelligence and Paramilitary Forces", Center for Strategic & International Studies, Arleigh A. Burke Chair in Strategy, August 16, 2007, http://csis.org/files/media/csis/pubs/070816\_cordesman\_report.pdf

[6] "Qassem Suleimani: the Iranian general 'secretly running' Iraq", The Guardian, July 28, 2011 http://www.guardian.co.uk/world/2011/jul/28/qassem-suleimani-iran-iraq-influence

[7] "Iran's Revolutionary Guards, the Al Quds Force, and Other Intelligence and Paramilitary Forces", Center for Strategic & International Studies, Arleigh A. Burke Chair in Strategy, August 16, 2007, http://csis.org/files/media/csis/pubs/070816\_cordesman\_report.pdf [8] Ibid.

[9]"Iran's Elite Force Is Said to Use Hezbollah as 'Proxy' in Iraq", The Washington Post, July 2, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/07/02/AR2007070200174.html

[10] "Iran Funnels New Weapons to Iraq and Afghanistan"Wall Street Journal, July 2, 2011, http://online.wsj.com/article/SB10001424052702303763404576420080640167182.html

[11] "Official: Militias using Iranian weapons to target U.S. in Iraq", CNN, July 5, 2011, http://edition.cnn.com/2011/WORLD/meast/07/03/iraq.us.militia.attacks/

[12] http://www.treasury.gov/press-center/press-releases/Pages/tg810.aspx

[13]"Iranian soldier captured in Afghanistan", The Telegraph, August 31st, 2011, http://www.telegraph.co.uk/news/worldnews/asia/afghanistan/8223431/Iranian-soldier-captured-in-Afghanistan.html

[14]"Iran Funnels New Weapons to Iraq and Afghanistan", The Wall Street Journal, July 2, 2011, http://online.wsj.com/article/SB10001424052702303763404576420080640167182.html

[15] "Europe Accuses Iranian Force of Aiding Syrian Crackdown", The New York Times, August 24, 2011, http://www.nytimes.com/2011/08/25/world/middleeast/25syria.html

[16]"EU releases new Syrian repression blacklist", EUBusiness, August 24 , 2011, http://www.eubusiness.com/news-eu/syria-politics-oil.bv8

[17] http://www.treasury.gov/press-center/press-releases/Pages/tg810.aspx

[18] "Iran's Quds force in Venezuela, Latin America: Pentagon", AFP, April 22, 2010, http://www.google.com/hostednews/afp/article/ALeqM5jvXOYLKMt3NWFER4xXMIDPSTmhBw

[19] "Iran anoints anti-Jewish bomb suspect as defence secretary", The Guardian, September 2, 2009, http://www.guardian.co.uk/world/2009/sep/02/iran-vahidi-argentina-jewish-bombing

[20] "Iran and Nigeria Discuss Seized Weapons", The New York Times, November 11, 2010, http://www.nytimes.com/2010/11/12/world/africa/12nigeria.html

[21] "Nigeria reports Iran arms seizure to U.N.", Reuters, Nov. 15, 2010, http://www.reuters.com/article/2010/11/16/us-nigeria-iran-idUSTRE6AE4TU20101116

[22] "Gambia cuts ties with Iran and orders diplomats to go", BBC, November 23, 2010, http://www.bbc.co.uk/news/world-africa-11819143

[23] "Senegal severs ties with Iran over rebel weapons", Reuters, Feb. 23, 2011, http://af.reuters.com/article/topNews/idAFJOE71M01A20110223

## **BOOK: Beyond Bin Laden: Global Terrorism Scenarios**



Source:http://www.security-risks.com/publication/books/beyond-bin-laden:global-terrorism-scenarios-9.html

Publisher: Vij Books, New Delhi, India

#### **Relevant Excerpts from the Preface**

2011 is an exceptional year in contemporary history. The tectonic shifts in the Arab world, fears of European economic melt down, American debt crisis and riots in Britain are events which have frenetically followed in quick succession hammered in our mind by 24/7 virtual and electronic media. These have to an extent overshadowed one of the seminal occurrence in countering terrorism. This was assassination of Osama Bin Laden, head of the al Qaeda, the Worlds most wanted terrorist for a decade in a cantonment town in Pakistan by United States Special Forces in a midnight raid on 2 May 2011.

For over a decade Osama has been the symbol of defiance of America, the West and the liberal world. Chased out of Afghanistan into tribal areas of Af Pak after 9/11, the deadliest terrorist attack in the United States on

11 September 2011, he succeeded in surviving what can now be seen as a mix of ingenuity, improvisation and luck. His group in the meanwhile expanded mainly due to the aura of invincibility that it acquired through 9/11 and Osama's capability to endure. Thus from Al Qaeda spawned, Al Qaeda in Iraq, the Arabian Peninsula, the Islamic Maghreb even as the principal wing, al Qaeda Central was being systematically decimated in successful counter terrorism operations from the air in tribal areas of Pakistan and on the ground in Afghanistan.

The elimination of Osama Bin Laden was a remarkable success for American intelligence and Special Forces. To track down a rebel leader who had cut himself off from communications with the World and operated from an isolated compound in an affluent locality where none would really suspect his presence requires diligence, patience and perseverance of the highest order. The intelligence techniques both human and technical that can literally find a pin in a global haystack are also extraordinary. The raid by US Special Operations Forces was also unique. Launched after careful preparation, using stealth helicopters, the deadly strike force known as the Seals swooped down on the target and in half an hour plus succeeded in achieving the mission and getting away, before local forces had even stirred.

While there was jubilation around the World, most countries in the Middle East and North Africa did not display a favourable response. In some regions there were gatherings mourning the death of Osama. Pakistan decried violation of sovereignty and the fact that the United States despite sharing special strategic relations had not provided information of the strike.

The al Qaeda and its cohorts the Taliban launched a series of deadly raids in Af Pak region targeting a number of military and non military assets including a naval base in Karachi. Soon Ayman al Zawahiri, an Egyptian doctor who was known to be the so called second in command to Osama was anointed leader of the Al Qaeda by consensus of its Majlis. In an incident on 6 August 2011 some members of the Seal team which had raided Bin Laden's compound were reportedly killed in a helicopter ambush in Maidan Wardak in Afghanistan. The, "affiliates and adherents," as the US Counter Terrorism Strategy June 2011 calls Al Qaeda's support groups as Lashkar e Taiyyaba and increasingly today individual lone rangers represent a new form of threat.

The wheel as it appears seems to have turned a full circle as the international community chasing one crisis after another could not capitalise on the deadly blow rendered to the al Qaeda in removal of its Sheikh. The surge of violence in Af Pak denotes that despite many claims by counter terror protagonists, it is apparent that while Osama has gone away terrorism may haunt us in the months and years ahead.

Will the World be a better place without Osama or will it sink to the doom that he had predicted continues to be a dilemma? There are many prognostications, some represent plain hope, others are borne out of historical experience while some spring from disparaging cynicism which see the ebb and flow of terrorism either receding or expanding as the years go on.

This Book is an attempt to work through this maze of uncertainty by examining key vectors related to the rise and fall of Osama Bin Laden and the Al Qaeda to envisage four possible scenarios ranging from the collapse of the state order [seen as unlikely] to containment of terror threat [equally challenged] in three dimensions globally, regionally and locally over the next decade or so.

The most significant impact of terrorism is likely to be in South Asia, where Af Pak region remains the centre of gravity so to say of the present genre of religious Islamic extremism. Thus the Book will mainly trace possible trajectory of terrorism in South Asia covering Pakistan, Afghanistan and India. Other streams of the Al Qaeda have received due attention however given significance of the region and impact of its spread in some of the most densely populated, under developed regions of the World the bias remains South Asia.

The evaluation of trajectory of terror is carried out by examining studies of how terrorism ends thereby providing a sound analytical footing supported by scenario building technique. Given contemporary nature of research the main resources used are statements and interviews of principal actors and primary news articles on Operation Neptune Spear that led to the death of Osama. For Al Qaeda and South Asia a series of works by a host of counter terrorism specialists across the globe have been used and mainly those who have attempted to link the past with the demise of Bin Laden and extrapolated it to the **Spear** 

Given the reach of the Book to the lay reader and policy planner alike referencing has been simplified.

## Why AI Qaeda is Unlikely to Execute Another 9/11

#### **By Scott Stewart**

Source:http://www.stratfor.com/weekly/20110831-why-al-qaeda-unlikely-execute-another-911?utm\_ source=freelist-f&utm\_medium=email&utm\_campaign=20110901&utm\_term=sweekly&utm\_content =readmore&elg=a443620731ca40c1a82a5444bd357dee

It is Sept. 1, and that means we are once again approaching the anniversary of al Qaeda's Sept. 11, 2001, attacks against the United States. In the 10 years that have passed since the attacks, a lot has happened and much has changed in the world, but many people can still vividly recall the sense of fear, uncertainty and helplessness they felt on that September morning. Millions of people watched United Airlines flight 175 smash into the south tower of the World Trade Center on live television. A short while later they heard that another plane had struck the Pentagon. Then they watched in horror as the World Trade Center's twin towers buckled and collapsed to the ground.

It was, by any measure, a stunning, cataclysmic scene, a kind of terrorist theater that transformed millions of television viewers into vicarious victims. Excerpts of the just-released memoir of then-Vice President Dick Cheney demonstrate that it was not just ordinary people who were affected by the attacks; America's leaders where shocked and shaken, too. And judging from the statements of foreign citizens and leaders in the wake of 9/11, those who proclaimed, "We are all Americans," it was also apparent that the toll on vicarious victims did not stop at the U.S. border.

One result of this vicarious victimization and the fear and helplessness it produced was that many people became fixated on the next attack and began anxiously "waiting for the other shoe to drop." This spawned an entire industry of fear as dire warnings were propagated by the Internet of the impending "American Hiroshima" that was certain to result when al Qaeda detonated all the nuclear devices it had hidden in major U.S. cities. Chain emails were widely circulated and recirculated quoting a dubious promised Israeli "security expert" who simultaneous catastrophic terrorist attacks against a number of American cities - attacks that never materialized outside of Hollywood productions.

Fast forward a decade and we are now commemorating 9/11's 10th anniversary, which seems more significant somehow because it is a round number. Perhaps of more meaningful significance is that this anniversary closely follows the death of al Qaeda leader Osama Bin Laden on May 2, 2011. Indeed, the buzz regarding this coincidence has caused many of our clients and readers to ask for our assessment of the terrorist threat inside the United States on this 10th anniversary of 9/11. While we believe that today holds some degree of symbolism for many, the threat of an attack on Sept. 11, 2011, is no higher than it was on Aug. 11 or than it will be on Sept. 12, and below we explain why.

### The State of Al Qaeda and the Jihad

All threats have two basic components: intent and capability. Al Qaeda's leaders have threatened to conduct an attack more terrible than 9/11 for nearly a decade now, and the threats continue. Here's what Ayman al-Zawahiri, now al Qaeda's No. 1, said to his followers on Aug. 15, 2011, in a message released on the internet via as-Sahab media: "Seek to attack America that has killed the

Imam of the Mujahideen and threw his corpse in the sea and then imprisoned his women and children. Seek to attack her so history can say that a criminal state had spread corruption on earth and Allah sent her his servants who made her a lesson for others and left her as a memory."

The stated intent of al Qaeda and the rest of the jihadist movement is, and has been, to strike the United States as hard and as often as possible. It logically follows, then, that al Qaeda would strike the United States on Sept. 11 — or any other day — if possible. With intent thus established, now we need to focus on capability.

One of the primary considerations regarding al Qaeda's capability to strike the United States is the state of the jihadist movement itself. The efforts of the U.S. government and its all against the core al Qaeda group, which is based in Pakistan, have left it badly damaged and have greatly curtailed its operational ability, especially its ability to conduct transnational attacks. In January we forecast that we believed the al Qaeda core was going to be marginalized on the physical battlefield in 2011 and that it would also struggle to remain relevant on the ideological battlefield. Indeed, it has been our assessment for several years now that al Qaeda does not pose a strategic threat to the United States.

Since we published our 2011 forecast, bin Laden has been killed as well as senior al Qaeda leader Atiyah Abd al-Rahman, who reportedly died in a strike by a U.S. unmanned aerial vehicle Aug. 22 in Pakistan's North Waziristan region. We continue to believe that the al Qaeda core group is off balance and concerned for its security — especially in light of the intelligence gathered in the raid on bin Laden's hideout. The core group simply does not enjoy the operational freedom it did prior to September 2001. We also believe the group no longer has the same operational capability in terms of international travel and the ability to transfer money that it had prior to 9/11.

Some people believe there is a greater chance of an attack on this year's 9/11 anniversary because of the killing of bin Laden, while others note that al-Zawahiri may feel pressure to conduct an attack in order to prove his credibility as al Qaeda's new leader.

Our belief, as noted above, is that al Qaeda has been doing its utmost to attack the United States and has not pulled any punches. Because of this, we do not believe it possesses the ability to increase this effort beyond where it was prior to bin Laden's death. As to the pressure on al-Zawahiri, we noted in December 2007 that the al Qaeda core had been under considerable pressure to prove itself relevant for several years and that, despite this pressure, had yet to deliver. Because of this, we do not believe that the pressure to conduct a successful attack is any heavier on al-Zawahiri today than it was prior to bin Laden's death.

Finally, we believe that if al Qaeda possessed the capability to conduct a spectacular attack it would launch the attack as soon as it was operationally ready, rather than wait for some specific date. The risk of discovery is simply too great. There are also some who still believe that al Qaeda maintains a network of "sleeper operatives" inside the United States that can be called upon to conduct a spectacular terrorist attack. We do not believe this for two reasons. First, because the pressure on the core al Qaeda leadership to conduct an attack in the United States has been so high for several years there is no reason that it would not have activated any sleepers by now. It would certainly not be in the group's best interest to keep any such operatives idle for a decade, especially since U.S. intelligence has made such headway in rolling up the organization. Al Qaeda has been faced with a use-it-or-lose-it scenario.

Second, while there is a long history of al Qaeda and other jihadist groups employing covert operatives and inspiring jihadist grassroots operatives or lone wolves like Fort Hood shooter Nidal Hasan, there is no history of al Qaeda employing true sleeper operatives, that is, operatives who burrow undetected into a society and then remain dormant until called upon to act. Because of this, we remain extremely skeptical that al Qaeda has ever had a sleeper network in the United States. If it had, it would have used it by now.

Would the al Qaeda core leadership like to conduct a spectacular terror attack on the 9/11 anniversary? Absolutely. Does it have the capability? It is unlikely.

#### A Grassroots Focus

As we noted in our annual jihadist forecast, we believe the greatest threat to the United States and the rest of the West in 2011 emanates from grassroots jihadists and regional franchises. However, the civil war in Yemen and developments in Somalia have preoccupied the attention of al Qaeda in the Arabian Peninsula (AQAP) and al Shabaab the two regional jihadist franchises that have shown the intent and capability to conduct transnational attacks — leaving them very little opportunity to do so. Therefore, we believe the greatest threat of an attack on the 9/11 anniversary will come from the grass roots.

The bad news is that grassroots operatives can be hard to identify, especially if they operate alone; the good news is that they tend to be far less capable than well-trained, more "professional" terrorist operatives. And this means they are more likely to make critical mistakes that will allow their attacks to be detected and thwarted.

As the past few years has demonstrated, there are almost certainly grassroots jihadists operating in small cells or as lone wolves who are presently planning attacks. In fact, we know that since at least 1990 there has not been a time when some group of grassroots jihadists somewhere in the United States has not been planning some kind of attack.

Is it possible, then, that such individuals could be inspired to try to conduct an attack on the 9/11 anniversary if they can coordinate their attack cycle in order to be ready on that date. However, given the increased law enforcement vigilance that will be in place at hard targets on that day and the capabilities of most grassroots operatives, we can anticipate that such an attempt would be conducted against a soft target rather than some more difficult target such as the 9/11 Memorial or the White House. We also believe that any such attack would likely continue the trend we have seen away from bombing attacks toward more simple (and effective) armed assaults.

It must be remembered that simple terrorist attacks are relatively easy to conduct, especially if the assailant is not concerned about escaping after the attack. As jihadist groups such as AQAP have noted in their online propaganda, a determined person can conduct attacks using a variety of simple weapons, from a pickup truck to a knife, axe or gun. Jihadist ideologues have repeatedly praised Nidal Hassan and have pointed out that jihadists operating with modest expectations and acting within the scope of their training and capability can do far more damage than operatives who try to conduct big, ambitious attacks that they lack the basic skills to complete.

And while the authorities in the United States and elsewhere have been quite successful in foiling attacks over the past couple of years, there are a large number of vulnerable targets in the open societies of the West, and Western governments simply do not have the resources to protect everything. Indeed, as long as the ideology of jihadism survives, its adherents will pose a threat.

All this means that some terrorist attacks will invariably succeed, but in the current context, it is our assessment that a simple attack in the United States or some other Western country is far more likely than a complex and spectacular 9/11-style operation. In their primary areas of operation, jihadists have the capability to do more than they do transnationally.

Indeed, despite the concept of a "war on terrorism," the phenomenon of terrorism can never be completely eliminated, and terrorist attacks can and will be conducted by a wide variety of actors (recently illustrated by the July 22 attacks in Norway). However, as we've previously noted, if the public will recognize that terrorist attacks are part of the human condition like cancer or hurricanes, it can take steps to deny the practitioners of terrorism the ability to terrorize.

#### **NEW Edition of Inspire**

Source: Homeland Security-FBI Joint Intelligence Bulletin

On 18 July 2011, AQAP released the sixth edition of its English-language magazine. Inspire. which provides detailed instructions for the production of the peroxide-based explosive peroxide-better acetone known triacetone as triperoxide (TATP) — but lacks explicit target AQAP suggestions. memorializes the death of



Usama bin Ladin, including an article by former Charlotte, North Carolina resident Samir Khan. The magazine also describes AQAP's activities related to ongoing political unrest in Yemen, with a special tribute to the recent deaths of several AQAP members. Unlike all previous editions of *Inspire*, the magazine does not include any articles written by Anwar al-Aulaqi; however, the magazine provides an advertisement — included in the previous edition—inviting readers to ex-

mail questions to be answered in an up-coming video interview with Aulaqi.

The sixth edition of *Inspire* provides a one page article encouraging individual violent acts; however, the magazine lacks specific guidance, such operational as target suggestions and operational security measures. Additionally, Inspire's latest "Open Source Jihad" section - featuring a picture of the Sydney Opera House - provides readers with step-by-step instructions for producing the explosive TATP, which is highly volatile and dangerous to make and store.

The "Open Source Jihad" instructions for making TATP include suggested locations for purchasing the ingredients, photographs illustrating each step of production, and safety precautions.

In its third installment of "Training with the AK," *Inspire* offers illustrations of individual firing stances for use in assaults.

# Study finds Somali piracy could cost global economy \$12 billion

#### **By Jeffrey Gettleman**

Source:http://www.businessdailyafrica.com/Study+finds+Somali+piracy+could+cost+global+economy++ 12+billion/-/539546/1217320/-/jrq8qt/-/

A pirate at the coastline of Somalia. Political instability and civil strife in the country have spurred piracy in the Indian Ocean into a global problem. AFP



Twenty years ago, when the government of Somalia collapsed, few imagined that the country's ongoing state of lawlessness would eventually spawn piracy on such a scale that the security of the western Indian Ocean region could be threatened.

At first, many assumed that pirate attacks on passing ships could be quickly stifled. But the problem has grown into a global malady that so far has warranted seven United Nations resolutions, one of which authorised "all necessary means to repress piracy and armed robbery at sea".

According to the UN's International Maritime Organisation (IMO), the problem is a global

one, with 276 acts of piracy or armed robbery against ships reported worldwide in 2010. With failed attempts added, the total climbed to 489, a 20 per cent increase from 2009. Although the South China Sea suffered the most attacks, piracy off East Africa, much of it carried out from Somalia, came in second.

Looking only at attacks in international waters, East Africa was well in the lead in 2010, reports the IMO. The only lives lost that year were during East African attacks, while the number of crew members taken hostage there, usually for ransom, reached 629, far higher than anywhere else. According to the International Maritime Bureau, a piracy reporting centre.

based in Malaysia, 54 crew and passengers have been killed worldwide since 2006.

The economic losses are also enormous. The US-based NGO One Earth Future Foundation, in a recent study on naval piracy, estimated that Somali pirates extorted some \$177 million in ransom in 2009 and \$238 million the following year. Including the costs of higher insurance premiums, re-routing ships, antipiracy security and the impact on regional economies, the total annual costs may range between \$7 billion and \$12 billion, the study finds.

Some arrested Somali pirates and senior officials have sought to justify the explosion of piracy off East Africa by citing illicit activities by foreign vessels off the Somali coast. Somali fishermen have long complained that foreign ships have been hurting their livelihoods by over fishing nearby waters, often with large illegal nets. Some have also claimed that toxic wastes have been dumped in the Indian Ocean. In 2008, the UN Secretary-General's then special representative to Somalia, Ahmedou Ould Abdalla, said: "I am convinced there is dumping of solid waste, chemicals and probably nuclear waste. There is no government (in Somalia) and there are few people with high moral ground." Others argue, however, that there is little evidence to substantiate such views.

In any case, key figures within Somalia's Transitional Federal Government strongly believe there is a connection. "If the international community wants to limit acts of piracy," says Deputy Premier Abdulrahman Adan Ibrahim Ibbi, "it has to help Somalis keep illegal foreign fishing and toxic waste dumping away from their coasts."



British Royal Marines intercept a Somali pirate vessel in the Gulf of Aden on June 2, 2009. Alex Cave-Royal Navy/AP

Whatever the factors that have contributed to Somali piracy, prompt action is needed to counter pirate activities, argue regional government officials, fishing industry executives and shippers.

President James Alix Michel of the Seychelles declared in November 2010 that piracy is "the greatest threat that currently exists to fisheries, trade and development in our region. The

scourge of piracy is hijacking not only our economy — but the whole of the Indian Ocean."

Two months later, East African transport ministers urged insurance firms to discourage the payment of ransoms, so as to reduce one of the main incentives for piracy and slow down the steady rise in shipping insurance costs.

Courts in Kenya and the Seychelles are actively prosecuting pirates who have been captured. According to the UN Office on Drugs and Crime, Kenya, the Seychelles and the semi-autonomous region of Puntland in Somalia have the highest number of convicted pirates in the world. As of April, Kenya and the Seychelles were holding 177 pirates.

"Kenya has had a strong tradition of a solid Commonwealth legal system," notes Prof David Crane of Syracuse University in the US. "There is a capacity and certainly they have an ability to try pirates."

Yet governments in the region have very limited resources, whether for prosecuting suspected pirates or trying to safeguard regional waters with tiny national navies. "We are doing more than our part," notes President Michel. "Piracy is exploiting the weaknesses that exist in global governance. It exists, not only because of the dire state of Somalia, but also because of the inaction of the international community."

#### Sharing the burden

Andrew J Shapiro, the US assistant secretary for political and military affairs, agrees that African countries need more support, given the complexity of the challenge. "Prosecuting pirates can be an incredibly complex proposition in today's globalised world," he said in a paper on anti-piracy policy presented last year to an American Law Review symposium. "The realities of international shipping and global commerce are such that in any given piracy case you could have suspected Somali pirates intercepted and apprehended by a British naval vessel after trying to attack a Liberian-flagged ship, owned by a Canadian company, crewed by Ukrainians, Indians, and Filipinos, with a Russian captain and carrying cargo owned by a Turkish company, en route for delivery to a company in Dubai. And the

case could be taking place in a courtroom in yet another country, like Kenya or the Seychelles, which are both currently prosecuting piracy cases. The logistic and diplomatic challenges presented by such a scenario are immense."

Referring specifically to Kenya and the Seychelles, Mr Shapiro continued, "The burden currently shouldered by these countries must be shared more broadly both within and beyond the piracy-affected region. The cost of this crime is borne globally. The cost of combating and defeating it should likewise be borne by many states in all corners of the world." Both Kenya and the Seychelles have signed pacts with the European Union (EU) and the US to try suspected Somali pirates captured elsewhere in return for financial and security assistance.

The US, EU and others have also stepped forward with aggressive counter-piracy naval operations. These include the US-led Combined Task Force and the EU Naval Force Somalia (EUNAVFOR). "My orders are clear," says Rear Admiral Juan Rodriguez, the EUNAVFOR force commander, "to protect vulnerable shipping, deter and prevent acts of piracy, protect vessels of the World Food Programme . . . and the African Union Mission in Somalia."

To better co-ordinate these and other initiatives, a Contact Group on Piracy off the Coast of Somalia has also been established. It brings together some 60 countries, as well as the UN, IMO, North Atlantic Treaty Organisation and African Union.

Ultimately, whatever measures are taken to contain Somali piracy, long-term solutions must address the source of the problem: the political instability and ongoing warfare within Somalia itself.

#### 1000 potential terrorists in Germany

Source: http://www.thelocal.de/national/20110905-37393.html

"We have almost 1,000 people who could be described as possible Islamist terrorists," he told the *Bild* daily, adding that 128 could be considered 'dangerous" and capable of committing attacks.

He said that around 20 of those had received training in camps associated with terror groups and that these individuals were under surveillance by the country's security services. Friedrich added that he thought there was little chance of a repetition of the scale of the terror attack on the United States on September 11, 2001 that brought down the twin towers of New York's World Trade Center. "We dispose of a wide range of modern security."

methods and we are investigating at the very heart of extremist networks," he said. The al-Qaida network, blamed for the New York attacks, has been diminished by the



recent death of its leader Osama bin Laden but it still represented a threat, he added. However, Friedrich estimated that the major danger was posed by individuals acting alone because they are more difficult to identify and track. He was speaking after the opening in Germany last week of the trial of a 21-year-old man from Kosovo who said he was acting alone under the influence of Islamist propaganda when he killed two US soldiers who were heading to Afghanistan by way of Germany in March.

In her weekly address on Saturday, German Chancellor Angela Merkel said that the fight against terrorism has still to be won a decade on from the 9/11 attacks and defended Germany's unpopular participation in the Afghan conflict Saturday. "Osama bin Laden is dead, but terrorism has not yet been defeated," Merkel said.

She also defended Germany's military role in the conflict in Afghanistan where bin Laden and other al-Qaida leaders were based at the time of the organization's attacks on September 11. 2001. "We must be prepared to fight" to defend democracy, Merkel said, adding that Germany would continue the fight against terrorism alongside its allies.

Germany forms the third-largest contingent of foreign troops in Afghanistan, with some 5,400 soldiers in the north under NATO command, despite polls showing a strong majority of the public opposed to its participation.

The German parliament approved a 12month extension of the unpopular Afghanistan mission in January, but with the proviso for the first time that troops start coming home from the end of 2011 if security allows. erkel also welcomed the wave of popular revolts against Arab regimes and said they were proof that "throughout the world people are fighting for freedom and want to build democracy". "Freedom and democracy are the best answers to terrorism and threats," she said.



Welcome to iReport, where people take part in the news with CNN. Your voice, together with other iReporters, helps shape how and what CNN covers every day. *Click on logo* 

#### Jihadists in Syria: Myth or Reality?

By Murad Batal al-Shishani Source: http://www.jamestown.org

In a speech on June 20, Syrian president Bashir al-Assad identified three components of the unrest in his country: citizens with legitimate grievances and needs that must be addressed; criminal elements; and "radicals" seeking to destabilise the country. He accused external forces, outlaws, and radicals of exploiting the "movement seeking legitimate reforms" (BBC Arabic, June 20).

Since February 2011, Syria has witnessed a series of demonstrations and protests demanding the ouster of the president Bashir al-Assad and his family and an end to the rule of the Ba'ath party. The protestors insist on the peaceful nature of their political movement, but in order to justify its violent reaction against them the Syrian regime claims that they are confronting "Takfiri-Salafi armed groups" and "outlaw gangsters."

When Bashir's father Hafiz Assad (1930-2000) clashed with the Muslim Brotherhood during his four-decade rule, he applied similar descriptions for his opponents. In a speech aired on Damascus Radio on June 30, 1979, the late Syrian president said:

"They [the Muslim Brotherhood] have exploited the atmosphere of freedom in order to tempt some young people into committing crimes and to cause [them] to become enemies of Islam. We cannot be lenient with this group, which has committed various acts of murder and one of the most odious massacres ever known in the history of Islam." [1]

#### **Democratic Protests**

Both presidents accused "extremism", but the historical contexts are different; in the late 1970s and the early 1980s there was an armed opposition to Syrian regime and the latter responded by using disproportionate measures of violence, causing the death of tens of thousands of people, most of them civilians. Currently, although the Syrian regime is confronted by peaceful demonstrations inspired by the success of revolutions in Egypt and Tunisia, it has responded in a fashion similar to the Hafiz Assad's crackdown on Islamists in the early 1980s, killing more than 2000 civilians since the uprising began six months ago (*Guardian*, August 8).

According to a report based on the testimony of Syrian opposition figures and prepared by the Henry Jackson Society (a London-based association devoted to democratization), the Syrian opposition is a democratic-leaning movement in which "the Islamist quotient among the opposition is very low." [2] Al-Qaeda leader Dr. Ayman al-Zawahiri indirectly confirmed the absence of jihadis from the Syrian scene when he addressed a video message to Syrian protestors saying:

"Our brothers and fellow Muslims of the Sham [Levant], the land of Ribat [steeds of war] and jihad, Allah knows that if it weren't for the raging war with the New Crusades in which we are engaged, and were it not for these borders restrictions penned by Sykes and Picot and sanctified by our rulers, my brothers and I would be at your side today, in your midst defending you with our necks and chests... but we are consoled by the fact that Sham, the land of Islam and martyrdom, enough mujahideen has for themselves as well as others." [3]

While all indicators show that no "Takfiri-Salafi armed groups" are leading the democratic protests in Syria, it seems that the Syrian regime seeking to tailor a message to the West, which seems to be willing to listen to Arab regimes once the spectre of "Jihadism" is raised. However, the violence that the regime is using against protestors might inadvertently lead to radicalization and the emergence of new jihadists as well as provoking existing Syrian jihadists, pushing them out into the streets in revolt.

#### **Syrian Jihadists**

The American invasion of Iraq in 2003 played a major role in increasing the numbers of Syrian jihadis. With the Syrian government turning a blind eye, regions bordering Iraq, like the Bou Kamal area, became hubs for facilitating the entry of jihadis to Iraq to fight the Americans. Abu Mus'ab al-Zarqawi, then the leader of al-Qaeda in Iraq, was also very keen to create the Levant branch of al-Qaeda, hence he was relying on jihadists from the region.

Since then the number of Syrian jihadists has increased. For instance, according to figures compiled by the author, Syrians formed a high proportion of the Salafi-Jihadists in Iraq, coming in second place by nationality with 13% of the Arab volunteers in Iraq. [4]

It seems that the activity of the Syrian Salafi-Jihadists was not limited to Iraq and Syria. They also formed a high proportion of jihadists acting on Lebanese soil before and during the confrontations at the Nahr al-Bared refugee camp between the Lebanese authorities and

militant Islamists in 2007. Syrians formed about 13% of those jihadists, after the Saudis with 16%, Palestinians from the refugee camps with 31%, and Lebanese with 33%. Seven per cent came from other sources. [5]

The increasing number of Syrian jihadists is also combined with the production of thousands of pages of literature theorizing a confrontation with the Syrian Alawite regime. The most well-known writings in this context are those of Abu Musa'b al-Suri (a.k.a. Mustafa bin Abd al-Qadir Sitt Maryam Nasr, currently believed to be imprisoned in Syria after rendition by the United States).

Al-Suri wrote several books on jihad in Syria and his vision of the Levant region, and Syria in particular, based on two levels: first, an intellectual theorizing, and at the second level, a focus on strategies for a revolution or confrontation with the Syrian regime, which he sees as a *kafir* regime representing "Nusayris" (a pejorative term for Alawites) and Ba'athists. [6]

Following the death of Hafiz al-Assad, al-Suri wrote a book entitled Ahl as-Sunna fi'l-Sham fi Muwajihat al-Nusayria wa'l-Salibeen wa'l-Yahoud (The Sunni People in the Levant in the Face of Nasiriyah, Crusaders and Jews." Al-Suri focuses on two fundamental issues in this work: the "Nusayri" sect and its unjust dominion in Syria and the Syrian state apparatus in its entirety, which, according to al-Suri, is supported by the West to establish peace with Israel. Al-Suri sees a Sunni revolution in Syria as a strategic solution: "We must highlight the basic identity of this confrontation with the Alawi Nusavris, focusing the axis of confrontation towards the correct key to this jihadi conflict between truth and falsehood, [which] is the Sunnis in the face of the Alawi Nasiriyah."

Another well-known jihadi writer, Husain Bin Mahmoud, wrote a March 26 article entitled "Demashq: Qa'dat a-Jihad fi al-Ard" (Damascus: the Jihad Base on the Earth), in which he presented several *hadiths* of the Prophet Muhammad that emphasize the qualities of the Levant for jihadists, being the "land of faith and science," the home of "the best soldiers on earth," and "the best place to migrate to." [7]

Stressing the sectarian understanding of the situation in Syria according to the jihadists' perspective, Bin Mahmoud claims 80% of the

people in Syria are Muslims who are being repressed by a "non-Muslim" Alawite minority and asks how a "despicable, humiliated minority became superiors of the best soldiers on the earth?" In answering himself, Bin Mahmoud says that the people of the Levant were humiliated when "they replaced the banner of jihad with [the banner of] national resistance, and replaced the identity of Islam with nationalism, and the doctrine of Islam with Ba'athism and socialism."

Like most jihadists tackling the Syrian issue, Bin Mahmoud expects the people of Syria to have a role in jihad:

"When the people of the Levant come back to the righteous, and the sound of bullets [is] exalted, and young people shout in the squares, 'God is great,' and the voices of minarets start to call for jihad, then I [will] preach the gospel of Muslims in the East and the West [that] infidels will be destroyed...and then woe to the infidels and its people from the soldiers of al-Sham."

#### Conclusion

Obviously, al-Qaeda and affiliated Salafi-Jihadist groups have an ideological and geopolitical perspective towards Syria, but their project is based on promoting a sectarian division inside Syria that is at odds with the Syrian protestors' ambition of having a post-Assad democratic state. This has prevented the jihadists from exerting political influence during the on-going crisis despite the allegations of the regime.

However, the violence that the regime is using to deal with protestors could serve as a source of radicalization that could activate the jihadists inside the country. If this happened, the Assad regime would face a political and security catastrophe by having to deal with "real" jihadists ready to engage the regime with violence.

By their peaceful political activity, the young protestors in Syria are building a barrier to prevent Salafi-Jihadists from making inroads into the Arab Spring. Meanwhile, the government is paving a way for their entry by its violent repression of a peaceful opposition movement.

474



#### Notes:

1. Quoted in Nikolaos van Dam, *The Struggle For Power in Syrian: Politics and Society Under Asad and the Ba'th Party*, I. B. Tauris, 1996, p.95.

2. Michael Weiss, Hannah Stuart and Samuel Hunter, *The Syrian Opposition: Political analysis with original testimony from key figures*, Henry Jackson Society, London, 2011 http://www.henryjacksonsociety.org/cms/harriercollectionitems /SyrianOpposition.pdf.

3. Al-Zawahri video message entitled *Ei'zul Shariq Awaloh Demashq* (the Glory of the East Begins with Damascus), disseminated on jihadist web forums on July 27. Downloaded from: http://aljahad.com/vb/showthread.php?t=9054

4. The Saudis came in first with 53%. See Terrorism Monitor, December 2, 2005.

5. Figures compiled by the author from open sources.

6. The term "Nusayri" refers to followers of Abu Shu'ayb Muhammad ibn Nusayr (d. 863 AD).

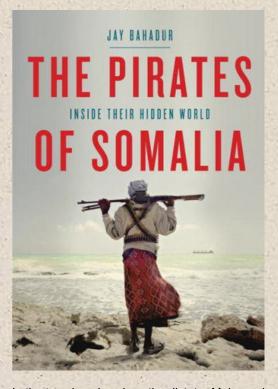
7. http://muslm.net/vb/showthread.php?t=446295

Murad Batal al-Shishani is an Islamic groups and terrorism issues analyst based in London. He is a specialist on Islamic Movements in Chechnya and in the Middle East. He is a regular contributor to several publications in both Arabic and English. He is also author of the book "The Islamic Movement in Chechnya and the Chechen-Russian Conflict 1990-2000", Amman, 2001 (in Arabic), and "Iraqi Resistance: National Liberation vs. Terrorism: A Quantitative Study," November 2005 Iraqi Studies Series, Issue 5, Gulf Research Center-Dubai.

#### Inside the world of piracy

#### By J. Peter Pham

Source:http://www.miamiherald.com/2011/08/21/2366368/inside-the-world-of-piracy.html#ixzz1XfQvG dHu



In the two decades since the dictator Mohamed Siad Barre ignominiously fled Mogadishu in 1991, leaving behind a ruined capital in the throes of uncontrolled street violence, Somalia has topped lists of the world's failed states, stubbornly resisting no fewer than 14 attempts to reconstitute a central government. The latest effort is limping to the expiration of its mandate next month, its senior officials having accomplished little more than stealing an astonishing 96 percent of the \$76 million they received in direct assistance from foreign donors.

The Pirates of Somalia: Inside Their Hidden World. Jay Bahadur. Pantheon. 300 pages. \$26.95.

The only sector in the country that has flourished has been the maritime piracy for which Somalia has become a byword. Despite the deployment of naval vessels from about two dozen nations, the first six months of 2011 saw the number of attacks by Somali pirates more than triple compared with the same period last year.

Motivated by rapidly escalating amounts being paid for the release of captured ships — in 2010, the average ransom was \$5.4 million, up from \$150,000 just five years earlier — the marauders have extended their reach well beyond the coasts of Somalia. They have attacked everything from supertankers to small pleasure craft like the yacht belonging to Scott and Jean Adam of Southern California, who, with two of their friends, earlier this year became the first Americans to be killed by the

pirates since the attacks began in the late 1990s.

Canadian journalist Jay Bahadur's The Pirates of Somalia is the fruit of the research trips that he took between 2009 and 2010 to the northeastern Somali region of Puntland, center of the piracy phenomenon. His choice of Mohamad Farole, son of Abdirahman Mohamed Farole, president of the selfproclaimed Puntland state of Somalia, as his sponsor had significant impacts, positive and negative, on his investigation.

Endowed with a perseverance that augurs well for his career, Bahadur secured extended interviews with some of the most notorious kingpins of Somali piracy, including Abdullahi Abshir Boyah and Mohammed Garaad. Chewing khat, the mildly narcotic leaves that are ubiquitous in the region, to fit in — he notes that it is "an incredible interviewing tool; it rendered my interviewees relaxed and talkative, with a compelling urge to express themselves" — he also engaged with other actors in what has emerged as the dominant local enterprise.

The result is the most creative of the book's 15 chapters, in which he employs the methodology developed by Sudhir Venkatesh and popularized by Steven D. Levitt and Stephen J. Dubner in Freakanomics to examine in detail the costs, risks and returns from the hijacking of the MV Victoria, a German-owned freighter captured in May 2009 while transporting rice to the Saudi Arabian port of Jeddah and held for over two months before a ransom of \$3.2 million was paid. Unfortunately, Bahadur's gratitude to the Faroles may have also gotten the better of his journalistic instincts. While foreign fishing trawlers moved aggressively in the early 1990s into territorial waters left unguarded in the absence of any government of Somalia, the story of Somali piracy as a "justified" response by poor artisanal communities against poaching and toxic-waste dumping by foreigners simply does not hold water. Few of the pirates' targets have been fishing boats, and the mere threat of pirate attacks has for years kept all but a handful of intrepid vessels bearing humanitarian aid away from anywhere near the country's coasts.

Equally unsettling is his rather contradictory defense of Abdirahman Farole, whom Bahadur professes to have "genuinely admired," against credible charges by the U.N. Monitoring Group for Somalia and other authorities that the Puntland president is a beneficiary of the pirates' largesse. The piracy problem cannot be resolved without the cooperation of the regional administration, but such engagement does not mean turning a blind eve to its faults. Bahadur's work would have benefited had he taken the time to study the pioneering work of such internationally recognized authorities as I.M. Lewis and Martin Murphy. Nonetheless, there is no denying that what he lacks in broad perspective or analytical rigor, he makes up with a fascinating narrative that opens a hitherto largely unknown world to a wider audience.

#### J. Peter Pham reviewed this book for The San Francisco Chronicle.

#### Combating the financing of terrorism

Source: http://www.homelandsecuritynewswire.com/combating-financing-terrorism

Terrorist organizations rely on financing and support networks to sustain operations and launch attacks. The U.S. Department of the Treasury has developed a sophisticated and comprehensive approach to identify, disrupt, and deter the funding networks of terrorist organizations

Terrorist organizations rely on financing and support networks to sustain operations and launch attacks. The U.S. Department of the Treasury's Office of Terrorism and Financial Intelligence (TFI) says it has developed a sophisticated and comprehensive approach — including intelligence analysis, sanctions administration and enforcement, financial regulatory action, policy expertise, and outreach to the international community and financial sector — aggressively to identify, disrupt, and deter the funding networks of terrorist organizations. Since 9/11, efforts to counter terrorist financing have played an increasingly critical role in our bracket

counterterrorism strategy. The establishment and growth of TFI since 2004 has strengthened and integrated various authorities in their pursuit of a comprehensive approach to countering terrorist financing.

## Among TFI's activities, programs, and capabilities:

— Intelligence analysis: Established in 2004, the Office of Intelligence and Analysis (OIA) remains the only full-fledged intelligence office in any finance ministry in the world. OIA serves Treasury's specialized intelligence needs, providing analytic products tailored to TFI's mission and Treasury's authorities.

OIA makes intelligence actionable by supporting designations of terrorists, weapons proliferators, and drug traffickers and by providing information to support Treasury's outreach to foreign partners. OIA also serves as a unique and valuable source of information to the Intelligence Community (IC), providing economic analysis, intelligence analysis, and Treasury intelligence information reports to support the IC's needs.

— *Targeted actions:* Treasury has numerous authorities to take targeted action against terrorists, weapons proliferators, narcotics traffickers and their supporters, and isolate them from the U.S. financial and commercial systems. These domestic authorities include Executive Order 13224 (terrorism), Executive Order 13382 (proliferators) and the Foreign Narcotics Kingpin Designation Act (narcotics traffickers), among others.

*— Bilateral engagement.* Treasury continues to engage with key foreign governments to disrupt and dismantle external funding sources to extremists, including through information sharing and coordinated enforcement actions. Enhanced bilateral engagement with Saudi Arabia and other partners in the region, along with comprehensive private sector outreach has yielded real action, including arrests and prosecutions of terrorist financiers and facilitators and more robust controls on funding streams emanating from those countries to extremists in Afghanistan and Pakistan.

— Attacking the finances of terrorists in Afghanistan and Pakistan. Denying the Taliban and other terrorist groups in Afghanistan and Pakistan access to funds has long been a priority within TFI. Treasury has intensified its efforts in this arena over the past year as part of the President's enhanced strategic focus in this critical region. Our approach is grounded in efforts to disrupt and dismantle illicit financial networks and to build domestic capacities within Afghanistan, all designed to undermine the financial networks of illicit actors and safeguard the nascent, but growing Afghan financial sector. Treasury staff in Washington and on the ground in Afghanistan, Pakistan and the Gulf are working with others to aggressively attack the finances of the Taliban, al Qaeda and other terrorist groups operating in the region.

- Threat Finance Cells: Treasury has helped pioneer a novel approach to attacking illicit financial networks - the Threat Finance Cell by providing threat finance expertise and actionable intelligence to U.S. civilian and military leaders. First developed in Iraq under Treasury and Defense Department coleadership, the Afghan Threat Finance Cell (ATFC) seeks to identify and disrupt financial networks related to terrorism, the Taliban, narcotics trafficking and corruption. Led by the Drug Enforcement Agency with Treasury serving as co-deputy, nearly sixty ATFC personnel are embedded with military commands across Afghanistan to improve the targeting of the insurgents' financial structure. Specially-vetted Afghan authorities have also partnered with the ATFC on raids of hawalas suspected of illicit financial activities, including insurgent finance, narcotics trafficking and corruption. This cooperation has resulted in the collection of tens of thousands of financial documents.

*— Expanded Treasury footprint in key regions.* Since 2005, Treasury has established Treasury Attaché offices in Abu Dhabi, Jerusalem, Riyadh, Islamabad, and Kabul.

## Combating the financing of terrorism and illicit finance

- Enhancing transparency in the financial system:TFI oversees the administration of regulations requiring financial services providers to collect, maintain and report information that supports law enforcement investigations and helps to deter the financing of terrorism and other illicit activities. Treasury's efforts, including at the 36-member promote Financial Action Task Force, international standards that enhance the transparency of the international financial system so that illicit financing networks are more susceptible to detection and disruption.

— Developing and applying targeted economic and financial measures: TFI works in collaboration with other federal agencies and the international community to develop and apply a range of targeted economic sanctions and financial measures to identify and disrupt financing networks of organizations including al Qaeda core, al Qaeda affiliates, the Taliban and other terrorist organizations.

— Fostering a global approach to combat terrorist financing. Bilateral and multilateral engagement amplifies Treasury's efforts by ensuring a collaborative and cooperative approach in achieving two key objectives: combating the sources of terrorist financing and building the systemic capacities of countries around the world to protect against illicit finance.

- Engaging in comprehensive private sector outreach: The private sector is an ally in combating terrorist financing. TFI's outreach aims to help facilitate a better understanding of terrorist financing activities and risks, promote the development and implementation of terrorist financing risk mitigation and enhance financial institutions' compliance with efforts to combat money laundering and the financing of terrorism.

— Interagency coordination: Implementing an effective counterterrorist financing strategy requires the involvement of different USG agencies, each of which brings specific expertise to the

expensive to the effort. Agencies involved include those charged with collecting information, analyzing information, engaging with foreign counterparts,



developing international standards, and implementing financial sanctions against targets unique to each agency's national security role. The USG has a strong infrastructure in place to coordinate these efforts, with a variety of mechanisms to coordinate U.S. counterterrorism financing initiatives.

## Parking attendants part of U.S. anti-terrorism effort

Source: http://www.homelandsecuritynewswire.com/parking-attendants-part-us-anti-terrorism-effort

More than 7,000 parking professionals have been trained in the First Observer parkingspecific program developed by the International Parking Institute with the DHS and the Transportation Security Administration.

The parking attendant who waves you into the parking garage or hands you a parking stub is increasingly likely to be a foot soldier in the war on terrorism thanks to a program launched just over one year ago by the International Parking Institute (IPI), the world's largest association of parking professionals and the parking industry. "Terrorists can use parked cars or trucks to carry, conceal or serve as bombs. Parked vehicles were involved in the bombing of the World Trade Center terrorist attack, the Oklahoma City bombing, and the more recent attempted bombing in Times Square," explains Shawn Conrad, IPI's executive director. "Parking professionals are truly on the front lines of counter-terrorism and we take that role very seriously."

To date, more than 7,000 parking First Observers have been certified as part of a parking-specific program developed by the International Parking Institute with DHS and the Transportation Security Administration (TSA). According to Conrad, that number is growing rapidly as more local government officials, universities, airports, sports venues, commercial parking companies and other public and private organizations mandate that their parking personnel be certified in counterterrorism awareness.

The parking-specific module of the First Observer arms parking professionals with the skills they need to address five critical security areas: on-street, surface lots, garages/decks, special events, and shuttle operations. It enables them to identify a potential threat, provides background on different terrorist groups and their patterns of operation, gives an overview of weapons, and details case studies of terror situations. IPI says that First Observers build the skills to report potential

situations using a concise, accurate and simple communications process.

First Observer is a national security and safety awareness program operated under a cooperative agreement with the Department of Homeland Security (DHS) and the Transportation Security Administration. Its mission is to enhance and promote through

**America's Next 12 Terror Threats** 

awareness our ability to protect our infrastructure from risks associated with terrorism.

William Arrington, general manager, Highway and Motor Carrier Division at TSA agrees: "Training thousands of parking professionals to serve as 'eyes and ears' within parking facilities is helping to keep our communities safe."

Source: http://www.thedailybeast.com/articles/2011/09/12/9-11-anniversary-america-s-next-12-terror-threats.html

With solemn grandeur, Americans celebrated a decade of resilience and resolve since the terror attacks of Sept. 11, 2001. And while the celebration of the anniversary—the first since Osama bin Laden's death—may have helped bring closure to some, it can't obscure the looming threat of new attacks as the United States enters its second decade in the war against terror.

Al Qaeda's attacks a decade ago exposed what the 9/11 commission concluded was "failures of imagination" in the security posture of the United States, the inability to envision the tactics that a determined, crafty enemy might use against Americans.

After hundreds of billions of dollars spent on

leadership in recent years, diminishing its operational capacity through relentless drone strikes and captures.

The 10th anniversary of the 9/11 attacks was an obvious date for al Qaeda to strike, but other upcoming dates would provide symbolic significance for the terror group and its sympathizers.

But just as few imagined using jetliners as missiles before 9/11, today there are new and evolving threats to guard against. A Daily Beast review of recent intelligence warnings and federal safety assessments shows the United States isn't fully prepared for some attacks on targets deemed to be high risk—from



homeland security, America clearly is safer and more aware of the threats surrounding it. Likewise, the U.S. military, the CIA, and the FBI have thinned out much of al Qaeda's cyberterror to offshore energy assets. "This array of threats underscores to me the key question posed by bin Laden's death. Does his killing represent the beginning of the end of

the 'war on terrorism,' or is it simply the end of the beginning?" says Clark Ervin, a terrorism expert at the Aspen Institute and the former inspector general of the Department of Homeland Security.

"It is, of course, a very good thing that there's not been a major terror attack in the U.S. since 9/11. But it would as much a 'failure of imagination' to suggest that we cannot be attacked again as it was for pre-9/11 policymakers to assume that we would not be attacked ever."

With little fanfare, FBI and Homeland Security officials have identified in recent bulletins several harrowing tactics that al Qaeda, its spinoff group in Yemen, or other affinity terrorists might use in coming months.

Gleaned from law-enforcement bulletins and terrorism experts, here are some of the threats, tactics, and players that Americans will have to be vigilant against at the dawn of the second decade of the war against terror.

#### 1. Biochemical Attacks

An intelligence report this summer warned that al Qaeda in the Arabian Peninsula was seeking castor beans, the simple but deadly ingredient needed to make a quick and lethal dose of the poison ricin. One concern was that ricin might be used in a subway attack, combined with an explosion to disperse the deadly toxin through the closed tunnels of a subway system. This is a scenario the U.S. military has

long feared, going back to the 1960s and 1970s, and the sarin gas attack in Japan's subways in the 1990s showed its lethality.

#### 2. Radiological Bombs

The so-called dirty bomb has been an obsession of U.S. intelligence and counterterrorism officials for years, dating to 2002, when the FBI suspected an Illinois man named Jose Padilla of plotting such an attack. Padilla was ultimately convicted of other crimes. Still, officials recognize it would be fairly easy for a terror group to collect radiological waste from hospital machines overseas and package it with an explosive.

#### 3. Backpack Bombs in Shopping Malls

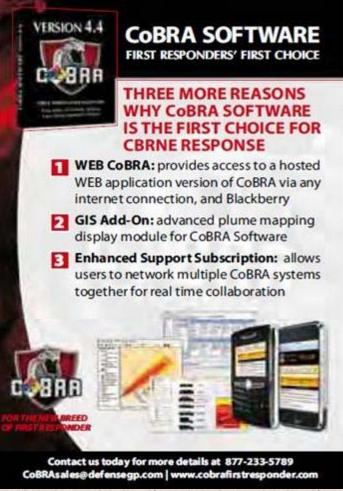
FBI Director Robert Mueller once said in an interview that this was a scenario that kept him up at night. It's a lowscale but tried-and-true approach in other countries, such as Israel and Afghanistan. But it would be new to the United States. And if unleashed in shopping malls, it could create the sort of panic that would shake consumer confidence in an already weak economy.

#### 4. Vehicle Bombs

This is one of the oldest forms of terrorism, but it's still a major threat. In the last few months alone, U.S. intelligence has picked up significant signs that al Qaeda and its allies have been plotting attacks with explosive-laden cars, trucks, and boats. The attack in June on a hotel in Afghanistan frequented by Westerners relied on a

fertilizer bomb embedded in a vehicle similar to that used by Timothy McVeigh in 1995 in Oklahoma City. The Yemen arm of al Qaeda tried such an attack in Times Square less than two years ago, and threat information last week warned of a possible car or truck bomb targeting bridges and tunnels in New York or Washington.

#### 5. Cyberterrorism





This may be one of our Achilles' heels. In the last year, cyberattackers have disrupted or accessed some of the Pentagon's most sensitive documents and computer systems while exposing private information of customers in the business world. Despite billions spent, the country still has relatively few defenses. A Government Accountability Office report last year warned that the U.S. government's efforts to ward off a cyberattack suffered from "overlapping and uncoordinated responsibilities" and a lack of clarity about who is in charge. With the help of a state sponsor well versed in cyberwarfare, a terror group could shut down parts of the U.S. electric grid, cause havoc with financial trades, or disable or hack into sensitive government computer systems at great cost to American security.

#### 6. Small Aircraft Loaded With Explosives

In the days immediately after 9/11, fighter jets roared through the American skies on constant patrol. But those are now a distant memory, and safeguards at rural and small airports are not the same as with major airliners and airports. U.S. officials have long worried about terrorists loading a small airplane with explosives and flying it into a major event with crowds, such as sporting events, concerts, amusement parks, or political debates.

#### 7. Train Bombs

While Amtrak has beefed up security and resources since 9/11, the 7/7 attacks in Britain in 2005 showed how devastating and easy train bombs can be as a tool of terror and death. And unlike the U.S. airlines, trains have fewer security precautions and far more access points for terrorists. Just two years ago, authorities thwarted a suspected bombing plot aimed at New York's subway trains.

#### 8. Energy Assets

When Pakistani officials working with the CIA captured Younis al-Mauritani, al Qaeda's No. 2, earlier this month, they were reminded anew that the terror network has plotted to blow up oil and energy assets ranging from nuclear-power plants and hydroelectric dams to oil-drilling rigs and tankers. Mauritani "was planning to target United States economic interests including gas [and] oil pipelines, power generating dams, and strike [oil tankers] through explosive laden speed boats in international waters," the Pakistani Army reported. Documents found in bin Laden's hideout also affirmed an interest in attacking offshore energy interests. Despite the repeated warning signs, a GAO expert in maritime safety told Congress last month that the government lacks a fully coordinated plan for stopping or responding to such an attack.

#### 9. Al Qaeda in the Arabian Peninsula

This is considered the most dangerous of the regional arms of al Qaeda. Based in Yemen, the group is responsible for two of the biggest foiled attempts at terror attacks: a Nigerian man with a bomb sewn into his underwear who tried to blow up a commercial airliner to Detroit on Christmas Day 2009, and packages with powerful explosives in cargo bound for Chicago in late 2010.

#### 10. Homegrown Terrorists

In the last year the Obama administration has placed a greater emphasis on preventing attacks from Americans inspired by al Qaeda's English-language propaganda on the Internet. In June, John Brennan, the deputy national-security adviser for counterterrorism and homeland security, said his new plan was the "first counterterrorism strategy that focuses on the ability of al Qaeda and its network to inspire people in the United States to attack us from within." One example was the November 2009 rampage of Army Maj. Nidal Malik Hasan at Fort Hood military base. Such small-arms attacks are less lethal than 9/11 by orders of magnitude but are also much harder to prevent—and rely on an alert citizenry. The Department of Homeland Security launched a campaign this year called "See Something, Say Something" to encourage Americans to alert law enforcement when they observe suspicious activity.

#### **11. Symbolic Dates**

The 10th anniversary of the 9/11 attacks was an obvious date for al Qaeda to strike, but other upcoming dates would provide symbolic significance for the terror group and its sympathizers. They include Oct. 7, the 10th anniversary of the invasion of Afghanistan; Dec. 9, the 10th anniversary of the fall of the Taliban government to coalition forces; and May 2, the one-year anniversary of bin Laden's death at the terror group and its sympathizers.

#### 12. Unfinished Business

Al Qaeda has a patience and determination to strike the same targets, a point made clear when the terror group targeted the World Trade Center in New York in 2001 after a less spectacular attack in 1993. There is evidence that al Qaeda has had its eyes on Los Angeles (a target of the failed millennium bomb plot of 1999 and recently mentioned in documents recovered from bin Laden's hideout), Las Vegas (which the 9/11 hijackers once visited), the Sears Tower in Chicago, and the U.S. Capitol building in Washington (supposed to be the target of the 9/11 jetliner that crashed in Pennsylvania).

John Solomon is the editor of news and investigations for Newsweek and The Daily Beast.

### 9/11 legacy: more resilient skyscrapers

Source: http://www.homelandsecuritynewswire.com/911-legacy-more-resilient-skyscrapers

Following the 9/11 attacks on the Twin Towers in New York, many predicted that the age of the skyscraper was over; there has been no slowdown in skyscraper orders, however -- but the skyscrapers being built today are much stronger than the Twin Towers were; new materials, innovative designs, and attention to safety make today's skyscraper much more resilient to man-made and natural disasters. ways, and are now using many new materials, to bolster the strength of these tall buildings and make them more resilient to man-made or natural disasters.

Fox News reports that among these innovations and improvements are:

 The typical cement sidewalk used to be able to resist a couple thousand pounds per square inch. There are now concretes that



Skybridge linking two significant buildings in Detroit // Source: m1dtw.com

The reason architects continue to design skyscrapers, and that builders continue to build them, is the engineers have devised many Very high-strength cement can help a building resist the type of impacts caused on 9/11 by protecting the steel that holds skyscrapers together — the weak point in the attacked towers. In 7 World Trade Center —

the first of the destroyed buildings to be rebuilt, in 2006 — three feet of concrete now surround the steel core.

- Steel has also been getting stronger as scientists have gradually found better alloys.
- Modern skyscrapers are also more likely to use explosion-resistant windows, which are made by using several panes of glass and putting a layer of chemicals in between each. The chemicals bond sheets of glass together, making shattering less likely.
- Bridges linking two or more skyscrapers would allow more avenue for evacuation.
   Fox News notes that skybridges have been used in many post-9/11 skyscrapers, including the 88-story Petronas Towers in

Malaysia. It was also considered among designs for the new World Trade Center.

- Sensitive measuring devices in the building that would take into account the strength of the elements holding it up at any given time. If there were a sudden change, the sensors would communicate that to a computer, and the building could physically shift its weight accordingly.
- Modern skyscrapers include more emergency escapes, protect these escapes with more concrete, and place them strategically.

"The past decade has been the most productive 10 years ever when it comes to tall buildings," a report from the Council on Tall Buildings and Urban Habitat concluded.

## The Evolution of a Pakistani Militant Network

#### By Sean Noonan and Scott Stewart

Source:http://www.stratfor.com/weekly/20110914-evolution-pakistans-militant-networks?utm\_source= freelist-f&utm\_medium=email&utm\_campaign=20110915&utm\_term=sweekly&utm\_content=readmore &elq=44df083a5d1a4c1eae8edc9bfd6b39a0

For many years now, STRATFOR has been carefully following the evolution of "Lashkar-e-Taiba" (LeT), the name of a Pakistan-based iihadist group that was formed in 1990 and existed until about 2001, when it was officially abolished. In subsequent years, however, several major attacks were attributed to LeT, including the November 2008 coordinated assault in Mumbai, India. Two years before that attack we wrote that the group, or at least its remnant networks, were nebulous but still dangerous. This nebulous nature was highlighted in November 2008 when the "Deccan Mujahideen," a previously unknown group, claimed responsibility for the Mumbai attacks.

While the most famous leaders of the LeT networks, Hafiz Mohammad Saeed and Zaki-ur Rehman Lakhvi, are under house arrest and in jail awaiting trial, respectively, LeT still poses a significant threat. It's a threat that comes not so much from LeT as a single jihadist force but LeT as a concept, a banner under which various groups and individuals can gather, coordinate and successfully conduct attacks.

Such is the ongoing evolution of the jihadist movement. And as this movement becomes more diffuse, it is important to look at brandname jihadist groups like LeT, al Qaeda, the Haggani network and Tehrik-e-Taliban Pakistan as loosely affiliated networks more than monolithic entities. With a debate under way between and within these groups over who to target and with major disruptions of their operations by various military and security forces, the need for these groups to work together in order to carry out sensational attacks has become clear. The result is a new, ad hoc template for jihadist operations that is not easily defined and even harder for government leaders to explain to their constituents and reporters to explain to their readers.

Thus, brand names like Lashkar-e-Taiba (which means Army of the Pure) will continue to be used in public discourse while the planning and execution of high-profile attacks grows ever more complex. While the threat posed by these networks to the West and to India may not be strategic, the possibility of disparate though well-trained militants working together and even with organized-crime elements does suggest a continuing tactical threat that is worth examining in more detail.

#### The Network Formerly Known as Lashkar-e-Taiba

The history of the group of militants and preachers who created LeT and their connections with other groups helps us understand how militant groups develop and work together. Markaz al-Dawa wal-Irshad (MDI) and its militant wing, LeT, was founded with the help of transnational militants based in Afghanistan and aided by the Pakistani government. This allowed it to become a financially-independent social-service organization that was able to divert a significant portion of its funding to its militant wing.

The first stirrings of militancy within this network began in 1982, when Zaki-ur Rehman Lakhvi traveled from Punjab, Pakistan, to Paktia, Afghanistan, to fight with Deobandi militant groups. Lakhvi, who is considered to have been the military commander of what was known as LeT and is awaiting trial for his alleged role in the 2008 Mumbai attacks. adheres to an extreme version of the Ahl-e-Hadith (AeH) interpretation of Islam, which is the South Asian version of the Salafist-Wahhabist trend in the Arab world. In the simplest of terms, AeH is more conservative and traditional than the doctrines of most militant groups operating along the Durand Line. Militants there tend to follow an extreme brand of the Deobandi branch of South Asian Sunni Islam, similar to the extreme ideology of al Qaeda's Salafist jihadists.

Lakhvi created his own AeH-inspired militant group in 1984, and a year later two academics, Hafiz Mohammad Saeed and Zafar Igbal, created Jamaat ul-Dawa, an Islamist AeH social organization. Before these groups were formed there was already a major AeH political organization called Jamaat AeH, led by the most well-known Pakistani AeH scholar, the late Allama Ehsan Elahi Zaheer, who was assassinated in Lahore in 1987. His death allowed Saeed and Lakhvi's movement to take off. It is important to note that AeH adherents comprise a very small percentage of Pakistanis and that those following the movement launched by Saeed and Lakhvi represent only a portion of those who ascribe to AeH's ideology.

In 1986, Saeed and Lakhvi joined forces, creating Markaz al-Dawa wal-Irshad (MDI) in Muridke, near Lahore, Pakistan. MDI had 17 founders, including Saeed and Lakhvi as well as transnational militants originally from places like Saudi Arabia and the Palestinian territories. While building facilities in Muridke for social services, MDI also established its first militant training camp in Paktia, then another in Kunar, Afghanistan, in 1987. Throughout the next

three decades, these camps often were operated in cooperation with other militant groups, including al Qaeda.

MDI was established to accomplish two related missions. The first involved peaceful, aboveboard activities like medical care, education, charitable work and proselytizing. Its second and equally important mission was military jihad, which the group considered obligatory for all Muslims. The group first fought in Afghanistan along with Jamaat al-Dawa al-Quran wal-Suna, a hardline Salafist group that shared MDI's ideology. Jamil al-Rahman, the group's leader at the time, provided support to MDI's first militant group and continued to work with MDI until his death in 1987.

The deaths of al-Rahman and Jamaat AeH leader Allama Ehsan Elahi Zaheer in 1987 gave the leaders of the nascent MDI the opportunity to supplant Jamaat al-Dawa al-Quran wal-Suna and Jamaat AeH and grow quickly.

In 1990, the growing MDI officially launched LeT as its militant wing under the command of Lakhvi, while Saeed remained emir of the overall organization. This was when LeT first began to work with other groups operating in Kashmir, since the Soviets had left Afghanistan and many of the foreign mujahideen there were winding down their operations. In 1992, when the Democratic Republic of Afghanistan was finally defeated, many foreign militants who had fought in Afghanistan left to fight in other places like Kashmir. LeT is also known to have sent fighters to Bosnia-Herzegovina and Tajikistan, but Kashmir became the group's primary focus.

MDI/LeT explained its concentration on Kashmir by arguing that it was the closest Muslim territory that was occupied by nonbelievers. Since MDI/LeT was a Punjabi entity, Kashmir was also the most accessible theater of jihad for the group. Due to the group's origin and the history of the region, Saeed and other members also bore personal grudges against India. In the 1990s, MDI/LeT also received substantial support from the Pakistani Inter-Services Intelligence directorate (ISI) and military, which had its own interest in supporting operations in Kashmir. At this point, MDI/LeT developed relations with other groups operating in Kashmir, such as Hizb-ul-Mujahideen, Harkat-ul-Jihad e-Islami and Jaish-e-Mohammad. Unlike these groups, however, MDI/LeT was considered easier

control because its AeH sect of Islam was not very large and did not have the support of the main AeH groups. With Pakistan's support came certain restraints, and many LeT trainees said that as part of their indoctrination into the group they were made to promise never to attack Pakistan.

LeT expanded its targeting beyond Kashmir to the rest of India in 1992, after the destruction of the Babri Masjid mosque during communal rioting in Uttar Pradesh state, and similar unrest in Mumbai and Gujarat. LeT sent Azam Cheema, who Saeed and Igbal knew from their university days, to recruit fighters in India. Indian militants from a group called Tanzim Islahul Muslimeen were recruited into LeT, which staged its first major attack with five coordinated improvised explosive devices (IEDs) on trains in Mumbai and Hyderabad on Dec. 5-6, 1993, the first anniversary of the destruction of the Babri Masjid mosque. These are the first attacks in non-Kashmir India that can be linked to LeT. The group used Tanzim Islahul Muslimeen networks in the 1990s and later developed contacts with the Student Islamic Movement of India and its offshoot militant group the Indian Mujahideen.

The Student Islamic Movement of India/Indian Mujahideen network was useful in recruiting and co-opting operatives, but it is a misconception to think these indigenous Indian groups worked directly for LeT. In some cases, Pakistanis from LeT provided IED training and other expertise to Indian militants who carried out attacks, but these groups, while linked to the LeT network, maintained their autonomy. The most recent attacks in India — Sept. 7 in Delhi and July 13 in Mumbai — probably have direct ties to these networks.

Between 1993 and 1995, LeT received its most substantial state support from Pakistan, which helped build up LeT's military capability by organizing and training its militants and providing weapons, equipment, campaign guidance and border-crossing support in Pakistan-administered Kashmir. LeT operated camps on both sides of the Afghan-Pakistani border as well as in Kashmir, in places like Muzaffarabad.

At the same time, MDI built up a major socialservices network, building schools and hospitals and setting up charitable foundations throughout Pakistan, though centered in Punjab. Its large complex in Muridke included schools, a major hospital and a mosque. Some of its funding came through official Saudi channels while other funding came through non-official channels via Saudi members of MDI such as Abdul Rahman al-Surayhi and Mahmoud Mohammad Ahmed Bahaziq, who reportedly facilitated much of the funding to establish the original Muridke complex.

As MDI focused on dawah, or the preaching of Islam, it simultaneously developed an infrastructure that was financially selfsustaining. For example, it established Al-Dawah schools throughout Pakistan that charged fees to those who could afford it and it began taxing its adherents. It also became well-known for its charitable activities, placing donation boxes throughout Pakistan. The group developed a reputation as an efficient organization that provides quality social services, and this positive public perception has made it difficult for the Pakistani government to crack down on it.

On July 12, 1999, LeT carried out its first fidayeen, or suicide commando, attack in Kashmir. Such attacks focus on inflicting as much damage as possible before the attackers are killed. Their goal also was to engender as much fear as possible and introduce a new intensity to the conflict there. This attack occurred during the Kargil war, when Pakistani soldiers along with its sponsored militants fought a pitched battle against Indian troops in the Kargil district of Kashmir. This was the height of Pakistani state support for the various militant groups operating in Kashmir, and it was a critical, defining period for the LeT, which shifted its campaign from one focused exclusively on Kashmir to one focused on India as a whole.

State support for LeT and other militant groups declined after the Kargil war but fidayeen attacks continued and began to occur outside of Kashmir. In the late 1990s and into the 2000s, there was much debate within LeT about its targeting. When LeT was constrained operationally in Kashmir by its ISI handlers, some members of the group wanted to conduct attacks in other places. It's unclear at this point which attacks had Pakistani state support and which did not, but the timing of many in relation to the ebb and flow of the Pakistani-Indian political situation indicates Pakistani support and control, even if it came only from factions within the ISI or military. The first LeT attack outside of Kashmir took place on Dec. 22, 2000, against the Red Fort in Delhi.

#### The Post-9/11 Name Game

In the months following 9/11, many Pakistanbased jihadist groups were "banned" by the Pakistani government. They were warned beforehand and moved their funds into physical assets or under different names. LeT claimed that it split with MDI, with new LeT leader Maula Abdul Wahid al-Kashmiri saying the group now was strictly a Kashmiri militant organization. Despite these claims, however, Zaki-ur Rehman Lakhvi was still considered supreme commander. MDI was dissolved and replaced by Jamaat-ul-Dawa, the original name used by Saeed and Iqbal's group. Notably, both al-Kashmiri and Lakhvi were also part of Jamaat-ul-Dawa executive the board. indicating that close ties remained between the two aroups.

In January 2002, LeT was declared illegal, and the Pakistani government began to use the word "defunct" to describe it. In reality it wasn't defunct; it had begun merely operating under different names. The group's capability to carry out attacks was temporarily limited, probably on orders from the Pakistani government through Jamaat-ul-Dawa's leadership.

At this point, LeT's various factions began to split and re-network in various ways. For example, Abdur Rehman Syed, a senior operational planner involved in David Headley's surveillance of Mumbai targets, left LeT around 2004. As a major in the Pakistani army he had been ordered to fight fleeing Taliban on the Durand Line in 2001. He refused and joined LeT. In 2004 he began working with Ilvas Kashmiri and Harkat-ul-Jihad e-Islami. Two other senior LeT leaders, former Pakistani Maj. Haroon Ashig and his brother Capt. Kurram Ashiq, had left Pakistan's Special Services Group to join LeT around 2001. By 2003 they had exited the group and were criticizing Lakhvi, the former LeT military commander.

Despite leaving the larger organization, former members of the MDI/LeT still often use the name "Lashkar-e-Taiba" in their public rhetoric when describing their various affiliations, even though they do not consider their new organizations to be offshoots of LeT. The same difficulties observers face in trying to keep track of these spun-off factions has come to haunt the factions themselves, which have a branding problem as they try to raise money or recruit fighters. New names don't have the same power as the well-established LeT brand, and many of the newer organizations continue to use the LeT moniker in some form.

#### **Operating Outside of South Asia**

Organizations and networks that were once part of LeT have demonstrated the capability to carry out insurgent attacks in Afghanistan, small-unit attacks in Kashmir, fidayeen assaults in Kashmir and India and small IED attacks throughout the region. Mumbai in 2008 was the most spectacular attack by an LeT offshoot on an international scale, but to date the network has not demonstrated the capability to conduct complex attacks outside the region. That said, David Headley's surveillance efforts in Denmark and other plots linked to LeT training camps and factions do seem to have been inspired by al Qaeda's transnational jihadist influence.

To date, these operations have failed, but they are worth noting. These transnational LeT-linked plotters include the following:

• The Virginia Jihad Network.

.

- Dhiren Barot (aka Abu Eisa al-Hind), a Muslim convert of Indian origin who grew up in the United Kingdom, was arrested there in 2004 and was accused of a 2004 plot to detonate vehicle-borne improvised explosive devices in underground parking lots and surveilling targets in the United States in 2000-2001 for al Qaeda. He originally learned his craft in LeT training camps in Pakistan.
- David Hicks, an Australian who was in LeT camps in 1999 and studied at one of their madrassas. LeT provided a letter of introduction to al Qaeda, which he joined in January 2001. He was captured in Afghanistan following the U.S.-led invasion.
- Omar Khyam of the United Kingdom, who attended LeT training camps in 2000 before his family brought him home.
- The so-called "Crevice Network," members of which were arrested in 2004 and charged with attempting to build fertilizer-based IEDs in the United Kingdom under the auspices of al Qaeda.
- Willie Brigette, who had been connected to LeT networks in France and was trying to contact.

bombmaker in Australia in order to carry out attacks there when he was arrested in October 2003.

While these cases suggest that the LeT threat persists, they also indicate that the transnational threat posed by those portions of the network focused on attacks outside of South Asia does not appear to be as potent as the attack in Mumbai in 2008. One reason is the Pakistani support offered to those who focus on operations in South Asia and particularly those who target India. Investigations of the Mumbai attack revealed that current or former ISI officers provided a considerable amount of training, operational support and even real-time guidance to the Mumbai attack team.

It is unclear how far up the Pakistani command structure this support goes. The most important point, though, is that Pakistani support in the Mumbai attack provided the group responsible with capabilities that have not been demonstrated by other parts of the network in other plots. In fact, without this element of state support, many transnational plots linked to the LeT network have been forced to rely on the same kind of "Kramer jihadists" in the West that the al Qaeda core has employed in recent years.

However, while these networks have not shown the capability to conduct a spectacular attack since Mumbai, they continue to plan. With both the capability and intention in place. it is probably only a matter of time before they conduct additional attacks in India. The historical signature of LeT attacks has been the use of armed assault tactics — taught originally by the ISI and institutionalized by LeT doctrine - so attacks of this sort can be expected. An attack of this sort outside of South Asia would be a stretch for the groups that make up the post-LeT networks, but the cross-pollination that is occurring among the various jihadist actors in Pakistan could help facilitate planning and even operations if they pool resources. Faced with the full attention of global counterterrorism efforts, such cooperation may be one of the only ways that the transnational jihad can hope to gain any traction, especially as its efforts to foster independent grassroots jihadists have been largely ineffective.

## SGT. DAKOTA L. MEYER, USMC

Source: http://www.marines.mil/community/pages/MedalofHonorSgtDakotaMeyer-Profile.aspx

Sgt. Meyer has been nominated to receive the Medal of Honor for his acts of extraordinary heroism in Afghanistan on 8 September 2009. He was born and raised in Columbia, Kentucky, attended local public schools, and graduated from Green County High School.

In 2006, he enlisted in the United States Marine Corps at a recruiting station in Louisville, Kentucky, and completed his basic training at Parris Island Recruit Training Depot later that year. In 2010, Sgt Meyer completed his active duty commitment and he currently serves in the Individual Ready Reserve of the U.S. Marine Corps Reserve.

He is a school trained sniper and highly skilled Marine infantryman. At the time of his deployment to combat duty in Afghanistan he was serving as a Turret Gunner and Driver. His unit assignment at the time of his heroic acts was with Marine Embedded Training Team 2-8, Regional Corps Advisory Command 3-7 operating in Kunar Province, Afghanistan.

Sgt. Meyer has deployed twice to combat duty, serving in both Iraq and Afghanistan. In 2007,

he deployed to Iraq for OPERATION IRAQI FREEDOM, and during 2009-10, he deployed to Afghanistan for OPERATION ENDURING FREEDOM.

In his civilian professional life, he has completed undergraduate college coursework and he currently works for McDan, Inc. in Kentucky's construction industry.

Sgt. Meyer is a highly decorated Marine combat veteran. His personal awards include a Purple Heart Medal, Navy and Marine Corps Commendation Medal with Combat "V" device for valor, Navy and Marine Corps Achievement Medal, and a Combat Action Ribbon. His other awards and decorations include a Good Conduct Medal, National Defense Service Medal, Afghanistan Campaign Medal with two bronze campaign stars, Irag Campaign Medal with one bronze campaign star, Global War on Terrorism Service Medal, Sea Service Deployment Ribbon, North Atlantic Treaty Organization (NATO) Medal ISAF Afghanistan, and a Rifle Expert Badge (3rd Award) and Pistol Expert Badge (2nd Award).

## **Official Citation**

The President of the United States in the name of The Congress takes pleasure in presenting the MEDAL OF HONOR to

## CORPORAL DAKOTA L. MEYER UNITED STATES MARINE CORPS

#### For service as set forth in the following

For conspicuous gallantry and intrepidity at the risk of his life above and beyond the call of duty while serving with Marine Embedded Training Team 2-8, Regional Corps Advisory Command 3-7, in Kunar Province, Afghanistan, on 8 September 2009. Corporal Meyer maintained security at a patrol rally point while other members of his team moved on foot with two platoons of Afghan National Army and Border Police into the village of Ganjgal for a pre-dawn meeting with village elders. Moving into the village, the patrol was ambushed by



more than 50 enemy fighters firing rocket propelled grenades, mortars, and machine guns from houses and fortified positions on the slopes above. Hearing over the radio that four U.S. team members were cut off, Corporal Meyer seized the initiative. With a fellow Marine driving, Corporal Meyer took the exposed gunner's position in a gun-truck as they drove down the steeply terraced terrain in a daring attempt to disrupt the enemy attack and locate the trapped U.S. team. Disregarding intense enemy fire now

concentrated on their lone vehicle, Corporal Meyer killed a number of enemy fighters with the mounted machine guns and his rifle, some at near point blank range, as he and his driver made three solo trips into the ambush area. During the first two trips, he and his driver evacuated two dozen Afghan soldiers, many of whom were wounded. When one machine gun became inoperable, he directed a return to the rally point to switch to another gun-truck for a third trip into the ambush area where his accurate fire directly supported the remaining U.S. personnel and Afghan soldiers fighting their way out of the ambush. Despite a shrapnel wound to his arm, Corporal Meyer made two more trips into the ambush area in a third guntruck accompanied by four other Afghan vehicles to recover more wounded Afghan soldiers and search for the missing U.S. team members. Still under heavy enemy fire, he dismounted the vehicle on the fifth trip and moved on foot to locate and recover the bodies of his team members. Corporal Meyer's daring initiative and bold fighting spirit throughout the 6-hour battle significantly disrupted the enemy's attack and inspired the members of the combined force to fight on. His unwavering courage and steadfast devotion to his U.S. and Afghan comrades in the face of almost certain death reflected great credit upon himself and upheld the highest traditions of the Marine Corps and the United States Naval Service.

#### Hamas May Resume Suicide Bombings

Source: http://www.israelnationalnews.com/News/News.aspx/147859#.TnLf3ezCnld

A senior counter-terrorism expert warned Tuesday that Hamas is weighing a resumption of suicide bomb attacks against Israeli civilians. Col. Jonathan Fighel (Ret.), a researcher with the Interdisciplinary Center's Institute for Counter-Terrorism, spoke at the Institute's eleventh annual terrorism conference.

"We're seeing more and more Hamas flags in



Hebron. The public atmosphere to Hamas is much more lenient. This allows the creation of operational terror cells. Hamas is taking into consideration the renewal of suicide bomb attacks," Fighel said.

Fighel, who served in various operational and field posts of intelligence and research at the IDF Intelligence Corps, and who has held several command positions in Judea and Samaria, added that Hamas is "gaining influence in the West Bank and acting more freely." Hamas was using the so-called Hamas-Fatah reconciliation agreement as a vehicle to raise its profile in the West Bank, he added. "Hamas's strategy is to replace the PLO as the legitimate representative of the Palestinian people," Fighel said.

The Hamas regime in Gaza is also "looking for duality, to govern while keeping its charter. This is the flexibility it enjoys," it added.

Fighel said Hamas was not deterred by Israel, adding that Israeli government and public opinion had become accustomed to Hamas' shelling of more and more cities with rockets.

At the same time, he noted, Hamas suffered a resounding failure when it tried to cause the Palestinians to enter a third intifada in recent months.

Col. Ronen Cohen, a research associate with the ICT, and a former head of the Terrorism Section of IDF Military Intelligence, said the main goal of Hamas and Hizbullah now is ensuring their own survivability amid regional turbulence.

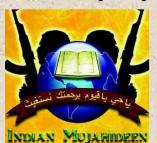
To that end, both have developed arsenals of rockets to pound the Israeli home front, and defensive asymmetrical fighting forces to target IDF forces, he added.

But analysts note tactical flexibility does not indicate strategic or ideological flexibility – or a change in either organization's long-term agenda.

# India has its own indigenous Islamist terrorist threat: US report

Source: http://articles.timesofindia.indiatimes.com/2011-09-14/india/30153983 \_1\_crs-bombings-simi

There is an dangerous growth of indigenous



Islamist terrorism in India despite New Delhi's reluctance to openly acknowledge it, a Congressional report has said, adding leading

such group is Indian Mujahideen. "Despite New Delhi's reluctance to openly acknowledge the

fact, India also has its own indigenous Islamist terrorism threat," the report said.

"The newly emergent 'Indian Mujahideen'(IM) group, widely believed to be an offshoot or pseudonym of the Students Islamic Movement of India (SIMI), has been found complicit in a number of recent bombings, even as government leaders continue to name Pakistan as an abettor of such episodes," the Congressional Research Service (CRS) said.



489

#### Threats and claims

The Indian Mujahideen have sent several emails claiming responsibility for several bombings.

Such an e-mail sent 4 minutes before Ahmedabad blasts refers to Islamic conquerors of India -Ibn-e-Qasim, Ghauri, Ghaznawi.

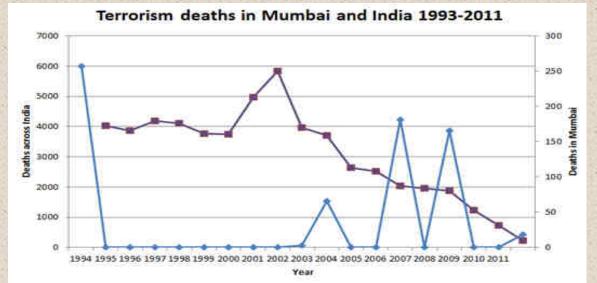
It warns about havoc about to happen in five minutes:

"... Here we are back - the Mujahideen of India - the terrorists on the disbelievers - the radicals of Islam - after our triumphant and successful assault at Jaipur, once again calling you all, who disbelieve in Allah and His Messenger Muhammad to accept Islam and bear witness that there is none to be worshipped except Allah, and that Muhammad is the Messenger of Allah. Accept Islam and save yourselves.

O Hindus! O disbelieving faithless Indians! Haven't you still realized proving your blood to be the cheapest of all mankind! Have you forgotten your history full of subjugation, humiliation, and insult? Or do you want us to repeat it again? Take heed before it is too late!

wait! So ..... Await now .....! Wait only for five minutes from now! .... Wait for the Mujahideen and Fidayeen of Islam and stop them if you can - who will make you feel the terror of Jihad. Feel the havoc cast into your hearts by Allah, the Almighty, face His Dreadful Punishment, and suffer the results of fighting the Muslims and the Mujahideen. Await the anguish, agony, sorrow and pain. Await, only for 5 minutes, to feel the fear of death .... ".

The email was in the form of a pdf document that included several Arabic quotes from the Quran with translation.



#### 

that the falsehood of your 33 crore dirty mud idols and the blasphemy of your deaf, dumb, mute idols are not at all going to save your necks, Insha-Allah, from being slaughtered?

We call you, O Hindus, O enemies of Allah, to take an honest stance with yourselves lest another attack of Ibn-e-Qasim sends shivers down your spines, lest another Ghauri shakes your foundations, and lest another Ghaznawi massacres you, The past emails by Indian Mujahideen include the following:

- Serial blasts in three towns of Uttar Pradesh in November 2007
- 13 May 2008, after the Jaipur blasts email, traced to a Ghaziabad cyber cafe.
- 26 July 2008, four minues before Ahmedabad blasts, email traced Kenneth Haywood's WiFi IP address in Sanpada, Navi Mumbai.
- August 2008, after the press conference held by the Gujarat Police, IP address

traced to WiFi network of Khalsa college in Matunga, central Mumbai.

 13 September 2008, during the Delhi serial blast, IP address traced to WiFi network of Kamran Power Control Pvt Ltd, at 201-202 Eric House, 16th Road, Chembur.

They did not send any e-mail messages claiming responsibility for the serial blasts in Bangalore on 25 July 2008.

#### Indians urged to buy terrorism insurance

Source: http://articles.economictimes.indiatimes.com/2011-09-14/news/30154352\_1\_health-insurance-sanjay-datta-mahavir-chopra

India's Economic Times is urging citizens to consider protecting their interests and purchasing insurance in light of recent terrorist attacks in the country; while there is no terrorism insurance policy, individuals can purchase health insurance as well as life insurance to ensure that family members are protected in the event that a catastrophic accident were to occur; "A terror attack can cause disability or dismemberment or loss of life in addition to the medical expenses that may be incurred for treating the same. A person needs to have both personal accident cover for death and disability and medical expenses cover to provide for both the eventualities," said Sanjay Datta, head of ICICI Lombard's customer service

### St. Andrews University promoting its certificate in terrorism studies

Source:http://www.homelandsecuritynewswire.com/st-andrews-university-promoting-its-certificate-terrorism-studies

The University of St. Andrews is promoting a program leading to a certificate in it terrorism studies. The Scottish university says that individuals whose responsibility it is to protect people, infrastructure, organizations or international and domestic terrorist threats. For many — including police authorities, close protection operatives, the military, government and private sector bodies — the subject of terrorism is so vast and complex that



investments, need to understand the threats, then prepare and implement best practice strategies to reduce the risk and counter educational insight is rarely available to the majority.

The university says that terrorists have grown their ability to target the military and civilians, and security risks are at their highest, so knowledge of this important subject will help prepare any company or organization to counteract and protect against the variety of threats posed by today's multi-faceted terrorist organizations.

This terrorism studies course fills a knowledge gap, enabling participants and organizations to prepare to meet the counter terrorism challenges and risks of



University of Andrews



evolving anti-terrorist techniques and counter the terrorist threat. "Knowing how and why terrorists are radicalized and plot against civilians,

governments, corporations, commercial operations, transport or IT networks makes an unmistakable difference to a nation's or

organization's anti terrorist and security strategies," the university says. "The knowledge you will gain from this unique terrorism course will prove invaluable in countering the ever present threat to security." The Certificate in Terrorism Studies is accessible globally through online e-learning, and can be studied from anywhere — all the student needs is an Internet connection.

The Certificate in Terrorism Studies was established in September 2006 in partnership with IBC Global Academy (part of Informa Plc). The university says that the Center for the Study of Terrorism and Political Violence (CSTPV) at the University of St Andrews was the first transnational counter terrorism online course to provide individuals, military, and police, as well as public and private sector organizations with an understanding of the latest thinking on terrorism and homeland security.





# New Upcoming Events



International Defense and Homeland Security Simulation Workshop (September 12-14; Rome) This workshop will focus on the advances and potential of using modeling and simulation in defense and homeland security applications. It will bring experts together to present and discuss all types of innovation: new concepts, methods,

techniques, and tools. View event website

Emergency Management Policy & Leadership Forum (October 3-7; Austin, TX) This forum of the National Emergency Management Association NEMA will encompass association committee meetings as well as workshops on "State Models for Effective Public-Private Partnerships," "Defining the Current Terrorist Threat," and "Cyber Security," along with presentations on "The Future of the Homeland

### 4<sup>TH</sup> ANNUAL DEFEATING IEDS TRAINING WORKSHOPS & EXHIBITION

Security Enterprise During Fiscal Crisis" and "Lessons to Be Applied From Recent Disasters." View event website

Some of the Key Highlights
> Current and future known USCENTCOM operational requirements

- > The use of UAVs and the Prioritization of ISR assets
- > Tactical & Operations consideration of attacking the Network
- > Use of High Power Electromagnetic Radiation for Remote Detonation of IEDs
- > Designing and delivering of a route proving and clearance capability
- > Developing Multinational Training standards
- > Tactical & Operations of Intelligence Challenges and Failures
- > The use of Biometrics in the fight against IEDs
- > Identifying gaps in the C-IED training and Capability requiremets

> Accelerating the development and fielding of affordable, sustainable and non-traditional capabilities for the warfighter

#### Workshops

During the event, all registered delegates will have full access to 3 Training Workshops:

- 1- Weapons Intelligence Team (WIT) Operations & Planning
- 2- Counter-Suicide Bomber Operations & Planning
- **3- NATO Counter-Insurgency Principles**

National Workshop on 9-1-1 Overload (October 4-5; Washington, DC) The 9-1-1 Industry Alliance is hosting this workshop to address the problem of 9-1-1 systems increasingly experiencing overload during routine emergencies, major weather events, natural disasters, mass shootings, and other incidents. People calling 9-1-1 for help are experiencing busy signals, unanswered calls, or long hold times, and public expectations are not matching the realities of 9-1-1 in these situations. View event website

Technology & Homeland Security Forum (October 5: Niagara Falls, NY) This conference, with over 50 vendors, 7 classrooms with many educational sessions, and over 350 attendees. will address the rapidly changing world of technology and how the homeland security inclusion

is using technology to drive productivity, comply with regulatory requirements, and adapt to converging markets, products, and investors. <u>View event website</u>

**Emergency & Disaster Planning for Colleges, Universities, and K-12 Schools** (October 5-6; Toronto) This event will cover balancing security with privacy, mass notification, emergency response training, lockdown protocols, bill 168, cost-effective budget planning, planning for unlikely emergencies, mental health awareness, cyberbullying, risk assessments, achieving buy-in, sexual assault response systems, and building security. A post-conference workshop will offer hands-on training in using the Internet as an effective tool to monitor and prevent school violence. <u>View event website</u>



**International Conference on Social Informatics** (October 6-8; Singapore) This interdisciplinary venue for researchers from informatics and the social and management sciences is interested in the implications of the influence of such technology on society at large, including its security implications for individuals' privacy and identity, as well as for cyber-infrastructure and homeland security. <u>View event website</u>

(October 11-13; Munich, Germany) This conference, to be held alongside Inter Airport Europe, is organized by the International Association of Emergency Managers for all involved in civil protection and emergency management. The themes of transport, environment, and emergency management as a profession will have links to the aviation sector but will not focus solely on that area of emergency management. The expo pavilion will have the latest technical, academic, and service-oriented emergency management

offerings from the public and private sectors. View event website



(October 11-14; Virginia Beach, VA) This is a multidisciplinary international conference for the exchange of modeling and simulation knowledge, research, and remment and academia One of the tracks is "Defense

technology across industry, government, and academia. One of the tracks is "Defense, Homeland Security & First Responders." <u>View event website</u>



**International Workshop on Updates in Emergency Management** (October 26-27; Suleimaniyah, Iraq) The workshop will address, explore, and exchange information on the state of the art in collaboration enterprises and their modeling and simulation, design and use, applications, and impact. Participation is extended to researchers, designers, educators, and

interested parties in all emergency management disciplines and specialties. <u>View event website</u>

**Emergency Preparedness & Hazmat Response Conference** (October 29–November 2; Pittsburgh) This all-hazards conference for government and industry offers education, training, and networking—meet and mingle with key decision makers in emergency preparedness and prevention. <u>View event website</u>

(October 13; Los Angeles) The Structural Engineers Association of Southern California will host this major earthquake loss reduction summit at the University of Southern California, a precursor to the Great California ShakeOut on October 20. Many building types in Southern California are at risk of significant damage in earthquakes, and this summit will present cost-effective ways to reduce this risk and bring building officials, owners, and engineers together to develop additional solutions. <u>View event website</u>



**Virginia Hazardous Materials Conference and Expo** (October 17-21; Hampton, VA) This event is presented by the Virginia Association of Hazardous Materials Response Specialists in conjunction with the Virginia Department of Emergency Management. This year's theme is "Confronting New Challenges: Are We Ready?" <u>View event website</u>



Join the Carnival

## **CBRNe South American**

### Save the Date!

### 13-14 March 2012, Sheraton Hotel and Resort, Leblon, Rio De Janeiro

South America has had to deal with many regional, social and criminal challenges for decades, but never has there been much of a CBRN threat. With Rio bringing two of the world's largest sporting events into the country – the FIFA Soccer World Cup and the Olympic Games – this is all going to change, as outside terrorist elements start making their plans. CBRNE South America is going to bring some of the brightest and best CBRNE minds from around the world to Rio, to meet with some of the decision makers and opinion formers from all the countries of the region – Brazil, Argentina, Chile, Peru, Venezuela, Colombia.

GOLD SPONSOR CRISTANINI CBRN DECONTAMINATION SYSTEMS

This two day conference and exhibition will be the best chance to learn about the many challenges that the region faces and to learn from those countries that have put on similar high profile sporting and political events. This will be **THE major conference in the region**, a landmark in the sub-continent that will set the agenda for the next ten years.

More information will be available shortly on www.icbrnevents.com

With the support of

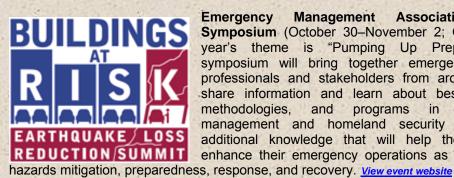


(October 20) Already, 6.8 million people have signed up to participate in this year's ShakeOut. In 2010, more than 7.9 million Californians practiced "Drop, cover, and hold on" to practice how they will protect themselves during earthquakes and to increase their overall preparedness. View event website



View event website

(October 30-November 1, 2011; Seattle) This conference of the Institute of Electrical and Electronics Engineers will gather engineers, technology professionals, academics, scientists. foundations, government and nongovernmental organizations, and individuals engaged in humanitarian work to discuss and develop solutions for present and future needs: health, medical technology, and telemedicine; disaster warning and response; and connectivity and communications technologies for remote locations-among other topics.



Emergency Management Association of Texas Symposium (October 30-November 2; Odessa, TX) This year's theme is "Pumping Up Preparedness!" This symposium will bring together emergency management professionals and stakeholders from around the state to share information and learn about best practices, new methodologies, and programs in the emergency management and homeland security fields and gain additional knowledge that will help them improve and enhance their emergency operations as they relate to all-

2011 National Symposium on Homeland Security and Defense (October 31–November 2: Colorado Springs, CO) The theme of this year's conference is "A 'Whole-of-Society' Approach to Homeland Security and Defense: It's Everybody's Job." This National Homeland Defense Foundation symposium is a public forum where leaders from various sectors of our society can come together to share information, ideas, and plans focused on securing our nation and our liberty. View event website



This conference, hosted by the Integrated Research on **Disaster Risk International** Programme Office and the China Association for Science

and Technology, will provide a platform from which to launch trans-disciplinary research alliances aimed at in-depth, practical disaster risk reduction studies. It will focus on characterization of hazards, vulnerability, and risk; understanding decision making in complex and changing risk contexts; and reducing risk and curbing losses through knowledge-based actions. View event website



(November 1-3; New York) Security Week is an all-in-one megaevent in New York City, organized by the Security Industry Association, that will offer information and business opportunities related to all aspects of the security industry. Existing events-Securing New Ground, Security 500, the Tri-Association Awards

Dinner, and ISC Solutions-for the first time will all work together to provide attendees with new levels of value and convenience. View event website



**National Cyberterrorism Conference** (November 1-3; San Diego) The conference will address the potential threat from terrorists' use of the Internet and technology to conduct or inspire attacks on small-town America and the nation's critical infrastructure as foreign terrorist organizations "increasingly seek to conduct asymmetric attacks on the U.S. from abroad." Foundry, the conference host, hopes to enhance the nation's ability to counter these threats by educating law enforcement, intelligence analysts, critical infrastructure personnel, the military, and policy makers. <u>View event website</u>



**CBRNe Convergence Conference** (November 1-3; Istanbul, Turkey) The theme of this year's conference is "Growing closer, staying distinct: merging civilian and military response to CBRN [chemical, biological, radiological, and nuclear] and IED [improvised explosive device] threats." Civil and military organizations will discuss how their recent attacks, exercises, and research are improving their CBRN defense capability. A pre-conference workshop will discuss wearable protective technology. <u>View event website</u>



#### **Stop Press**

#### Final Day Convergence Exercise Postponed

Due to the impact on the Turkish Government of the June 2011 elections CBRNe Convergence has had to postpone the final day exercise. "We are bitterly disappointed," said Gwyn Winfield, Editor of CBRNe World, "but there is really very little that can be done. With the election in June it leaves very little time - after the

Summer holidays – to plan a quality exercise that will showcase Turkish capability to a level that is of value to all partners. We understand entirely that the focus at this time is, and should be, on the elections and that unless we can put together an exercise that is able to deliver the end objective then it is best left to another time."

The CBRNe Convergence Conference and Exhibition will now finish after the second day of the Conference – the 3rd of November, after the pre-conference workshop on protective garments on November 1st and over 30 expert speakers have presented their best thoughts on CBRNE defence during the conference.



### 22-23 February 2012

Grand Copthorne Waterfront Hotel Singapore

C

C

http://www.smi-online.co.uk/events/overview.asp?is=16&ref=3773

2012

2<sup>nd</sup> CBRN

Asia-Paci

Conferen

**Terror on Trial** (November 3-5; Washington, DC) The theme of this conference sponsored by the Association for the Study of the Middle East and Africa is "Out of the Past, Into the Future: Reflections on the Middle East and Africa." It will feature a keynote address by Barham Salih, Prime Minister of the Kurdistan Region, along with presentations by top policymakers and scholars, roundtable discussions on "Turkey as a Democratic Ally Under the AKP [Party for Justice and Progress]" and "The Saddam Tapes, 1978-2001: The Inner Workings of a Tyrant's Regime," and panel discussions of the latest academic research in Middle Eastern and African studies and related disciplines. <u>View event website</u>



(November 7-8; São Paulo, Brazil) The second Chief Security Officer Roundtable Latin America Summit, sponsored by the American Society for Industrial Security International, will cover critical business and security issues such as public-private collaboration during a crisis, dealing with cultural differences in a global organization,

corporate security's role in preventing internal fraud, protecting executives and their families, and Brazil's security preparations for the World Cup and the Olympic Games. Last year's summit drew more than 100 security executives from around the world. <u>View event website</u>



(November 7-9; San Diego) Border management professionals will come to learn effective practices to secure and protect the nation's borders. They will hear about technology needs and gaps directly from top border security officials, receive an up-to-date overview of 2012 procurement and acquisition strategies, and gain access to

the latest border security technology. The conference and expo are being held in conjunction with UAV West and Maritime Homeland Security West. <u>View event website</u>



(November 11-17; Las Vegas) The International Association of Emergency Managers annual conference provides a forum for current trends and topics, provides information about the latest tools and technology in emergency management and homeland security, and advances the association's committee work. Sessions encourage

stakeholders at all levels of government, the private sector, public health, and related professions to exchange ideas on collaborating to protect lives and property from disaster. <u>View event website</u>



(November 14-16; Phoenix) The Government Security Conference and Expo provides insights, tools, and tactics to anticipate, prepare for, prevent, and respond to terrorism, accidental and natural disasters, and attacks on critical infrastructure. <u>View event website</u>



(November 14-16; Washington, DC) The conference and expo unite the major global shareholders in maritime security and defense to discuss and debate maritime capabilities and concepts, evaluate future and state-of-theart enabling technologies, and develop international partnerships. <u>View event</u> website



Chemical and Biological Defense Science & Technology Conference (November 14-18; Las Vegas) Attendees will be able to examine the best, new, dynamic developments in basic and applied research in the chemical and biological defense

landscape and interact and collaborate with other researchers concerning the medical and physical sciences related to chemical and biological defense. They will also be able to meet Defense Threat Reduction Agency science and technology managers and other members of the chem-bio technologies team. Through keynote, oral, and poster presentations, the conference will address key areas of foundational research and areas of increased focus. <u>View</u>

### MASTERCLASS

### SMi Training Presents...

### CBRN in the Maritime Environment

How to prepare for, protect from and prevent an incident and how to deal with the effects should an incident occur

Thursday December 8th, Central London



#### **Overview:**

CBRN in the Maritime Environment focuses upon the CBRN threat to those that operate in the maritime domain. This exceptional Masterclass will be delivered through a series of presentations and group interaction throughout the day. Neil Hall will be joined by further expert presenters during the masterclass.

#### Who should attend?

This masterclass is aimed at Security Professionals, Transport Operators, Company, Ship & Port Security Officers, Naval & Military Personnel, Police, Fire & Ambulance Emergency Responders and other private and public sector professionals that operate in the maritime domain.

Benefits of attending:

- Gain a thorough understanding of how catastrophic and devastating a CBRN incident in the Maritime Environment could be
- Learn how to protect from and prevent such an attack
- Risk assessment & SOPs
- Be prepared to deal with such an incident, when it occurs

TPACE

Examine existing capabilities

- Identify gaps
- Look at options for development
- Identify priorities
- Improve understanding
- The impact on trade
- Business challenges when managing global
- risk rinited
- The view of the Emergency Services
- Casualty handling
- Media handling
- Protecting Reputation

### Register online at www.smi-online.co.uk/ts01.asp

To attend contact Teri Arri on email tarri@smi-online.co.uk Tel: +44 (0)20 7827 6162 or send your booking form to fax number: +44 (0)20 7827 6163 GROUP DISCOUNTS AVAILABLE





**IEEE Conference on Technologies for Homeland Security** (November 15-17; Waltham, MA) This Institute of Electrical and Electronics Engineers conference will address cybersecurity; attack and disaster preparation, recovery, and response; land and maritime border security; and biometrics, forensics, and physical security. All four areas will cover strategy and threat characterization, concepts of operation, and risk analysis; modeling, simulation, experimentation, and training; and testbeds, standards, and evaluations. <u>View event website</u>

**International Workshop on Innovation, Diversity and Sustainable Development in Areas of Social Vulnerability** (November 17-18; Boston) This workshop organized by the Center for Rebuilding Sustainable Communities After Disasters will discuss strategies for the empowerment of residents in the areas of social vulnerability and the implementation of public policies with a sustainable basis in such areas. <u>View event website</u>



(November 23-24; Coventry, England) Emergency and resilience professionals will discuss multi-agency collaboration, best practices, ideas, and initiatives; learn about the latest equipment and innovations;

network and listen to industry experts; and explore how they can make vital cost-saving efficiencies with equipment and service suppliers. <u>View event website</u>



# **CRISTANINI CBRN** DECONTAMINATION SYSTEMS



CONFORM TO THE QUALITY SYSTEM STANDARD AGAP 2110 and ISO 9001:2008



DEPLOYABLE CBRN ANALYTICAL LABORATORY (STANAG 4632)



DEPLOYABLE BIO LABORATORY CLASS II BIO SECURITY LEVEL



RICERN TRAILER FOR CERN DECONTAMINATION AND DETOXIFICATION



TSON-TACTICAL STEAM DECON MODULE



SCH CERN DECONTAMINATION OF SENSITIVE EQUIPMENT AND SURFACES

## ONLY ONE PERSON ONLY ONE MACHINE ONLY ONE PRODUCT





#### CRISTANINI

37010 RIVOLI - VERONA - ITALY Tel. +39-045-6269400 - Fax +39-045-6269411 cristanini@cristanini.it - www.cristanini.com



DOMAS LARGE SCALE DECONTAMINATION SYSTEM HIGHLY DEPLOYABLE



DDMAS LARGE SCALE DECONTAMINATION SYSTEM DUAL OPERATORS



MOBILE SYSTEM FOR AIRCRAFT DECONTAMINATION



SANUET C 1125 HR CBRN DUAL OPERATOR DECONTAMINATION AND DETOXIFICATION GROUP



**CERN PRODUCTION LINE** 

