Financial Profile of AQ – Madrassah & Terrorism

Collection

CBRNE-TERRORISM Newsletter

Δελτίο ΧΒΡΠΕ-ΤΡΟΜΟΚΡΑΤΙΑΣ

Volume 5 - 2010

- Russian tribute to 911 victims
- Smart surveillance from Israel
- USS Cole: 10 years on
- AQ Brigade 313 goes online
- Poison plot by AQ
- Insect-size HAZMAT detectors
- Anthrax: human/livestock in France
- Nuclear bomb in urban environment
- EMP impact: far and wide
- EOD PPE standards
- Camera-fitted suicide vests
- Counter-IEDs robots
- Tribute to bomb-sniffing dogs
- 3rd generation Smallpox vaccines

TEEM EKAM

US Medal of Honor

www.rieas.gr

CBRNE-Terrorism Newsletter®
Δελτίο ΧΒΡΠΕ-Τρομοκρατίας
Volume 5
(Winter 2010)

Editor
BG (ret) Ioannis Galatas MD, MSc, MC
Consultant in Allergy & Clinical Immunology
Medical CBRN Planner
Senior Terrorism/WMD Analyst

Contact e-mail
igalatas@yahoo.com

DISCLAIMER

The CBRNE-Terrorism Newsletter® is a free online publication for the fellow First Responders
of both the civilian and military relevant fields.
Newsletter is a collection of papers relevant to the stated thematology - relevant sources are provided.
All info provided herein is from open Internet sources.
Full-page products are not paid advertisements; they are just another way to provide information on useful products of interest to First Responders.
Occasional opinions and comments from the Editor do not necessarily represent those of RIEAS.

EDITOR'S CORNER

ISDS-2010 Seminar

From October 28th until November 3rd I had the pleasure to participate at the ISDS-2010 Seminar held in Tel Aviv and Jerusalem, Israel. This very important seminar was organized by International Security and Defense System (ISDS) one the leading security companies in the world. In a week time, participants had the unique chance to meet the living history of counter-terrorism specialists of Israel and chat with colleagues from other countries that came face to face with the enemy – terrorism. Beside this, it was a good opportunity to travel from East to West and from North to South and came to close contact with the people of this beautiful country. The afternoon spent at the Israeli Training Academy and practical training obtained will be remembered for many years. Participating at the 1st Israel Homeland Security International Conference provided the opportunity to have a close look to all Israeli companies activated in this field – and they were too many of them! Finally, the inside visit at the Ben Gurion International Airport was a fantastic opportunity to watch from the inside the security and operational aspects of one of the most secure airports in the world. Thank you Leo Glesser and ISDS Team for the wonderful and most interesting time we spend in your country! – ID

The Guardium unmanned ground vehicle, developed jointly by G-NUIS Unmanned Ground Systems, IAI, and Elbit Systems, and designed to assist the IDF in routine patrols along the Gaza border, has undergone several structural changes in order to provide protection services to busy airports. Such vehicles are already in trial use at Ben Gurion Airport. Among other things, the vehicle is capable of accurately directing attack helicopters to the location of an incident.

ISDS 2010 Seminar

Leadership in Emergency Times:
Strategies, Tactics, and Operations in Homeland Security

Mordechai Rahamim
Matkal Combatant and Sky Marshall responded to the Zurich attack. He was also part of the rescue team for the Sabena case (1972)

Rafi Eitan
Former High Ranking Mossad Officer - Crucial team member in mission to capture Adolf Eichmann (1961)

Amnon Biran
Special Forces Officer, Operation Entebbe Hostage Rescue Mission (1976)

Brig. Gen. (Res.) Relik Shafir
IAF pilot; former commander of the "Tel Nof" Air Force Base. One of the eight pilots that attacked Iraq's Osirak Nuclear Facility (1981)

Shlomo Vider
El Al Flight Steward who defended the flight and subdued attacker during hijacking of EL AL 219 by the Laila Haled and PFLP (1970)

Admiral Carlos Tello,
Head of "Operation Chavin de Huadar" Rescue Mission at the Ambassador's Residence in Lima, Peru (1996-1997)

Prof Oscar Tulio Lizcano
Colombian held in captivity by FARC for nine years until he managed to escape along with guard.

The New World Order

Source: http://www.newgeography.com/content/001786-the-new-world-order

Tribal ties—race, ethnicity, and religion—are becoming more important than borders.
For centuries we have used maps to delineate borders that have been defined by politics. But it may be

time to chuck many of our notions about how humanity organizes itself. Across the world a resurgence of tribal ties is creating more complex global alliances. Where once diplomacy defined borders, now history, race, ethnicity, religion, and culture are dividing humanity into dynamic new groupings.
Broad concepts—green, socialist, or market-capitalist ideology—may animate cosmopolitan elites, but they generally do not motivate most people. Instead, the "tribe" is valued far more than any universal ideology. As the great Arab historian Ibn Khaldun observed: "Only Tribes held together by a group feeling can survive in a desert."
Although tribal connections are as old as history, political upheaval and globalization are magnifying their impact. The world's new contours began to emerge with the end of the Cold War. Maps designating separate blocs aligned to the United States or the Soviet Union were suddenly irrelevant. More recently, the notion of a united Third World has been supplanted by the rise of China and India. And newer concepts like the BRIC nations (Brazil, Russia, India, and China) are undermined by the fact that these countries have vastly different histories and cultures.
The borders of this new world will remain protean, subject to change over time. Some places do not fit easily into wide categories—take that peculiar place called France—so we've defined them as Stand-

Alones. And there are the successors to the great city-states of the Renaissance—places like London and Singapore. What unites them all are ties defined by affinity, not geography.

1. New Hansa

Denmark, Finland, Germany, Netherlands, Norway, Sweden

In the 13th century, an alliance of Northern European towns called the Hanseatic League created what historian Fernand Braudel called a "common civilization created by trading." Today's expanded list of Hansa states share Germanic cultural roots, and they have found their niche by selling high-value goods to developed nations, as well as to burgeoning markets in Russia, China, and India. Widely admired for their generous welfare systems, most of these countries have liberalized their economies in recent years. They account for six of the top eight countries on the Legatum Prosperity Index and boast some of the world's highest savings rates (25 percent or more), as well as impressive levels of employment, education, and technological innovation.

2. The Border Areas

Belgium, Czech Republic, Estonia, Hungary, Iceland, Ireland, Latvia, Lithuania, Poland, Romania, Slovakia, U.K.

These countries are seeking to find their place in the new tribal world. Many of them, including Romania and Belgium, are a cultural mishmash. They can be volatile; Ireland has gone from being a "Celtic tiger" to a financial basket case. In the past, these states were often overrun by the armies of powerful neighbors; in the future, they may be fighting for their autonomy against competing zones of influence.

3. Olive Republics

Bulgaria, Croatia, Greece, Italy, Kosovo, Macedonia, Montenegro, Portugal, Slovenia, Spain

With roots in Greek and Roman antiquity, these lands of olives and wine lag behind their Nordic counterparts in virtually every category: poverty rates are almost twice as high, labor participation is 10 to 20 percent lower. Almost all the Olive Republics—led by Greece, Spain, and Portugal—have huge government debt compared with most Hansa countries. They also have among the lowest birthrates: Italy is vying with Japan to be the country with the world's oldest population.

4. City-States

London

It's a center for finance and media, but London may be best understood as a world-class city in a second-rate country.

Paris

Accounts for nearly 25 percent of France's GDP and is home to many of its global companies. It's not as important as London, but there will always be a market for this most beautiful of cities.

Singapore

In a world increasingly shaped by Asia, its location between the Pacific and Indian oceans may be the best on the planet. With one of the world's great ports, and high levels of income and education, it is a great urban success story.

Tel Aviv

While much of nationalist-religious Israel is a heavily guarded borderland, Tel Aviv is a secular city with a burgeoning economy. It accounts for the majority of Israel's high-tech exports; its per capita income is estimated to be 50 percent above the national average, and four of Israel's nine billionaires live in the city or its suburbs.

5. North American Alliance

Canada, United States

These two countries are joined at the hip in terms of their economies, demographics, and culture, with each easily being the other's largest trade partner. Many pundits see this vast region in the grip of inexorable decline. They're wrong, at least for now. North America boasts many world-class cities, led

by New York; the world's largest high-tech economy; the most agricultural production; and four times as much fresh water per capita as either Europe or Asia.

6. Liberalistas

Chile, Colombia, Costa Rica, Mexico, Peru

These countries are the standard--bearers of democracy and capitalism in Latin America. Still suffering low household income and high poverty rates, they are trying to join the ranks of the fast-growing economies, such as China's. But the notion of breaking with the U.S.—the traditionally dominant economic force in the region—would seem improbable for some of them, notably Mexico, with its close geographic and ethnic ties. Yet the future of these economies is uncertain; will they become more state--oriented or pursue economic liberalism?

7. Bolivarian Republics

Argentina, Bolivia, Cuba, Ecuador, Nicaragua, Venezuela

Led by Venezuela's Hugo Chávez, large parts of Latin America are swinging back toward dictatorship and following the pattern of Peronism, with its historical antipathy toward America and capitalism. The Chávez-influenced states are largely poor; the percentage of people living in poverty is more than 60 percent in Bolivia. With their anti-gringo mindset, mineral wealth, and energy reserves, they are tempting targets for rising powers like China and Russia.

8. Stand-Alones

Brazil

South America's largest economy, Brazil straddles the ground between the Bolivarians and the liberal republics of the region. Its resources, including offshore oil, and industrial prowess make it a second-tier superpower (after North America, Greater India, and the Middle Kingdom). But huge social problems, notably crime and poverty, fester. Brazil recently has edged away from its embrace of North America and sought out new allies, notably China and Iran.

France

France remains an advanced, cultured place that tries to resist Anglo-American culture and the shrinking relevance of the EU. No longer a great power, it is more consequential than an Olive Republic but not as strong as the Hansa.

Greater India

India has one of the world's fastest-growing economies, but its household income remains roughly a third less than that of China. At least a quarter of its 1.3 billion people live in poverty, and its growing megacities, notably Mumbai and Kolkata, are home to some of the world's largest slums. But it's also forging ahead in everything from auto manufacturing to software production.

Japan

With its financial resources and engineering savvy, Japan remains a world power. But it has been replaced by China as the world's No. 2 economy. In part because of its resistance to immigration, by 2050 upwards of 35 percent of the population could be over 60. At the same time, its technological edge is being eroded by South Korea, China, India, and the U.S.

South Korea

South Korea has become a true technological power. Forty years ago its per capita income was roughly comparable to that of Ghana; today it is 15 times larger, and Korean median household income is roughly the same as Japan's. It has bounced back brilliantly from the global recession but must be careful to avoid being sucked into the engines of an expanding China.

Switzerland

It's essentially a city-state connected to the world not by sea lanes but by wire transfers and airplanes. It enjoys prosperity, ample water supplies, and an excellent business climate.

9. Russian Empire

Armenia, Belarus, Moldova, Russian Federation, Ukraine

Russia has enormous natural resources, considerable scientific-technological capacity, and a powerful military. As China waxes, Russia is trying to assert itself in Ukraine, Georgia, and Central Asia. Like the old tsarist version, the new Russian empire relies on the strong ties of the Russian Slavic identity, an ethnic group that accounts for roughly four fifths of its 140 million people. It is a middling country in terms of household income—roughly half of Italy's—and also faces a rapidly aging population.

10. The Wild East

Afghanistan, Azerbaijan, Kazakhstan, Kyrgyzstan, Pakistan, Tajikistan

This part of the world will remain a center of contention between competing regions, including China, India, Turkey, Russia, and North America.

11. Iranistan

Bahrain, Gaza Strip, Iran, Iraq, Lebanon, Syria

With oil reserves, relatively high levels of education, and an economy roughly the size of Turkey's, Iran should be a rising superpower. But its full influence has been curbed by its extremist ideology, which conflicts not only with Western countries but also with Greater Arabia. A poorly managed economy has turned the region into a net importer of consumer goods, high-tech equipment, food, and even refined petroleum.

12. Greater Arabia

Egypt, Jordan, Kuwait, Palestinian Territories, Saudi Arabia, United Arab Emirates, Yemen

This region's oil resources make it a key political and financial player. But there's a huge gap between the Persian Gulf states like Saudi Arabia and the United Arab Emirates and the more impoverished states. Abu Dhabi has a per capita income of roughly $40,000, while Yemen suffers along with as little as 5 percent of that number. A powerful cultural bond—religion and race—ties this area together but makes relations with the rest of the world problematic.

13. The New Ottomans

Turkey, Turkmenistan, Uzbekistan

Turkey epitomizes the current reversion to tribe, focusing less on Europe than on its eastern front. Although ties to the EU remain its economic linchpin, the country has shifted economic and foreign policy toward its old Ottoman holdings in the Mideast and ethnic brethren in Central Asia. Trade with both Russia and China is also on the rise.

14. South African Empire

Botswana, Lesotho, Namibia, South Africa, Swaziland, Zimbabwe

South Africa's economy is by far the largest and most diversified in Africa. It has good infrastructure, mineral resources, fertile land, and a strong industrial base. Per capita income of $10,000 makes it relatively wealthy by African standards. It has strong cultural ties with its neighbors, Lesotho, Botswana, and Namibia, which are also primarily Christian.

15. Sub-Saharan Africa

Angola, Cameroon, Central African Republic, Congo-Kinshasa, Ethiopia, Ghana, Kenya, Liberia, Malawi, Mali, Mozambique, Nigeria, Senegal, Sierra Leone, Sudan, Tanzania, Togo, Uganda, Zambia

Mostly former British or French colonies, these countries are divided between Muslim and Christian, French and English speakers, and lack cultural cohesion. A combination of natural resources and poverty rates of 70 or 80 percent all but assure that cash-rich players like China, India, and North America will seek to exploit the region.

16. Maghrebian Belt

Algeria, Libya, Mauritania, Morocco, Tunisia

In this region, spanning the African coast of the Mediterranean, there are glimmers of progress in relatively affluent countries like Libya and Tunisia. But they sit amid great concentrations of poverty.

17. Middle Kingdom

China, Hong Kong, Taiwan

China may not, as the IMF recently predicted, pass the U.S. in GDP within a decade or so, but it's undoubtedly the world's emerging superpower. Its ethnic solidarity and sense of historical superiority remain remarkable. Han Chinese account for more than 90 percent of the population and constitute the world's single largest racial-cultural group. This national cultural cohesion, many foreign companies are learning, makes penetrating this huge market even more difficult. China's growing need for resources can be seen in its economic expansion in Africa, the Bolivarian Republics, and the Wild East. Its problems, however, are legion: a deeply authoritarian regime, a growing gulf between rich and poor, and environmental degradation. Its population is rapidly aging, which looms as a major problem over the next 30 years.

18. The Rubber Belt

Cambodia, Indonesia, Laos, Malaysia, Philippines, Thailand, Vietnam

These countries are rich in minerals, fresh water, rubber, and a variety of foodstuffs but suffer varying degrees of political instability. All are trying to industrialize and diversify their economies. Apart from Malaysia, household incomes remain relatively low, but these states could emerge as the next high-growth region.

19. Lucky Countries

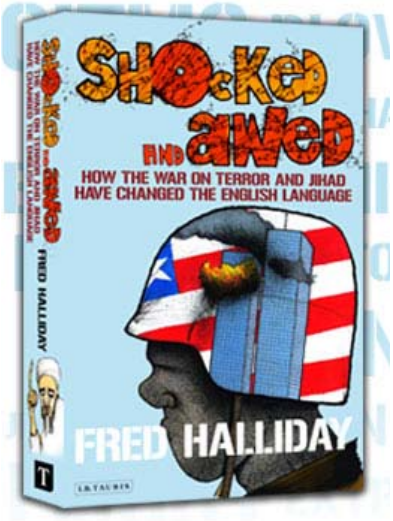
Australia, New Zealand

Household incomes are similar to those in North America, although these economies are far less diversified. Immigration and a common Anglo-Saxon heritage tie them culturally to North America and the United Kingdom. But location and commodity-based economies mean China and perhaps India are likely to be dominant trading partners in the future.

Joel Kotkin is executive editor of NewGeography.com and is a distinguished presidential fellow in urban futures at Chapman University and an adjunct fellow with the Legatum Institute in London. He is author of The City: A Global History. His newest book is The Next Hundred Million: America in 2050, released in February, 2010.

Shocked and Awed in English Language

Drawing on years of painstaking collation, Fred Halliday shows how the 'War on Terror' has brought us not just new words, such as 'Gitmo', and new imports, such as 'jihad', but also new ways of using existing language, such as 'extraordinary rendition'. Scanning the pock-marked semantic landscape of the post 9/11 world, he uncovers hidden twists of phrasing and word associations, which in themselves tell a story about the violent clash of ideologies that has marked the opening of the 21st century. Part indispensable reference, part polemic, part entertaining snapshot of our times, Shocked and Awed is a bristling arsenal of the 21st century's most potent weapons: words.



Fred Halliday, who died in April 2010 aged 64, was Professor Emeritus of International Relations at LSE and a Research Professor at the Barcelona Institute for International Studies. He was familiar with 10 languages, including Arabic and Persian, and published over 20 books.

Extracts

terrornomics

Pseudo-scientific, newly concocted, field of study analysing the flow of funds to terrorist organisations, and how they raise, store, move and disburse money, especially groups supporting Islamic fundamentalists. One of the most time-wasting ideas to come out of the study of terrorism, since the flows of money involved inwhatwere usually highly decentralised operations was very small, and the motivation of those involved was based on belief, ideology and rage.

ticking bomb

Situation where information has to be extracted very quickly, often justification for torture. Cf. TV series 24.

general level of arrogant incompetence

Thus stated the British Member of Parliament, Gwyneth Dunwoody, in regard to the application of airport security measures in US airports, after having been subjected to them three years after the 9/11 attacks. Other passengers had been arrested or deported because their names had somehow appeared on 'no-fly' lists, and some journalistswere detained in shackles because no one had informed them that they needed a special type of visa. Giovanni Bisignani, head of the International Air Transport Association, described the lack of coordination as 'inexcusable', noting that requirements in one country can break the laws of another. This was especially so after an agreement was signed between the USA and EU governments in May 2004 requiring European airlines to share data on arriving air passengers, including names, addresses, itineraries, telephone numbers and credit card details.

Jihadi jet set

Otherwise known as 'flying jihadis', term for 'second generation of Arab-Afghans' that appeared in the 1990s. Transnational in activity and engagement, they were sometimes moreWesternised than their predecessors and had few links with any particular Muslim country.

three-legged stool argument

Argument that US policy in Iraq had to make progress on three fronts – military, but also economic and political – to succeed. Used to justify the February 2007 'surge' in Iraq, but also taken up by 'moderate' Democrat Representative Tim Mahoney of Florida in explaining his change of heart over Iraq policy, to one of opposition, on grounds of the financial costs of the war. As late as July 2007, after a visit to Iraq, he was quoted by a Republican press release in a Florida newspaper, while attempting to establish himself in a firm centrist position in a traditionally Republican district, as saying that the escalation had really gotten Al-Qa'ida 'on their heels'. Later, his, revised, argument was that, while things had improved militarily [sic], '…everybody I talked to at the beginning of the surge back in February all said the same thing, "This is a three-legged stool." There has got to be economic progress.We haven't seen it. There has got to be political progress – nonexistent.' He added, 'We put the $100 billion in, and two legs of this stool are broken, the two things the army can't solve' (David M. Herszenhorn, 'A Moderate Democrat Hardens His Stance on Iraq', IHT, 4 September 2007).

enhanced interrogation techniques

One of several US euphemisms for torture, see also CID treatment, waterboarding. Analogous to, and possibly derived at least indirectly from, the Gestapo term, verfsch¨arfte Vernehmung, 'sharpened' or 'enhanced' interrogation.

waterboarding

Form of torture used by US armed forces in interrogation especially after 9/11; euphemism given a superficially innocuous veneer by association of name with the sports of surfboarding and waterskiing. Involves strapping a prisoner down, placing a cloth over his face and dousing him with water to simulate

the sensation of drowning. Despite the fact that two laws passed by Congress after 2001, and a Supreme Court ruling on the treatment of detainees, were generally interpreted to have banned the CIA's use of this interrogation method, theWhiteHouse itself declared that it was legal and that President Bush could authorize the CIA to resume using the simulated-drowning method under 'extraordinary' circumstances. In support of this position, CIA DirectorMichael V. Hayden stated that depriving the CIA of enhanced techniques would place 'America' in greater danger, while 'a senior US intelligence official' argued that waterboarding should not be considered torture because the US military had subjected its own personnel – 'tens of thousands of American Air Force and naval airmen' – to the method to prepare them for the possibility of being captured (Greg Miller, 'Waterboarding Is Legal White House Says', Los Angeles Times, 7 February 2008). Yet in a 2007 letter to Senator Patrick Leagy, four retired military lawyers, led by Rear Admiral Donald J. Guter, stated, 'waterboarding is inhumane, it is torture, and it is illegal' (Moustafa Bayoumi, In These Times, October 2008). Cheney, when asked on TV about waterboarding, had said that for him it was a 'no-brainer', 'a dunk in the water' (Nicholas Kristof, New York Times, 20 March 2007).

third-country dungeons

'Secret locations' outside the USA where 9/11 suspects were held and, reportedly, also tortured.

corkscrew journalism

Instant comment, bereft of research or originality, leading to a cycle of equally vacuous, staged polemics between columnists who have been saying the same thing for the past decade, or more. The term originated in the film The Philadelphia Story (George Cukor, 1940).

Empire lite

Termed used by Canadian philosopher, writer and politician Michael Ignatieff to describe US power and actions in the early twenty-first century. See also grace notes (Michael Ignatieff, 'The Burden', The New York Times Magazine, 5 January 2003).

Absurdistan

Addition, in the form of a title (of a book by Gary Shteyngart, Random House, 2007) to the growing number of '-istans' invented since 9/11 (FT Magazine, 8–9 March 2008). See also Hamastan, Richistan, Talibanistan.

expectation management

Official euphemism for propaganda designed to backtrack on earlier commitments and deflect criticism of Western policies, e.g. 'after all the promises made by the coalition before and after the invasion of Iraq that the countrywould be rebuilt once the fighting was over, the chaos and violence after liberation fell far short of expectations – and these expectations had to be "managed"' (Steve Tatham, Losing Arab Hearts and Minds: The Coalition, Al Jazeera and Muslim Public Opinion [London:Routledge, 2007]). Also, when the final announcement of a British troop withdrawal from Iraq was made, in December 2008, the BBC reported that 'it was met with relief '. This apparently positive message serving to deflect any discussion of what the more than five years of involvement in Iraq had actually achieved.

astroturfing

As a political term said to have been coined by Senator Lloyd Bensen, to yield a satirical redefinition of 'grassroots democracy', in regard to faking by politicians or companies of opinion or behaviour that is supposedly supported by the public. Originally, the term refers to corporate practice, in particular the Big Pharma companies that fabricate illness out of symptoms that are supposedly chemically reparable. For example, shyness becomes a 'depressive disorder' but the solution is at hand in the form of SSRIs, 'selective serotonin reuptake inhibitors', marketed as Prozac, Zoloft, Paxil, Luvox, Exefor and Celexa, inter alia. Ditto the vast wellbeing and antiaging industry designed to pathologise, and make money from, normal biological change. In politics and international affairs, the same practice is applied in threat

inflation, e.g. fabricating a threat of WMDs and then creating a national security crisis that requires urgent and costly action.

Compassionate Conservatism

Bushite euphemism for greed. See haves and have mores.

Weapons of Mass Destruction

Category of weapons covering nuclear, biological and chemical weapons, i.e. broader than nuclear weapons but beyond what were previously called 'conventional' weapons. The term was first used by The Times (28 December 1937) to report the German bombing of the Basque town of Guernica in the Spanish civil war and revived in US arms control and official vocabulary of the 1970s. Despite the canonical usage of the abbreviation WMD, this term is far less precise than is often claimed: many biological and chemical weapons are, while capable of wreaking terrible suffering on their specific targets at any one time, not capable of 'mass destruction'. Thus Professor Lawrence Freeman, writing of the lumping together of chemical, biological and chemical weapons through use of this term: 'Their routine elision, which is nowso ingrained as to be beyond remedy, encourages carelessness in public debate in failing to distinguish between systems that cause containable tragedies to those that would lead to the most unimaginable catastrophe' (See Survival. The IISS Quarterly, Vol. 46, No. 2, Summer 2004, p. 40n2).

Shock and Awe

Supposedly resolute and intimidatoryphrase espoused by the US administration prior to the 2003 Iraq invasion, to denote use of overwhelming force to break opposition forces and will power, and impose control on that country. Six years later, as George W. Bush prepared to leave office, with over 100,000 US troops still tied down in Iraq, and over 4,000 US soldiers dead, the words had changed to morass, nightmare, quagmire and other self-exculpatory terms (see Chapter 11). The term Shock and Awe was originally coined in a book published by the US National Defence University in 1996, Shock and Awe: Achieving Strategic Dominance by Harlan Ullan and James Wade. Designed as a post-Cold War strategy for the US military, that would use its superiority in firepower, precision and information control, it resumed concepts long present in military thinking, such as Blitzkrieg, full spectrum dominance and rapid dominance. The word awe, its resonance strengthened in the 1990s in the slang word awesome, served to attribute superhuman, possibly invincible, qualities to the US armed forces. Like many supposedly scientific military doctrines, it made assumptions that in reality never applied, such as complete knowledge of the enemy and, not least, of one's own side. Later adopted as a term of commercial promotion by, among others, sellers of golf clubs, condoms and financial services. It is also the name of a Scottish pop group. In phonetic terms, an example of the English language trope of supposed greater emphasis given by pairing of two, sometimes rhyming, monosyllables such as cut and run, huff and puff, kiss and tell, pump and dump, rock and roll, spit and polish.

collateral damage

US military euphemism, developed in regard to nuclear targeting policies in the 1970s, for civilian casualties. From the Latin collateralis (col-, 'together with' and lateralis, from latus, 'side'), the word is now perhaps best used as a synonym for 'unintended'.The US Department of Defense defines collateral damage as, '[u]nintentional or incidental injury or damage to persons or objects that would not be lawful military targets in the circumstances ruling at the time'. Consequently 'collateral' is 'not unlawful': 'Such damage is not unlawful so long as it is not excessive in light of the overall military advantage anticipated from the attack' (US Department of Defense, Joint Publication, 3–60, 3 April 2007).

Euthanizing War Hero Dog

Source: http://www.foxnews.com/us/2010/11/20/ariz-worker-fired-euthanizing-war-hero-dog/#ixzz17EfFnsyS

A county employee in Arizona has been fired after mistakenly euthanizing a dog that saved soldiers in Afghanistan and lived through explosions in the war-torn country, officials announced Friday. The

unidentified Pinal County animal control employee euthanized the female shepherd mix on Monday and was immediately placed on administrative leave. The dog named Target had been brought to the Phoenix area in August by Sgt. Terry Young after his tour of duty. Target frightened a suicide bomber inside a military base and potentially saved dozens of soldiers' lives, Young said. He said the dog was treated like royalty from then on at the base at Dand Patan, near the Pakistan border. The dog escaped from the family's back yard last Friday. Target didn't have a tag or microchip and eventually wound up at the county pound. Last Friday night, Young found Target's picture on a Web site used by county dog catchers to help owners track lost pets. Young figured the shelter in Casa Grande was closed for the night and weekend. He showed up at the facility to claim his dog on Monday, only to find out she was dead. County officials say the employee mistakenly took the dog out of its pen Monday morning and euthanized it. "I just can't believe that something like this would happen to such a good dog," Young told The Arizona Republic, which said the soldier and his family will get Target's cremated, remains. County officials are declining to name the employee because of threats made to that person and angry telephone calls to the facility. "We are continuing to look into management practices and procedures to ensure that something like this cannot happen again," said Lisa Garcia, assistant county manager for Health and Human Services.

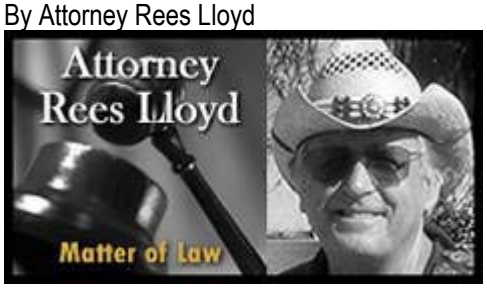
Russian Tribute to 911 Victims

I had never heard of this before receiving an e-mail. Why the press didn't report it?

This is the "TEAR DROP" made and installed by the Russians to honor those who died in 9 11 and a statement against terrorism. It is very impressive. The tear drop is lined up with the Statue of Liberty. Created by Russian sculptor Zurab Tsereteli, the memorial was a gift from the Russian people. Dedicated on September 11, 2006, it stands in direct view of the Statue of Liberty and the former World Trade Center. Standing at 100 feet tall and weighing 175 tons, the monument was shipped from Russia to the United States in six sections — weighing between 28 and 63 tons each — and assembled by a group of Russian artisans. Zurab Tsereteli spent several months in the U.S. overseeing construction of the memorial.

WHY NO SALUTE BY OBAMA AT MEDAL OF HONOR CEREMONY?

By Attorney Rees Lloyd



November 26, 2010
Source: http://www.newswithviews.com/Lloyd/rees110.htm

A moment of national pride took place recently in the White House when an American soldier, Staff Sgt. Salvatore Giunta, received the Medal of Honor for bravery above and beyond the call of duty in combat in Afghanistan.

Sgt. Giunta became the first living American soldier to receive the Medal of Honor since the Vietnam War. He is now one of only eighty-eight (88) living holders of the Medal of Honor.

As modest and self-effacing as he is brave, Sgt. Giunta brought further honor to himself by his humility in receiving the nation's highest medal of valor. While he made no comment in the ceremony, Giunta said before the ceremony that he was "not at peace" with being "singled out" for the honor as so many other soldiers did so much. And after the ceremony, he said he would trade the honor in a moment if he could bring back those whose lives he attempted to save under enemy fire but was unable to save. He definitely showed that he was an American in whom America could be proud.

In contrast, there was another "first" at the ceremony involving the Commander-in-Chief, President Barack Hussein Obama, in whose conduct the nation cannot and should not take pride: As far as is known, Obama became the first President, the first Commander-in-Chief , not to salute the living recipient of the Medal of Honor after presenting the medal.

It is a tradition in the military for all military personnel, no matter how high their rank, including the Commander-in-Chief, to salute a holder of the Medal of Honor no matter how lowly his or her rank. If General David Petreas was to encounter Sgt. Giunta, it would be the General who would salute the enlisted man, as a sign of respect for that soldier's extraordinary bravery, but also to show respect to all

those who have received the Medal of Honor.

At all gatherings of veterans of the American Legion, or VFW, or other veterans organizations, if a Medal of Honor recipient enters the room, even a National Convention involving thousands, the proceedings stop to render military honor to that holder of the Medal of Honor. All veterans rise, come to attention, and salute. It is a matter of pride, of respect, of tradition.

And, as far as is known, it is tradition that every President who has had the honor to present the Medal of Honor to a living recipient, has shown humility, respect, and national pride in that recipient by stepping back and rendering a salute.

It was missing in action in the Obama presentation. He is apparently above all that; "like a God," as an editor of Newsweek once wrote.

Instead of rendering the traditional salute, after fumbling as if all-thumbs in trying to affix the blue-ribboned Medal of Honor, Obama, equally awkwardly, tried to "hug" the Sergeant. Yes, a "hug" for the

soldier who remained at attention with eyes front in military bearing.
But a "hug" is not a "salute," even in the Age of Obama. While there may be some comedic value in Obama's pathetic display, it was more emetic than comedic. I didn't write about it at the time, so as not to distract from Sgt. Giunta's receipt of the Medal of Honor. But days have past, and it needs to be said.
Why? Is it naught but petty carping of poor President Obama? I think not. He is the "Commander-in-Chief" who has in his power the lives of those who serve in defense of the country, which he himself did not deign to do. It is pointing out that this man, this professional politician, repeatedly evidences contempt for America, for America's traditions, and for Americans who respect those traditions.
It is as if he loathes the nation he was so desperate to lead, and be loved by, Messiah-like. It is of a piece with his constant misquoting of the Declaration of Independence by leaving out the words "endowed by their Creator" when speaking of "unalienable rights."
Perhaps more aptly: It is of a pathetic piece with Obama's penchant for declining to abide by the U.S. Flag Code when the Flag passes to place his hand over his heart. Instead, he drapes his arms down and enfolds his hands at his crotch Michael Jackson-style. It is now mocked as Obama's "crotch salute." But it isn't funny. It is contempt by Obama for the Flag, for America.
Perhaps it is unfair to criticize this President of the United States for displaying such contempt for American traditions. Perhaps it is too much to expect an American President to salute a recipient of the military Medal of Honor when that president never served in the uniform of his country; has said that the Rules For Radicals of the America-hating socialist revolutionist Sol Alinsky are "seared into my [his] brain;" who launched his political career in Chicago from the living room of the revolutionist Weather Underground rich-brat-bombers Bill Ayers and Bernadine Dohrn; and who sat for twenty years in a pew of the church of Rev. "God D...n America" Wright, being marinated in hate-filled, grievance-filled, self-defined "anti-white" and "revolutionary" Black Liberation Theology.
Then again, perhaps it is not too much to expect anyone who would be America's president to at least respect American traditions, including honoring the Flag, and saluting those who receive the Medal of Honor.

See the whole ceremony at: http://www.youtube.com/watch?v=R2RWscJM97U

*REES LLOYD is a longtime civil rights attorney and veterans activist whose work has been honored by, among others, the California Senate and Assembly, and numerous civil rights, workers rights, and veterans rights organizations. He has testified as a constitutional expert at hearings before the U.S. House and Senate representing The American Legion. He has been profiled, and his work featured, by such varied print media as the Los Angeles Times and American Legion Magazine, and such broadcast media as ABC's Nightline and 20/20, Fox News In The Morning, and, among others, by Hannity. His writings have appeared in a variety of national, regional, and local newspaper, magazine, and other publications. He is a frequent radio commentator, and a sought after speaker.**

*[*For identification only. The views expressed here are solely Rees Lloyd's and not necessarily any person, entity or organization he may otherwise represent.]*

CBRNE-TERRORISM Newsletter

Δελτίο ΧΒΡΠΕ-ΤΡΟΜΟΚΡΑΤΙΑΣ

Volume 5 - 2010

TERR –News

Resource Scarcity, Climate Change and the Risk of Violent Conflict

Alex Evans[1]
Center on International Cooperation
New York University
September 9, 2010

[1] Head of Program, Resource Scarcity, Climate Change and Multilateralism, Center on International Cooperation, New York University. Source: http://www.cic.nyu.edu/internationalsecurity/scarcity.html

Abstract
This paper provides a brief assessment of how natural resource scarcity and global climate change may change the risk of violent conflict in the future. The resource scarcity element of the paper is primarily focused on resources required to meet basic needs such as food, land and water, as opposed to high-value commodities associated with the 'resource curse', such as diamonds, coltan or hardwood (although oil is touched on in the paper, primarily because of the linkages between oil and other scarcity issues). The paper begins with an overview of projected trends in resource scarcity and climate change. It emphasises that problems of resource availability may be as much the result of poor governance as physical constraints, and that the risk posed by climate change or resource scarcity depends as much on the vulnerability of populations, ecosystems, economies and institutions as on the magnitude of climate or scarcity impacts themselves. Resource availability must be seen not as a stand-alone issue, but rather in the context of the overall political economy landscape. The paper then discusses ways in which these trends may affect conflict risk, including already-established links and ways in which such links may evolve in the future, including under abrupt change scenarios. The paper concludes with some brief remarks on possible avenues of exploration for conflict prevention and building resilience in the light of scarcity and climate change.

WORLD DEVELOPMENT REPORT 2011
BACKGROUND PAPER

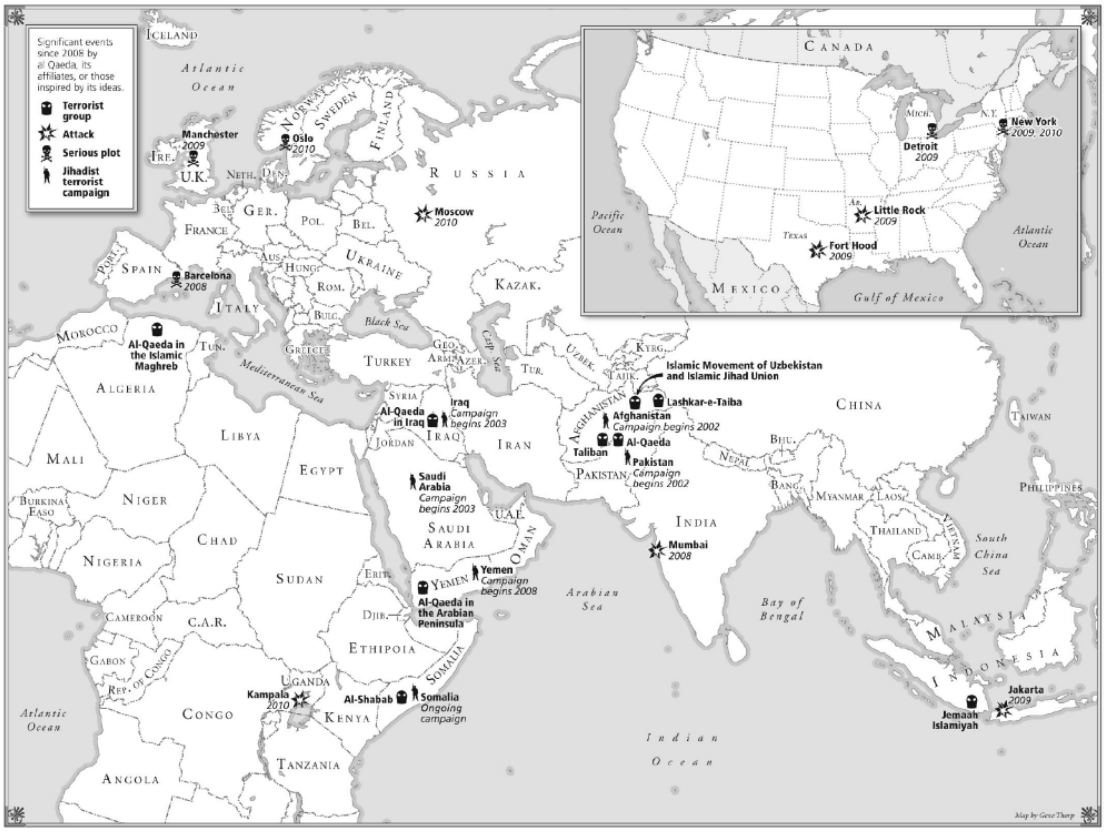
Assessing the Terrorist Threat

A Report of the Bipartisan Policy Center's National Security Preparedness Group
☞Peter Bergen and Bruce Hoffman
September 10, 2010

Executive Summary
Al-Qaeda and allied groups continue to pose a threat to the United States. Although it is less severe than the catastrophic proportions of a 9/11-like attack, the threat today is more complex and more diverse than at any time over the past nine years. Al-Qaeda or its allies continue to have the capacity to kill dozens, or even hundreds, of Americans in a single attack. A key shift in the past couple of years is the increasingly prominent role in planning and operations that U.S. citizens and residents have played in the leadership of al-Qaeda and aligned groups, and the higher numbers of Americans attaching themselves to these groups. Another development is the increasing diversification of the types of U.S.-based jihadist militants, and the groups with which those militants have affiliated. Indeed, these jihadists do not fit any particular ethnic, economic, educational, or social profile. Al-Qaeda's ideological influence on other jihadist groups is on the rise in South Asia and has continued to extend into countries like Yemen and Somalia; al-Qaeda's top leaders are still at large, and American overreactions to even unsuccessful terrorist attacks arguably

BIPARTISAN POLICY CENTER

have played, however inadvertently, into the hands of the jihadists. Working against al-Qaeda and allied groups are the ramped-up campaign of drone attacks in Pakistan, increasingly negative Pakistani attitudes and actions against the militants based on their territory, which are mirrored by increasingly hostile attitudes toward al-Qaeda and allied groups in the Muslim world in general, and the fact that erstwhile militant allies have now also turned against al-Qaeda. This report is based on interviews with a wide range of senior U.S. counterterrorism officials at both the federal and local levels, and embracing the policy, intelligence, and law enforcement communities, supplemented by the authors' own research.



Conclusions

The conventional wisdom has long been that America was immune to the heady currents of radicalization affecting both immigrant and indigenous Muslim communities elsewhere in the West. That has now been shattered by the succession of cases that have recently come to light of terrorist radicalization and recruitment occurring in the United States. And while it must be emphasized that the number of U.S. citizens and residents affected or influenced in this manner remains extremely small, at the same time the sustained and growing number of individuals heeding these calls is nonetheless alarming. Given this list of incidents involving homegrown radicals, lone wolves, and trained terrorist recruits, the U.S. is arguably now little different from Europe in terms of having a domestic terrorist problem involving immigrant and indigenous Muslims as well as converts to Islam. The diversity of these latest foot soldiers in the wars of terrorism being waged against the U.S. underscores how much the terrorist threat has changed since the September 11, 2001, attacks. In the past year alone the United States has seen affluent suburban Americans and the progeny of hard-working immigrants gravitate to terrorism. Persons of color and Caucasians have done so. Women along with men. Good students and well-educated individuals and high school dropouts and jailbirds. Persons born in the U.S. or variously in Afghanistan, Egypt, Pakistan, and Somalia. Teenage boys pumped up with testosterone and middle-aged divorcees. The only common denominator appears to be a newfound hatred for their native or adopted country, a degree of dangerous malleability, and a religious fervor justifying or legitimizing violence that impels these very impressionable and perhaps easily influenced individuals toward potentially lethal acts of violence. The diversity of this array of recent terrorist recruits presents new challenges for intelligence and law enforcement agencies, already over-stressed and inundated with

information and leads, to run these new threats to ground. There seems no longer any clear profile of a terrorist. Moreover, the means through which many of these persons were radicalized -- over the Internet -- suggests that these days you can aspire to become a terrorist in the comfort of your own bedroom. In short, the threat that the U.S. is facing is different than it was nine years ago. It has also changed and evolved since the 9/11 Commission presented its report six long years ago. Today, America faces a dynamic threat that has diversified to a broad array of attacks, from shootings to car bombs to simultaneous suicide attacks to attempted in-flight bombings of passenger aircraft. In the aftermath of September 11, 2001, the consensus within the national security and intelligence communities was that when it came to attacks on the U.S. homeland, al-Qaeda was intent on matching or besting the loss of life and destruction it caused that day. Since catastrophic-scale attacks require high levels of planning and coordination to succeed, they also generate more opportunities for detection and intervention. Now it is clear that terrorist groups see operational value in conducting more frequent and less sophisticated attacks that can place severe stress on finite intelligence and law enforcement resources. In addition, al-Qaeda has concluded that these attacks can have strategic value by generating a "big bang for the buck," given that even a near-miss (e.g. the Christmas Day 2009 plot) can generate so much media and political fallout. Improving the odds of effectively countering today's increasingly dynamic and diversified terrorist threat will require a much greater degree of engagement of state and local public safety officials. As the ranks of U.S. recruits have grown, the new frontlines have become the streets of Bridgeport, Denver, Minneapolis, and other big and small communities across America. Making sure that the nation's 50,000 public safety agencies are kept apprised of the changing face of terrorism poses a significant training and information-sharing challenge, but one that America neglects at its peril. However, even if America's intelligence, law enforcement, and homeland security communities are far better prepared to counter this new collection of adversaries, it still will not be enough. On Christmas Day 2009, it was not a federal air marshal, but the courageous actions of the passengers and flight crew aboard Northwest Flight 253 that helped disrupt the attack once it was underway. In Times Square, it was a sidewalk T-shirt vendor, not the New York Police Department patrolman sitting in a squad car directly across the street, who sounded the alarm about Faisal Shahzad's explosive-laden SUV. It is reckless to leave the task of combating terrorism only to the professionals when the changing nature of the threat requires that ordinary Americans play a larger support role in detecting and preventing terrorist activities. It is also important to acknowledge that how Americans respond to terrorist attacks can influence the worrisome trend by terrorist groups to radicalize and train recruits to carry out less sophisticated operations on U.S. soil. If any attack can succeed in generating significant political and economic fallout, then there is a greater motivation for undertaking these attacks. Alternatively, terrorist attacks that have limited potential to inflict serious casualties or cause disruption become less attractive if Americans display a greater degree of resilience by being better prepared to respond to and recover from these attacks. Since as a practical matter it is impossible to prevent every terrorist attack, the United States should be working in any event to improve the capacity of its political system, along with citizens and communities, to better manage how America deals with such attacks when they occur. When the U.S. demonstrates its national resilience in the face of terrorism, terrorist groups will have little to gain by attacking the American homeland. When federal agencies work well with one another and their counterparts at the state and local levels, and reach out to everyday Americans, the United States will be far better able to detect and prevent future attacks. In short, nine years after the September 11, 2001, attacks on New York and Washington, the changing nature of the terrorist threat makes clear that the U.S. must be willing to re-examine many of its counterterrorism assumptions and approaches. Only then can America succeed at maintaining the upper hand in the face of an adversary who continues to demonstrate the ability to learn and adapt.

Terror threat to restaurants as Al Qaeda calls for attacks on government workers in D.C.

Source: http://www.nydailynews.com/news/national/2010/10/11/2010-10-11_terror_threat_to_ restaurants_ as_al_qaeda_calls_for_attacks_on_government_workers.html

The terror group tied to the Ft. Hood killings and the Christmas Day undies airbomber urge wannabe American jihadis to open fire on crowded restaurants in the nation's capital to massacre U.S. government workers. The advice appears in "Inspire," the latest issue of a slick propaganda publication by Al Qaeda in the Arabian Peninsula, Osama Bin Laden's franchise in Yemen. "A random hit at a crowded restaurant in Washington, D.C., at lunch hour might end up knocking out a few government employees," Yahya Ibrahim writes in the 74-page jihadi how-to magazine. "Targeting such employees is paramount and the location would also give the operation additional media attention," Ibrahim added. Other trash talk came from "Samir Khan," an American who came to AQAP from North Carolina, who produces the publication and wrote that he is "proud to be a traitor in America's eyes." "This guy is bad news, and given the fact that he helps publish AQAP trash, he certainly spreads a lot of it around, too," said a senior U.S. official.

According to a copy of the magazine obtained by the SITE intelligence group, AQAP also urged those bent on murdering for Islam to use everything from pickup trucks to improvised pressure-cooker bombs to kill. The trucks can be fashioned into "the ultimate mowing machine," with steel blades welded to the grill to "mow down the enemies of Allah" by running down Americans on crowded sidewalks "to achieve maximum carnage" in a "martyrdom operation." "This method has not been used before," advises AQAP in its "Tips for our brothers in the U.S." Ibrahim praised the killings of a dozen victims at the U.S. Army post in Texas allegedly committed by accused homegrown terrorist Maj. Nidal Hasan, who was in contact with and inspired by U.S.-born AQAP cleric Anwar al-Awlaki. In 1993, Pakistani killer Mir Aimal Kasi opened fire on CIA employees at a stoplight, who were targeted because their cars were in a turn lane for the agency's Virginia headquarters.

Handful Of Americans Play Key Roles In Terrorism Threat

Source: http://www.npr.org/templates/story/story.php?storyId=130439513&ft=1&f=1001

The single biggest change in terrorism over the past several years has been the wave of Americans joining the fight — not just as foot soldiers but as key members of Islamist groups and as operatives inside terrorist organizations, including al-Qaida. These recruits, a number of whom are profiled in this "Terror Made In America" series, are now helping enemies target the United States. The list of American terrorists is growing, and they are coming from the unlikeliest of places: Miramar, Fla.; Charlotte, N.C.; Brooklyn; Albuquerque; and Winchester, Calif.

Adnan Shukrijumah (clockwise from left), Anwar al-Awlaki, Yousef al-Khattab and Samir Khan.

This series looks at a handful of what are arguably America's most successful jihadis — people who have risen to a position of prominence in the world of radical Islam. They have emerged as masterminds, propagandists, enablers and media strategists who, because of their understanding of America, pose a new challenge for law enforcement. One, Adnan Shukrijumah, was born in Saudi Arabia, reared in Trinidad and came of age in Florida. He is now considered one of Osama bin Laden's top lieutenants. Samir Khan is a North Carolina man thought to have edited and created a new English-language magazine for al-Qaida's arm in Yemen. Yousef al-Khattab was the founder of Revolution Muslim, an extremist group that operates openly in New York City. He has since left the group. The organization has become a gateway for young Muslims looking to sign up for violent jihad. And Adam Gadahn and Anwar al-Awlaki are two Americans who have helped al-Qaida develop a savvy online presence that is attracting recruits from around the globe. Authorities had been so concerned about al-Awlaki, a radical cleric now living in Yemen, and his ability to recruit jihadis to attack the U.S. that they put him on a capture or kill list — essentially targeting him for assassination. All of these people have brought uniquely American qualities to the groups they support. Shukrijumah's path to power in al-Qaida reads like a typical American success story. He worked his way up. Khan's magazine has a glossy American quality to it — from the jazzy headlines to the articles on how to pack for jihad — and he tested its prototype in the United States. Members of Revolution Muslim have openly demonstrated in support of al-Qaida, and its founders are converts taking full advantage of how easy it is in America to reinvent oneself. Gadahn and al-Awlaki learned how to reach an American audience by watching how it is done in America, firsthand. Together, these Americans within their groups have changed the nature of the terrorist threat against this country: They are more threatening because they understand the United States better than the United States understands them.

Al-Qaeda is a bigger threat today than 10 years ago, says terrorism expert

Source: http://www.dw-world.de/dw/article/0,,6087974,00.html?maca=en-rss-en-world-4025-rdf

Al-Qaeda is far more dangerous than it was 10 years ago, the former head of the CIA's bin Laden unit tells Deutsche Welle in an interview. He is also worried about the increased domestic threat the West is facing.

Michael F. Scheuer is an adjunct professor of security studies at Georgetown University in Washington, DC. A long time counterterrorism official, he was the former head of the CIA's Osama bin Laden unit. Scheuer is the author of "Through Our Enemies' Eyes: Osama bin Laden, Radical Islam & the Future of America" (2003) and "Imperial Hubris: Why the West is Losing the War on Terror" (2004).

Deutsche Welle: There is some confusion about the current threat of terrorism in Europe, specifically in Germany, France and Britain. While the US, British and Australian authorities have issued a travel alert for Europe, German officials have downplayed the threat saying there were no indications of an imminent attack. Since the US and Europe share intelligence information, how do you explain the discrepancy in judgment?

Michael F. Scheuer: At least in the American case we have a government that's extraordinarily incompetent in terms of experience with these kinds of things. And they are covering their behinds as much as they can. Certainly in the last weeks running up to the midterm elections here in the United States they don't want to be blamed for any kind of a security failure. That said, it was very unusual in my experience for the United States to issue a travel alert for Europe. They are always very reluctant to do that because they are afraid to hurt the transatlantic economy. So I suspect there is something to the overall discussion of a current threat.

Law enforcement and intelligent officials are of course walking a fine line in deciding when to go public with a warning about a possible terrorism threat. It seems that the US government is generally quicker to issue terrorism warnings than European countries. From your experience what's the better approach?

I think every government has to decide that for themselves. But my own impression is that since 9/11 the approach by the United States government is often quite juvenile in the sense that they want to cover their backside so nothing happens that they can get blamed for. Certainly in my experience while I was working at the CIA the British and the European services were more willing to follow a threat a little longer than we were in order to try to break it up more thoroughly.

Intelligence officials point to an increased amount of chatter as a reason for the terror alert and the German interior minister said there is a high level of abstract threat for Germany. Can you explain what that means from your experience in practical terms?

Very often information about terrorism is not clear cut one way or another. You are trying to figure out what they are saying, they are using code words, so it's very hard to tell whether it's imminent. I think what he (Germany's interior minister - the ed.) means by abstract is that people are debating whether to do it or not or whether they have the capability to do it.

In the European context though I think one thing that perhaps Europeans don't realize is that they are begging to be attacked, they have done virtually everything they can to make sure that they will be attacked whether it's the caricatures of the prophet Mohamed in a Danish newspaper that are now published in a book, the French ban on the burka. At least in cultural terms, many of the Europeans countries appear to have declared war on Islam and its traditions. And so the idea that we are getting this threat now and that there is a lot of chatter about it should not be a surprise to the Europeans.

From your perspective, have European governments done enough to secure their countries from an attack?

No of course not. Like the United States they have no idea who is in their country. Their immigration policies have been anything from a shambles to a disgrace for the last 20 years. They have no idea who is in Germany or Spain or Italy or the United Kingdom. So the police authorities really don't have an ability to preempt these things with any degree of certainty. They do a very good job, but the politicians flooded the playing field if you will with players that no one can identify.

You have worked closely with European and German authorities during your long career with the CIA. How would you rate the work of German intelligence services and the transatlantic cooperation on intelligence matters?

I thought that the German BND was always a little bit standoffish, who were not always ready to cooperate in terms of terrorism activities. That may have changed, I have not been working now for five years. On the other hand, the state and the federal police force in Germany were always very helpful and eager to help protect their citizens.

Basically I found the same thing in Britain, that the external service was a little less cooperative than MI5 for example. The MI5 was always an extremely good ally and a very competent service.

And finally, you have been tracking al-Qaeda and Osama bin Laden for years. How dangerous is al-Qaeda nine years after 9/11 and what's bin Laden's role within the organization today?

Certainly it's a much more dangerous organization today than it was in 2001. Just from the perspective of where we had to focus, we in the West, in Europe and in the United States. Before 9/11 most of the activities that were directed against us came out of Pakistan and Afghanistan. Today we have them coming from there, but we also have them coming out of Yemen, out of Iraq, out of the Levant, out of Somalia and out of North Africa. So the platforms from which people are being directed toward us have grown considerably.

As for the second part of the question, al-Qaeda and bin Laden have always seen their role primarily as violence or military activities, but also through inspiration, providing the materials whether written or spoken that would inspire other Muslims to conduct Jihad against the West and especially the United States. And I can't think how you can avoid the conclusion that that has been tremendously successful. The number of young Muslim males in Europe and the United States, Canada and Australia who are willing to at least consider and increasingly are ready to pick up the tools of violence against their home countries has increased dramatically since 2006.

Part of that is due of course to our own foolish invasion of Iraq, but much of it is due to the religiously consistent rhetoric of Osama bin Laden. And so I think this is a fight that we are really not cognizant of in terms of its dimensions and of its length. And one that will turn out much more bloody than we expected.

Interview: Michael Knigge
Editor: Rob Mudge

Berlin: Germanophobia in school

Source: http://islamineurope.blogspot.com/2010/10/berlin-germanophobia-in-school.html?utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+IslamInEurope+%28Islam+in+Europe%29&utm_content=Yahoo!+Mail

The Local reports that Germany's commissioner for integration, Maria Böhmer, said that Berlin officials should deal with anti-German views among immigrant students. Böhmer was responding to recent reports of Germanophobia in schools. Two teachers from a Kreuzberg (Berlin) school recently wrote in the GEW Teachers' Union paper of the anti-German harassment some German students experience in schools. They wrote that German students are threatened and bullied, and that the non-German students often receive help from relatives or friends in conflicts. The German students are asked what they are doing there.Berlin youth coach Oliver Lück (44) says such incidents happen every day. For years he's been working with bully-victims and with the harassers. He told BILD of three cases which particularly moved him:

• Dennis (14) from Reinickendorf - a quiet boy with glasses and pale skin. The problems started once there were more and more foreigners in his class. They called him a wimp. they wanted him to smoke with them, which he didn't want to do. Dennis was pushed around and beaten. They could do whatever they wanted with him, and he had to pay protection money to the older foreign students. In the end, he couldn't take it anymore and thought of suicide. Finally, his parents helped him.

• Lena (15) from Schöneberg - a confident teen, she died her head red and wore black clothes. When she came to the school, she was a foreigner among the other girls, who wore a headscarf. The girls whispered about her, they laughed at her and caller her the 'fire alarm'. Lena began to smoke, and later started up with alcohol and harder drugs.

• Kevin (16) from Neukölln - There were hardly any Germans in his school. The Arab guys provoked him, first with insults, then tripped him and pushed him. At some point, he fought back, and found himself facing twelve boys, relatives of the attackers, who beat him up. From that point on he started dressing like his tormentors and imitating their language. He wasn't beaten up anymore, but had to run errands for the others.

BILD also brings the story of Domitian E. (15), from Berlin-Charlottenburg. He was an outsider from the beginning, since he lighter skin and hair, spoke standard German and respected his teachers. In August Domitian E. changed schools due to his poor grades. It was supposed to be a new beginning, but it became the worst time of his life. "I was harassed because I speak German," says Domitian. "Altogether we were 29 students in the class, and besides me there was only one other German student," he says. "The rest were mainly Arabs and Turks." From the first few days he was discriminated against, harassed and insulted. "They asked me what I wanted here. Since I cam from a gymnasium, I didn't belong." he says that they cursed him behind his back since he came from a 'smart' school, and that his classmates often accosted him in groups, asking him why he didn't speak like they did. His classmates spoke "Kanake German" (German with a foreign accent and foreign terms). Domitian says he didn't want to speak that way. He avoids the other students and tried not to respond to them. Eventually, he avoided school and became increasingly sick.

Domitian says he was often sick and constantly threw up when he came home from school. He had stomach pains and severed colds. His teachers couldn't protect him from his classmates and nobody listened to him. When his mother noticed how much he was suffering, she decided to send him to another school. In a few weeks he'll move to a different school where there are more Germans, and where, he hopes, he won't be harassed.

Fanning the Flames of Jihad

Source: http://www.stratfor.com/weekly/20100721_fanning_flames_jihad
By Scott Stewart

On July 11, 2010, al-Malahim Media, the media arm of al Qaeda in the Arabian Peninsula (AQAP), published the first edition of its new English-language online magazine “Inspire.” The group had tried to release the magazine in late June, but for some reason — whether a technical glitch, virus (as rumored on some of the jihadist message boards) or cyberattack — most of the initial file released was unreadable. The magazine was produced by someone who has a moderate amount of technological savvy, who speaks English well and who uses a lot of American idioms and phraseology. We did not note any hint of British or South Asian influence in the writing. A government source has suggested to us (and we have seen the claim repeated in the media) that Inspire was produced by a U.S citizen who was born in Saudi Arabia named Samir Khan. Khan is a well-known cyber-jihadist — indeed, The New York Times did an excellent story on Khan in October 2007. Given Khan’s background, history of publishing English-language jihadist material and the fact that he reportedly left the United States for Yemen in 2009 and has not returned, it does seem plausible that he is the driving force behind Inspire. The magazine contains previously published material from Osama bin Laden, Ayman al-Zawahiri, Abu

Musab al-Suri and Anwar al-Awlaki. While it also contains new material, this material, especially from al-Awlaki and AQAP leader Nasir al-Wahayshi (aka Abu Bashir), is consistent with their previously published statements. One of the messages by al-Awlaki featured in Inspire, "A Message to the American People," was previously released to CNN and reissued by al-Malahim on the Internet July 19, almost as if to validate Inspire. Even though the way in which some of the material in Inspire is presented is quite elementary, and could lead some to believe the magazine might be a spoof, we have found no analytical reason to doubt its authenticity. Presentation aside, the material is quite consistent with what we have seen released by al-Malahim Media in its Arabic-language materials over many months. When closely examined, the inaugural issue of Inspire provides a good gauge of AQAP's thought and suggests the general direction of the broader jihadist movement.

Inspiration

In a letter from the editor appearing at the beginning of the magazine, the purpose of Inspire is clearly laid out: "This magazine is geared towards making the Muslim a mujahid." The editor also clearly states that Inspire is an effort by al-Malahim Media to reach out to, radicalize and train the millions of English-speaking Muslims in the West, Africa, South Asia and Southeast Asia. Inspire does not represent any sort of major breakthrough in jihadist communication. English-language jihadist material has been available on the Internet since the early 1990s on sites such as Azzam.com, and jihadists have released other magazines directly targeting English-speaking audiences. What is remarkable about Inspire is that it was released by al-Malahim and AQAP. Within the jihadist movement, AQAP has assumed the vanguard position on the physical battlefield over the past year with links to several attacks or attempted attacks in the West. AQAP has also been frequently mentioned in Western media over the past several months, and it appears that al-Malahim is trying to exploit that notoriety in order to get the attention of English-speaking Muslims.

Regarding AQAP's links to recent attacks, Inspire follows the trend of AQAP publications and leaders in recent months in praising Fort Hood shooter Maj. Nidal Hasan and failed Christmas Day bomber Umar Farouk Abdulmutallab and lifting them up as examples for all jihadists to follow. "We call on every Muslim who feels any jealousy for their religious beliefs to expel the polytheists from the Arabian Peninsula, by killing all of the crusaders working in embassies or otherwise, and to declare war against the crusaders in the land of the Prophet Muhammad — peace be upon him — on the ground, sea and air. And we call on every soldier working in the crusader armies and puppet governments to repent to Allah and follow the example of the heroic mujahid brother Nidal Hassan [sic]; to stand up and kill all the crusaders by all means available to him…." In the article discussing Abdulmutallab, the author again brags about the manufacturing of the improvised explosive device used in the Christmas Day attack even though that device, like the one used in the assassination attempt against Saudi Deputy Interior Minister Prince Mohammed bin Nayef, failed to achieve the objective. "The mujahidin brothers in the manufacturing department managed with the grace of Allah to make an advanced bomb. The bomb had been tested and proven effective as it has passed through the detector ports. The martyrdom bomber managed with the grace of Allah to reach his target, but due to a technical glitch, the bomb did not explode completely; and we will continue on our path until we get what we want…." This statement would seem to indicate that if AQAP is able to recruit a willing suicide bomber who is able to travel to the West, they will again attempt to attack an airliner using a similar device. Airliners remain vulnerable to such attacks. STRATFOR has previously noted when discussing AQAP and its innovative IED designs, there are many ways to smuggle IED components on board an aircraft if a person has a little imagination and access to explosives. As we wrote in September 2009, three months before the Christmas Day bomber's attempted attack, efforts to improve technical methods to locate IED components must not be abandoned, but the existing vulnerabilities in airport screening systems demonstrate that an emphasis needs to be placed not only on finding the bomb but also on finding the bomber. Throughout the magazine, articles criticize the U.S. operations in Afghanistan, Iraq and Yemen; Saudi operations against jihadists; the burqa ban in Europe and even global warming — Inspire carried a reproduction of a statement purportedly authored by Osama bin Laden earlier this year titled "The Way to Save the Earth" that criticizes U.S. policy regarding climate change and calls for economic jihad against the United States. The magazine also contained a portion of a previously-released message titled "From Kabul to Mogadishu" by al Qaeda second-in-command Ayman al-Zawahiri that

encouraged the people of Yemen to join al Qaeda in its global struggle. It only quoted a part of the original message that pertained to Yemen and omitted portions that pertained to other locations.

AQAP Revealed

In addition to the recycled content from al Qaeda's core leadership, Inspire also contains quite a bit of new and interesting content from AQAP's military and theological leaders. An interview with AQAP leader Nasir al-Wahayshi provided al-Wahayshi the opportunity to reinforce several points he has been making for months now regarding his call for jihadists to conduct simple attacks using readily available weapons. "My advice to my Muslim brothers in the West is to acquire weapons and learn methods of war. They are living in a place where they can cause great harm to the enemy and where they can support the Messenger of Allah." Al-Wahayshi continued "…a man with his knife, a man with his gun, a man with his rifle, a man with his bomb, by learning how to design explosive devices, by burning down forests and buildings, or by running over them with your cars and trucks. The means of harming them are many so seek assistance from Allah and do not be weak and you will find a way." This call was echoed by Adam Gadahn in March 2010 when the American-born spokesman for al Qaeda prime advised jihadists to strike targets that were close to them with simple assaults and urged his audience to not "wait for tomorrow to do what can be done today, and don't wait for others to do what you can do yourself." These calls are part of a move toward a leaderless resistance model of jihadism that has accompanied the devolution of the jihadist threat from one based on al Qaeda the group to a broader threat based primarily on al Qaeda franchises and the wider jihadist movement. (STRATFOR is currently putting the finishing touches on a book that details our coverage of this devolutionary process since 2004.) With this shift, more attacks such as the Times Square bombing attempt, the Fort Hood shooting and the June 1, 2009, Little Rock shootings can be anticipated. In an effort to provide training in terrorist tradecraft to such grassroots and lone-wolf jihadists, Inspire contains a section called "Open Source Jihad," which is the term that AQAP uses to refer to leaderless resistance. This section is intended to serve as "a resource manual for those who loathe tyrants." The material is intended to allow "Muslims to train at home instead of risking a dangerous travel abroad," and one part exclaims, "Look no further, the open source jihad is now at hand's reach." The section also contains a lengthy step-by-step guide to constructing simple pipe bombs with electronic timers, bearing the rhymed title "Make a Bomb in the Kitchen of Your Mom." The images of New York City contained in this section serve as a reminder of the importance New York holds in jihadist thought as a target. Such rudimentary improvised explosive devices are unlikely to cause mass casualties, but like the pipe bombs employed by Eric Rudolph, they could prove deadly on a small scale if they are employed effectively. When considering this concept of leaderless resistance and of using publications like Inspire to train aspiring jihadists, it is important to remember that this type of instruction has only a limited effectiveness and that there are many elements of terrorist tradecraft that cannot be learned by merely reading about them. In other words, while the jihadist threat may be broadening in one way, it is also becoming less severe, because it is increasingly emanating from actors who do not possess the skill of professional terrorist operatives and who lack the ability to conduct complex and spectacular attacks.

Cartoon Controversy

One of the other features in Inspire is an article by Anwar al-Awlaki, the American-born Yemeni cleric who has been linked to Nidal Hasan, Umar Farouk Abdulmutallab, Faisal Shahzad and two of the 9/11 hijackers. In his article, titled "May Our Souls be Sacrificed for You," al-Awlaki focuses on the controversy that arose over the cartoons of the Prophet Mohammed that first appeared in 2005. Although the cartoons were published nearly five years ago, the jihadists have not allowed the issue to die down. To date, the jihadist response to the cartoons has resulted in riots, arsons, deaths, the 2008 bombing of the Danish Embassy in Islamabad and an attack in January 2010 in which a man armed with an axe and knife broke into the home of Jyllands-Posten newspaper cartoonist Kurt Westergaard in Denmark and allegedly tried to kill him. The Kashmiri militant group Harkat-ul-Jihad e-Islami (HUJI) also dispatched American operative David Headley to Denmark on two occasions to plan attacks against Jyllands-Posten and Westergaard in what HUJI called "Operation Mickey Mouse." In his Inspire article, al-Awlaki states, "If you have the right to slander the Messenger of Allah, we have the right to defend him. If it is part of your freedom of speech to defame Muhammad it is part of our religion to fight you." Al-Awlaki continues: "This effort, the effort of defending the Messenger of Allah, should not be limited to

a particular group of Muslims such as the mujahidin but should be the effort of the ummah, the entire ummah." He also referred to a 2008 lecture he gave regarding the cartoon issue titled "The Dust Will Never Settle Down" and notes that, "Today, two years later, the dust still hasn't settled down. In fact the dust cloud is only getting bigger." He adds that "Assassinations, bombings, and acts of arson are all legitimate forms of revenge against a system that relishes the sacrilege of Islam in the name of freedom." Inspire also features a "hit list" that includes the names of people like Westergaard who were involved in the cartoon controversy as well as other targets such as Dutch politician Geert Wilders, who produced the controversial film Fitna in 2008; Ayaan Hirsi Ali, who wrote the screenplay for the movie Submission (filmmaker Theo Van Gogh, the director of Submission, was murdered by a jihadist in November 2004); and Salman Rushdie, author of the book The Satanic Verses. Most of these individuals have appeared on previous jihadist hit lists. A new notable addition was American cartoonist Molly Norris, who was added due to her idea to have a day where "everybody draws Mohammed." Norris made her suggestion in response to threats against the irreverent animated television program South Park by Muslims over a brief scene in an episode that lampooned the Prophet. Comedy Central censored the South Park episode featuring Mohammed because of the threats, provoking Norris's suggestion. Al-Awlaki and AQAP appear to believe they can use the anger over the Mohammed cartoons to help them inspire Muslims to conduct attacks. In this edition of Inspire, they are clearly attempting to fan the flames to ensure that the dust will not settle down. They are also seeking to train these radicalized individuals to kill people, although, as we note above, that is a difficult task to do remotely over the Internet. One other thing the magazine seeks to accomplish is to help make the jihadist training experience better for English speakers who seek to travel to jihadist training camps abroad. There have been anecdotal reports of Westerners who have traveled to get training and who have not had positive experiences during the process — and of at least one Somali-American who was executed after expressing his desire to leave an al Shabaab training camp and return home. In light of this problem, AQAP includes an article in Inspire titled "What to Expect in Jihad" and designed to reduce the "confusion, shock and depression" that can be experienced by trainees at such camps. The article also provides a list of things to bring to the training camp, including a friend to help ease the loneliness, and recommends that aspiring jihadists learn the local language. The time and effort that AQAP put into this first issue of Inspire, and the support the magazine apparently receives from important AQAP figures such as al-Wahayshi and al-Awlaki, are strong indicators of the group's intent to support leaderless resistance as a way to attack the West, something AQAP has had some difficulty doing itself.

A Financial Profile of the Terrorism of Al-Qaeda and its Affiliates

by Juan Miguel del Cid Gómez

Source: http://www.terrorismanalysts.com/pt/index.php?option=com_rokzine&view=article&id=126&Itemid=54

Abstract

This working document offers an analysis of the sources of financing of the Al-Qaeda network including some of its affiliated groups. The development of Al-Qaeda's financing has been similar to the evolution of its operational structure. The organization is currently under significant financial pressure. However, the number and magnitude of terrorist attacks attributed to Al-Qaeda in a number of countries implies that the network continues to have access to substantial financial resources to support its activities. The international community has so far not succeeded in cutting off many of Al-Qaeda's sources of financing; the organisation continues to access funding from wealthy benefactors, legitimate business and criminal activities.

Introduction

Since its foundation in 1988, *Al-Qaeda* has used various methods to obtain funding. Currently, its cells, branches and affiliated groups are obliged to act autonomously; many of them have, to a great extent, to finance themselves, including by means of ordinary crime. These groups have also had to resort to

hawala (a trust-based informal banking system) and cash couriers to move money or operate on the margins of the formal financial system. There are also other methods that are used by terrorist groups to transfer funds with little risk of detection. International trade is particularly vulnerable, due to its size and the complexity of methods of payment. The emergence of new methods of payment through new developments in information technology present additional risks for the authorities as these enable terrorists to move money with total anonymity.
The measures established by the United Nations Security Council, based on asset freezing, have failed to disrupt *Al-Qaeda*'s activities to a significant extent. On the other hand, the enforcement of due diligence with bank clients has been helpful in detecting some terrorist operations, although in general reports of suspicious financial transactions made by financial institutions are currently of limited value in actually seizing assets of terrorist organisations.

Al-Qaeda's Operational Costs

According to a CIA report, *Al-Qaeda*'s financial requirements before the 11 September 2001 attacks amounted to 30 million US dollars annually.[1] This money was earmarked for carrying out attacks, for the maintenance of its quasi-military apparatus, for training and indoctrination of its members, for contributions to the Taliban regime but also for the occasional support of associated terrorist organisations. It is currently very difficult to make a reliable estimate of the operating cost of *Al-Qaeda*, as it now acts through a large number of cells and satellite terror groups which are more or less autonomous.
The means these terrorist groups use to perpetrate attacks (vehicles, maps, components of explosives, surveillance material, etc.) are of relatively low cost compared to the damage they can cause. Certain estimates, whose accuracy may be open to question, provide an idea of the ratio of the approximate direct costs of certain attacks carried out by *Al-Qaeda* or its affiliates and the damage caused in terms of economic destruction and loss of human lives.

Table 1: Cost of Carrying out Various Terrorist Attacks

Attack	Date	Estimated Cost
London Underground/Bus	7 July 2005	8,000 GBP [3]
Madrid Railway Atocha)	11 March 2004	100,000 EURO [4]
Istanbul	15 & 20 November 2003	40,000 US $
Marriot Hotel Jakarta	5 August 2003	30,000 US $
Bali Bombings	12 October 2002	50,000 US $
New York Twin Towers	11 September 2001	400,000-500,000 US $ [5]
USS Cole, Aden	12 October 2000	10,000 US $
US Embassies: Kenya and Tanzania	7 August 1998	50,000 US $

However, terrorist organisations have to defray both the costs of carrying out an attack and the more substantial structural costs of maintaining the organisation and disseminating its ideology. In addition to purchasing weapons, vehicles, explosive material and detonators to be used in attacks, terrorist groups need to anticipate other needs, such as:

1. Subsistence living costs for its members and sometimes also their families. These expenses are considerable, despite the terrorists' generally frugal life styles. Costs vary according to the proximity of terrorists to their targets. The costs of activities in Western Europe will be considerably higher than those in African or Asian countries.

2. A terrorist cell also needs for its members reliable channels of communication, including highly secret channels to its leadership, from which it receives its instructions. Although communications costs have been reduced considerably through the use of mobile telephones, pre-paid cards and e-mail (often sent from Internet cafés), the procurement and use of communication tools can entail significant expenses.

3. Training new recruits constitutes a large investment for terrorist groups, both in terms of ideological indoctrination as well as the procurement of practical items to prepare for attacks. Although part of the general preparation can be carried out in terrorist training camps, some specific operations may require specialist skills (such as piloting planes)which can only be achieved with expensive training.

4.Travel costs for group members in preparation of an attack and acquiring false documentation papers, which may also involve travel. Further travel is required to meet other members of the network, to meet senior members of the hierarchy or to meet individuals able to provide material or financial support.

5. Propaganda for the cause via various channels of communications. *Al-Qaeda*'s capability of using camrecorders to broadcast its video footage is well-known. This terrorist organisation also makes extensive use of the Internet for recruitment, to spread its jihadi message and to raise funds. Al-Qaeda has managed to develop powerful propaganda materials that advocates violence, suicide attacks and the murder of infidels – which includes many Muslims deviating from Salafist ideals as understood by the group and its affliliates.

6. Charitable activities as a means of social legitimisation in order to win and maintain a constituency are another significant cost for some organisations that pursue their goals by means of terrorism (however, this does not apply to Al-Qaeda as much as to some other terrorist groups).

The points listed above lead us to conclude that although individual terrorist attacks can be performed at relatively low costs, organizations that are responsible for them need to be able to finance a considerable infrastructure to sustain themselves and to promote their objectives.

Sources of Al-Qaeda's Financing

In the past eighteen months, groups associated with *Al-Qaeda* have made many appeals for funds. A leader of *Al-Qaeda*, Mustafa Abu al Yazid, also known as Jeque Saeed, complained in a declaration published in extremist forums on 10 June 2009 that "many of the mujahidin have been inactive and failing to participate in jihad through lack of money".

Various extremist Internet sites have discussed the risks militants face while fundraising and laundering the money obtained by various methods. A report published in April 2009 warned members of Al-Qaeda's network that intelligence services could identify jihadists through banks, money transfer services, credit cards and online websites.

Such statements indicate that *Al-Qaeda* is under significant pressure resulting from international measures aimed at freezing its assets and cutting off its traditional sources of income. According to the US Treasury Department, Al-Qaeda is in its worst financial position for many years. In addition, the organisation cannot transfer money with the same ease as in the past. Parts of the purportedly charitable organisations that formed the backbone of its financing have been liquidated by national authorities and added to the UN list of organisations that support terrorism. However, the number and magnitude of terrorist attacks attributed to *Al-Qaeda* throughout the world indicate that the network continues to have access to considerable funding to support its activities.

In order to understand how the organisation currently finances itself, it is necessary to study the development of its operational structure. Since the 11 September 2001 attacks, *Al-Qaeda* has morphed into a decentralised organisation. Currently, three distinct but interlinked entities co-exist within *Al-Qaeda*. The first and original entity, established by its previous leaders and led by Osama Bin Laden, retains its importance and influence. It is most likely located in the rugged area on the border between Afghanistan and Pakistan.

The second group, consisting of veteran combatants who had received training in Afghanistan, extends to dozens of countries. It serves as an example and provides training and instructions to new recruits wish to become part of the jihadist enterprise.

The third group consists of newly radicalised militants who form local cells. They neither depend on a centralised authority, nor are they directly linked to it. Although these cells share fundamental objectives with *Al-Qaeda's* leadership, they are quite independent of it. They are anonymous and to a

great extent invisible until they decide to carry out an attack. These cells exist in various parts of the world and include individuals from widely different social status, education, age and racial background.
Among the sources of *Al-Qaeda*'s income we find since its inception funds diverted from charitable organisations, profits gained from businesses run by its members and sympathisers and money collected by fundraisers seeking donations. It is currently highly unlikely that the local groups receive significant financial support from the core leadership. Although they may receive funding from other traditional sources, the *Al-Qaeda* cells, branches and affiliates are currently obliged to act independently, and to a great extent finance themselves to varying degrees also from criminal activities such as kidnappings, and, in some cases maybe also drugs trafficking.

Fundraisers

Since its inception, *Al-Qaeda* has used a core of fundraisers tasked to solicit money from a range of donors.[10] The main group of donors is based in the Gulf area, principally Saudi Arabia, but donors also exist in other parts of the world. Some of these donors have been fully aware of the final destination of their money; others were not. Many donors make their contributions to money collectors. Other funds come from corrupt employees of charitable organisations, in particular during the holy month of Ramadan. Fundraisers often have also access to imams in the Mosques and obtain part of *zakat* (obligatory almsgiving) donations to support the cause of radical Islam. Fundraisers have sometimes used legitimate charitable organisations; in other cases they have used front organisations and legitimate businesses to provide cover for their activities. This mix of fund raising methods has enabled *Al-Qaeda* to construct a considerable financial network throughout the Muslim world and in foreign diasporas allowing it to obtain the money needed to operate.
Many of the original fundraisers, such as Khalid Sheikh Mohamed, a senior leader of *Al-Qaeda*, have been arrested. New fundraisers have been added to the UN Security Council's Sanctions Committee list. Although the names of some of these fundraisers are known, and the funds and the businesses they use are subject to assets freezing orders in many countries, a good number of them have been able to continue their activities without major problems. In some cases, *Al-Qaeda* has been able to replace known fundraisers with as yet unknown individuals and organisations.

Charitable Organisations

Charities have certain characteristics that make some of them particularly vulnerable to exploitation for the financing of terrorism. They generally enjoy the confidence of the public and have access to significant resources, in many cases in the form of cash. In addition, many of these organisations have a transnational presence which provides them with the necessary infrastructure to enable national and international transactions. In certain countries they are subject to only limited or no regulation at all (in terms of registration, accountability, transparency and audits of their accounts). They are also often easy to establish where there is no need for initial capital and where no background checks on employees are made).
Since its inception, *Al-Qaeda* has made attempts to use charitable organisations to finance some of its activities. Charities enable a number of terrorist organizations to collect, transfer and distribute the necessary funds for the purposes of indoctrination, recruitment and training. They also enabled them often to meet logistical and operational requirements.
Charity is one of the fundamental principles of the Islamic religion, and all those who have a certain amount of money are obliged to pay *zakat* (2.5% annually of savings and assets). Apart from the obligatory *zakat,* the Koran and Islamic tradition also advocate *sadaqah (*voluntary contributions) to the most needy. Most Muslims pay these contributions to Islamic charities and to their mosque, which use them to finance a great variety of religious, humanitarian and social activities.
Al-Qaeda's strategy has been to infiltrate employees in charities to divert money from the charities' legitimate humanitarian or social programmes towards its own illicit activities. In some cases, *Al-Qaeda* has created its own networks of charitable institutions as a cover to obtain funds directly. Some of these networks originated during the *jihad* against the Soviet occupation of Afghanistan in the 1980's. *Al-Qaeda* has also used charitable organizations to disseminate and teach the most radical forms of Islamic fundamentalism. In a number of countries, these organisations function outside the scrutiny and supervision of state authorities. It has proven difficult to shut them down completely, even in cases where they have been investigated and accused of financing terrorism.

An example of this lack of control can be found in one of the largest co-ordinating institutions of Islamic charities, the International Islamic Relief Organisation (IIRO), based in Jeddah (Saudi Arabia). Although most of its activities are dedicated to religious, educational, social and humanitarian programmes, IIRO and some of its subsidiary organisations have reportedly been used, knowingly or otherwise, to finance *Al-Qaeda*. The International Islamic Relief Organisation has subsidiaries throughout the world, although most of its financial contributions come in the form of private donations from Saudi Arabia. It has established an Endowment Fund (*Sanabil al Khair*) to generate a stable flow of revenues to finance its activities. It also works in close co-operation with the Global Islamic League. Many prominent individuals and financiers from the Middle East are associated with this Islamic charity. Various reports have linked it also to the financing of terrorist operations.

Another case that has raised suspicion is the Al Haramain Islamic Foundation headquartered in Saudi Arabia. It presented itself as a private non-governmental organisation with charitable and educational objectives. Considered a single entity, Al Haramain was one of the principal NGO's operating worldwide and allegedly supporting *Al-Qaeda*. The financing generally came from individual donors but special campaigns were also directed at certain commercial enterprises throughout the world.

The founder and former head of the Al Haramain Islamic Foundation, Aqeel Abdul Aziz Al Aqeel, and Al Haramain's subsidiaries in other countries, were accused of providing financial and material support to *Al-Qaeda* and other terrorist organisations such as Jemaah Islamiya, Al Itihaad al Islamia, the Egyptian Islamic Jihad and Lashkar e Tayyiba. These terrorist organisations had received funding from Al Haramain; they also used it as a cover for collecting funds.[14] In 2008, the US Treasury accused the entire Al Haramain organisation, including its Saudi Arabian headquarters, of financing the *Al-Qaeda* network. Between 2002-2004, three of its subsidiaries in various countries were designated financers of terrorism. However, its leaders succeeded in re-establishing part of the organisation and continue to operate under another name. According to a 2009 report from the Pakistani police, Al Haramain had contributed approximately 15 million dollars to jihadist groups in Pakistan. Most of the funding went to the Tehrik e Taliban (TTP), which was responsible for several suicide attacks and also accused of the assassination of Benazir Bhutto.

Although the Saudi Arabian government took some counter-terrorism measures immediately after 9/11, only *Al-Qaeda* attacks against Saudi Arabia in 2003 and 2004 marked a clear change of mind for Saudi authorities. They began to combat terrorist financing and considered *Al-Qaeda* as a threat to the regime itself. Despite these developments, the United States has recently demonstrated its concern about the ability of certain charities to support terrorism outside Saudi Arabia and about their use of money transfers to move funds to various remote locations.

Another charitable organisation, based in Kuwait, called the Revival of Islamic Heritage Society (RIHS) has also been accused of providing material and financial support to *Al-Qaeda* and its affiliates. For their support of *Al-Qaeda*, RIHS delegations in Afghanistan and Pakistan were in 2002 designated as terrorists by the US government and the Sanctions Committee of the UN Security Council. Yet there was at first no evidence indicating that RIHS's headquarter itself was aware that subsidiaries were financing *Al-Qaeda*. Since then, however, the authorities have established proof of the express consent of its leaders to the illegitimate use of the organisation's funds. RHIS subsidiaries in Albania, Azerbaijan, Bangladesh, Bosnia, Cambodia and Russia have been closed down by their respective governments on suspicion of supporting the financing. of terrorism. In countries where RIHS activities were banned or placed under State supervision, the central organisation developed various ways of continuing its activities. Among these was the channelling of funds through another organisation or changing the name of the subsidiary to avoid control by the authorities. Amongst other charges, the RIHS headquarter has been accused of lending financial and logistical support to Lashkar e Tayyiba (LeT), a Pakistani terrorist organisation linked to the *Al-Qaeda* network and involved in the 2006 train attacks in Mumbai and the attacks on the Indian parliament in 2001. It was a key source of financing that enabled the Bangladesh terrorist organisation known as Jamaat Mujahidin Bangladesh (JMB) to carry out a series of co-ordinated attacks in 2005 that left 2 people dead and 64 injured. Followers of *Al-Qaeda* in Somalia said that they had received significant amounts of money from RIHS.

The current situation of many of these charities is opaque. Despite the freezing of assets, in many cases financial activities have continued in the same locations, using bank accounts and resources in the name of third parties.

Offshore Entities and Companies

Al-Qaeda has used commercial companies to finance itself as well as to transfer funds. One example is Barakaat, a network of companies which, in 2001, had a foothold in 40 countries operating its telecommunications, construction, money remittance and cash exchange services from the United States and Somalia.

For Bin Laden, Barakaat was a suitable instrument for making cash transfers; he had invested in its telecommunications network. Barakaat acted as a source of financing and arranged cash transfers for him. Its owners channelled millions of dollars every year from the USA to *Al-Qaeda* or its associates. Barakaat also managed, invested and distributed funds for *Al-Qaeda*. Most of Bin Laden's transactions were carried out between Mogadishu and Dubai, Mombassa (Kenya) and Nairobi. In general, these funds were interlinked with transfers made in the name of non-governmental organisations such as Al Haramain and the International Islamic Relief Organisation.

Another case is the one of the Somalian group Al Itihaad Al Islamiya which, according to UN officials, led terrorist training centres and collected money from followers in Europe and the Middle East. Al Itihaad Al Islamiya financed its activities with distinct commercial operations. Among these activities was the export of coal to the Middle East, the provision of transport, security and protection services, telecommunications, commercial centres, running *hawalas* andother financial services, agricultural and hotel companies and was even involved in the distribution of fishing rights. Some of these services held genuine monopolies in certain areas; they were also employed by international relief organisations.

The use of fictitious companies and offshore fiduciary companies to shield the identity of individuals or entities taking part in terrorist financing poses difficult problem for those trying to regulate business transactions. These are companies, funds, entities or businesses that are registered in an extra-territorial financial centre. One example are International Business Corporations (IBC) which are used to create complex financial structures. They can be established using bearer shares and do not have to publish accounts. Residents of financial centre can act as fictitious directors or shareholders in order to disguise the genuine directors or owners. These entities are attractive to investors who seek anonymity or wish to carry out their activities beyond the official scrutiny of their national government.

In Spain, according to investigations made by the Fiscalía of the High Court (Audiencia Nacional), the former Salafist Group for Preaching and Combat (GSPC), -now integrated into *Al-Qaeda* in the Islamic Maghreb (AQIM) - obtained funds that its front men and couriers transported to Algeria and Syria. In order to do this, they used inactive companies or companies in the process of liquidation in tax havens such as the Bahamas and Delaware. The Audiencia Nacional followed the trail of an Algerian citizen in Spain with bank accounts in Palma de Mallorca in the name of an American company formed in Delaware. He transmitted funds totalling US $ 200,000 with the supposed purpose of paying invoices for the services of an IT company with bases in the Netherlands and Germany. The company concerned denied having issued these invoices these turned out to be false. This led investigators to believe that this money had left Spain for other purposes.

Drugs Trafficking and other Common Crime

The Afghan Taliban is an insurgent-cum-terrorist organization that makes extensive use of taxing proceeds from drugs to finance itself. In Afghanistan, the links between both pro- and anti-government elements and drugs trafficking is well-established. Unlike the *Al-Qaeda* network, the Afghan Taliban is an insurgent group whose activities and range is (so far) limited to Afghanistan and Pakistan. Although the Taliban receives (or received) support from *Al-Qaeda* and private donors from the Gulf States, a large part of its revenue in Afghanistan and Pakistan is derived from collections in Mosques, contributions from sympathisers and taxes on opium.

The Taliban practises extortion at several points in the heroin business in Afghanistan: taxing poppy farmers, laboratories where the drugs are processed and traffickers who transport precursors into the country and heroin out of it. Currently, many of those involved in the destabilisation of Afghanistan are directly or indirectly involved in illicit drug production, processing or procurement. In addition, the Taliban also raises "taxes" on legitimate business seeking to operate in Afghanistan.[23] It is more than likely that part of the money that these activities generate leaves the country and enters the international financial system.

Al-Qaeda and its associated groups have greatly diversified their methods of raising money to finance jihad. They finance themselves to varying extents through common crime, according to the conditions

and opportunities in the locations in which they operate. It is therefore often difficult to distinguish between terrorist groups, insurgents and organised crime groups since these categories often overlap. Their methods and sources of financing are often similar if not the same.

Amongst other sources of income, *Al-Qaeda* in the Islamic Maghreb (AQIM), which is active in the desert region between Mauritania, Mali and Algeria, obtains money from kidnapping ransoms, contraband and apparently also from drugs trafficking. The discovery of the remains of a Boeing 727 in the Mali desert raised serious suspicions amongst intelligence services in Europe and the United States that Latin American drugs traffickers have been using some areas partly controlled by AQIM to transport drugs from Colombia's FARC to European markets. From West African coastal countries such as Guinea-Bissau, the illicit drugs are reportedly taken across Mauritania, Mali and Niger to Egypt and Libya, from where they are transported further in containers.

According to Spanish police informants, drugs trafficking groups operating in the North African enclaves Ceuta and Melilla send a portion of the profits from hashish trafficking to finance Islamic terrorist groups, with whose cause they sympathise. A report from the National Intelligence Centre (NIC) dated 27 October 2003 concluded that members of *Al-Qaeda* sleeper cells are financed by drugs trafficking and credit card theft.

The 11 March 2004 bombings in Madrid represent an example of how attacks were funded by drug money and crime. Various members of the unit that carried out these bombings were involved in drugs trafficking, falsification of documents and other crimes by which they managed to raise substantial amounts of revenue. This criminal structure was used to acquire explosives for those who commit terrorist acts, with the ultimate aim is to establish a Sharia-based Islamic State.

Some radical groups which have financed themselves in Spain for years through hashish trafficking have taken a step further in their strategy to seek new resources. According to Spanish counter-terrorist sources, AQIM uses revenue from trafficking cocaine and synthetic drugs between Spain and Algeria to finance a campaign of terror in northern Africa. Having obtained cocaine from Latin America and synthetic drugs pills manufactured in the Netherlands and elsewhere in Europe, they resell these in Algeria, where the price is reportedly substantially higher than in the EU.

Such drugs trafficking activities form another link in a large chain of criminal activities to raise financing across borders. Joint investigations by the Spanish, Italian, Swiss and French police have revealed how robberies and drugs trafficking in Spain, robberies in Switzerland and tax fraud in Italy generate a significant amount of money which is then used to finance armed attacks and terrorist training. In addition to hashish trafficking, Moroccan radicals have specialised in robbery and the resale of all kinds of modern information technology such as GPS, new generation mobile telephones and electronic diaries. In many cases such items are later resold in Morocco or Spain.[27] According to another official Spanish investigation, the sale of designer watches, gold bracelets and emerald necklaces stolen from around 20 villas on the Costa del Sol by a Salafist group that goes by the name "Group of the Truth" was used to finance several murders in Algeria and Mauritania.

There is also an emerging relationship between Islamic terrorist groups and the commission of cyber crimes. According to investigations led by the UK police, three members of a terrorist cell that planned to carry out attacks in the US, Europe and the Middle East used several stolen credit cards to buy items such as GPS systems, night vision goggles, sleeping bags, telephones, knives and tents from hundreds of websites. These were meant to be sent to jihadists in Iraq. Among their purchases were hundreds of pre-paid mobile telephones and more than 250 airline tickets. These were bought with 110 different credit cards from 46 different airline companies and travel agencies. The three men involved also laundered money plundered from bank accounts with the help of on-line gambling sites. Numerous stolen credit cards and hacked bank accounts were also used to buy web-based services in the United States and Europe with the apparent aim of creating an online network to be used by jihadist cells throughout the world to exchange information, recruit members and plan attacks. The three cell members involved spent 3.5 million dollars from credit cards stolen by phishing on hundreds of websites. They also distributed spyware contained in emails or websites which enabled them to gain control of infected computers.

Pakistani extremists based in Spain developed operating methods of their own. These groups have close relations with radical cells in the UK that specialize in stealing credit cards. Such cards are cloned and sent to Spain, where hundreds to thousands of euros in charges are made by a certain business owner who then transfers the money to radical organisation, asking a commission of 10% for himself.

Radical Pakistani groups also obtain funds by collecting a 'revolutionary tax' from fellow countrymen based in Spain. On occasions they even engage in so-called *express* kidnappings which end once family members pays a ransom in Pakistan.
According to Interpol, there are also important links between intellectual property crimes and the financing of Islamic terrorist networks. Some terrorist groups participate directly in the production and sale of fake items and divert part of the profits to finance attacks. Also, part of the profits from the sale of non-genuine items (such as illegally copied CDs) apparently go to fundamentalist networks and such monies are eventually sent to terrorist groups via informal money transfers.

The Movement of Terrorist Funds

In the more than twenty years of its existence, *Al-Qaeda* and later its affiliates have used various methods to transfer funds with the aim of avoiding detection by the authorities. Among them are informal systems of money transfers such as *hawala*, cash transfers and the use of official financial systems. However, other mechanisms such as external trade and new methods of payment allowing anonymity have emerged in recent years.

Hawala

Alternative money transfer systems are a cheap and rapid way of sending funds and making transactions. Originally they mainly served those who did not have a bank account, particularly in remote areas without a functioning normal financial system. One of the most frequently used informal mechanisms is *hawala* ("transfer" in Arabic), a form of transporting financial obligations from one place to another without the physical movement of money and often also without a paper trail. What distinguises hawala from other informal systems are trust and a strong sense of honour as these often exist in extensive family networks based on regional and tribal connections of those who use it. The security, anonymity and the versatility of hawala is also attractive for criminals and terrorists who wish to move legally obtained funds or launder money raised by illegal activities.
These informal systems constitute a risk factor for the authorities since operators usually do not need to reveal the true identity of their client or apply official due diligence procedures. Hawala is widely used in the Middle East, the Indian subcontinent, in South East Asia and parts of Africa, particularly in rural areas where people have no access to the formal financial system. It is also prevalent in countries populated by émigrés and refugees, who use this system to send money to families in their countries of origin in order to avoid paying excessive bank charges.
Before 9/11, *Al-Qaeda* moved a large part of its funds through hawala networks. After the organisation's leadership moved to Afghanistan in 1996, there was no practical alternative as the Afghan national banking system was antiquated and insecure. Later, hawala became again *Al-Qaeda*'s system of choice when the government-regulated official financial systems stepped up controls on bank-based money transfers across national borders.
Many hawala transactions originate in, or are destined for, Dubai or Yemen, or pass through these places. Some countries such as the UAE have tried to regulate hawala operations and require users to register and provide information about the identity of remitters and beneficiaries on special forms which must be submitted periodically to the Central Bank. There are also requirements to report suspicious transactions. Currently in Afghanistan, all businesses that offer hawala services must obtain a licence, and report transactions to a financial intelligence agency of the Central Bank.
However, other countries have paid no attention to informal money transfer systems, or simply attempted to prohibit them. Although the vast majority of these unregulated services transmit legitimately obtained funds, terrorist organisations such as *Al-Qaeda* and the Taliban use them to hide or manage many of their legal and illegal financial transactions. They are often used to transfer funds obtained from charities, common crime, drugs trafficking or wealthy donors.

Cash Transactions

The physical movement of money across borders is predominant in countries where bank transfers are rarely used by common people. Couriers carrying money are also used where financial institutions have increased the efficiency of due diligence practices with clients. It is also one of the methods used by terrorist organisations such as *Al-Qaeda* to move funds whilst avoiding anti-money laundering and counter-terrorism financing measures implemented by national and international financial institutions.

The investigation into the 9/11 attacks provided a good example of how *Al-Qaeda* used human couriers to move money. One of the financial backers of the attack, Khalid Sheikh Mohamed, passed a large amount of money (possibly as much as US $ 200,000) to Abdul Aziz Ali in Dubai, who subsequently transferred it to the hijackers in the US.
Various counter-terrorism operations have demonstrated that money couriers moved funds between Middle Eastern and South Asian countries. They often did so by using indirect flights between origin and destination, with large numbers of couriers and frequent exchanges of money. Moving money by using couriers can be more expensive than a simple transaction, but it leaves no trace even if the courier is detained, since the origin and final destination of the money might be unknown to him or her. Some terrorist groups have converted the money into high-value goods where the source is difficult to trace, such as gold and precious stones, moving smuggling activities away from formal financial systems.
Algerian and Moroccan cells based in Europe use human couriers, as the Italian police discovered when a bus company connecting France and Italy with Algeria was transporting three individuals at least twice a week, each of whom carrying an average of 1,500 euros. Pakistani radicals also sent money to the United Kingdom with the help of couriers who fly to the UK carrying the equivalent of thousands of euros.

The Formal Financial System

Government-regulated financial institutions and other regulated financial service providers constitute the formal financial system It is the world's principal gateway for financial transactions across borders. *Al-Qaeda* has in the past used the formal financial system as a means of moving money to support its own cells and affiliated terrorist groups, financing their actions. The speed and ease with which money can be moved via the international financial system enables terrorists to move funds efficiently, unfortunately often still with relatively small risk of detection.
The 9/11 terrorists used official financial institutions both within and outside the US to deposit, transfer and withdraw money. The money was deposited in US banks, generally via transactions, cash deposits and travellers cheques bought overseas. Some of them kept funds in overseas bank accounts to which they had access through cash-point machines (ATM) and credit cards. Of the overall cost of the 9/11 operation (between US $ 400,000-500,000), at least US $ 300,000 came from bank accounts in the United States. None of the terrorists or their backers were experts in using the international financial system. The money laundering controls at the time were primarily designed to detect drugs trafficking and large-scale financial fraud. Therefore bank employees at that time were not suspicious of apparently routine transactions as those carried out by the 19 hijackers. One of those involved in the 7 July 2005 bombings in London financed the operation with his own funds, which were deposited in various accounts These movements did not attract the attention of bank employees.
Combined with other mechanisms such as offshore companies, the formal financial system can still provide terrorists with sufficient cover to carry out operations and launder crime money. The sheer volume and speed with which sums of money rush through the computer-linked international financial system make watertight CFT measures impossible.
Money remittance companies are particularly attractive to terrorist groups such as *Al-Qaeda*, which has used branches of such companies, which often operate globally, to send and receive money. These companies are in principle obliged to register identification details of the individual who has sent the money from one country and of the person who is meant to receive it in another. This should enable the authorities to track individual transactions by means of the logged details of every transaction. However, the lack of a consistent and worldwide application of due diligence procedures (involving identification, record keeping and report of suspicious transactions) are an obstacle for investigators when trying to track specific financial transactions.

International Trade

International trade has a range of characteristics which make it vulnerable to abuse by terrorist groups such as *Al-Qaeda* because the enormous volume of international commercial transactions obscures individual transactions. International trade is characterised by the complexity of its transactions and payment methods. The mixture of funds from a variety of sources together with the limited resources available to customs agencies in tracing them makes it very difficult to detect illegal transactions without case-specific additional intelligence.

International commercial operations lend themselves often to the hidden transfer of currency. Various techniques are used for this: over-invoicing or under-invoicing of goods and services, anticipated payments which are never made and re-invoicing through free trade areas. Laundering through over-invoicing and under-valuing of goods and services is a longstanding method of fraudulently transferring currency across borders; it continues to occur frequently. It involves attributing a set price to goods and services which differs from the actual market price. By invoicing goods and services at a price lower than the market, the exporter transfers currency to the importer, since the ultimate value will be lower than the amount the importer receives in selling them on the market. On the other hand, invoicing at an amount higher than the market price, the exporter receives currency from the importer since the price of the goods and services will be higher than their value.

In order for such operations to succeed, it is necessary that both the exporter and importer agree on manipulating prices. For example, if Company "A" exports 1,000 units of an item whose value is 2 euros per unit but invoices Company "B" at 1 euro per unit, it would lose 1,000 euros in the operation. This would make no sense unless both exporter and importer had agreed to carry out such a rigged transaction. Another possibility would be for the two companies to be controlled by the same organisation.

Banks play a fundamental (but no longer unique) role in making international transactions possible. They sometimes act as simple intermediaries to enable the movement of funds from one country to another, whilst in other cases they carry out a dual function of intermediary and guarantor to ensure that the conditions in the buying and selling contract are met. Payment methods that can be used in international trade vary in terms of the guarantees offered and the costs involved (personal and bank cheques, transfers, payment orders, banking remittances and credits). The participation of various parties in these operations and the complexity of payment methods can make the process of observing due diligence complicated. In addition, international trade is vulnerable to the use of falsified documents for the purposes of money laundering, terrorist financing and the avoidance of sanctions to breach international embargos. The use of front companies in high-risk jurisdictions can make it all the more difficult to track these operations. In other cases, international trade in services or commodities is used as part of more complex money laundering schemes such as the peso exchange black market, hawala and carousel fraud.

New Payment Methods

As an alternative to cash transfers and the use of bank accounts, various payment methods have evolved which are generally used by legitimate customers who lack access to regular banking services. They also are convenient for terrorist groups. Among these methods are pre-paid phone cards, online payment services, virtual money that is exchanged in the form of gold, silver and other metals and, most recently, mobile phone payments.

Pre-paid phone cards are a much used alternative to cash. They can often be obtained with complete anonymity and are easily transported, making them particularly attractive. One type of such cards can be used to withdraw money from various ATM cash-point networks throughout the world. They do not require a bank account; nor do they require the user to deal with a bank employee who would verify the identity of the client to 'top' them up. They can also be used to buy items in shops. In some countries, these cards have become very popular amongst immigrants who wish to send money to their families overseas.

From the point of view of countering the financing of terrorism, these cards present a risk, since they can be 'topped up' by a member of a terrorist organisation in any country, allowing other members of the organisation access to money from cash-points. The vulnerability of these cards lies principally in the way they can be obtained. Terrorists can buy cards on the Internet, by fax and in those shops which do not require identification from customers or apply any system for tracing suspicious transactions. They can also move money through massive scale purchase of such cards and their subsequent sale.

Online payment services are often a service used by people without bank accounts or credit cards when they wish to make purchases over the Internet. People who use this service can first use their bank accounts, credit cards, electronic transfers or pre-paid cards or, in some cases, simply cash to open an account with an online intermediary which will then carry out payments. One of these online services is PayPal, which enables anybody or any business with email to send and receive money quickly over the

Internet. It is more difficult to know the client's identity if the service provider does not insist on sufficient proof of identity or is willing to accepts cash or giro transfers to open the account.
Other payment systems such as E-gold are based on virtual money which is exchanged via ounces of gold and other precious metals. One of the characteristics of such business transactions is that the funds which are transferred to them are automatically converted into a specific metal (for example, gold). At any time, the client can see the value of the gold in various monetary denominations such as dollars, euros, etc, and can make a payment of a specific amount of dollars.
These systems can be used to pay for articles exchanged for specific items through commercial websites. The CFT risks associated arise from registration of the online user with a limited amount of information, the lack of identification details, the speed of business transactions, access to items of any value whose price is difficult to establish, and fictitious transactions whereby companies do not guarantee delivery. All this can enable the transfer of money between members of a terrorist organisation pretending to pay for business transactions while the price of items is manipulated or the goods are simply not delivered.
Payments via mobile telephones are another alternative to the use of cash and the formal financial system, principally in countries where it is difficult to find a reliable banking network. Technology enables the users of mobile telephones to pass funds between individuals in anonymity: the money sender buys a pre-paid phone card which is 'topped up' anonymously with funds which are subsequently transferred to the other person's card. This person can withdraw money from a cash-point using the pre-paid card. Thus, both the sender and receiver remain anonymous - another method that may be used by terrorist organisations to transfer money.

The International Response to the Financing of Al-Qaeda

A range of international organisations such as the World Bank, the International Monetary Fund (IMF), the United Nations and the International Financial Action Group (FATF-GATT) are involved in combating the financing of terrorism.
The World Bank and the IMF provide technical assistance to countries where the counter terrorist financing system is weak and where this can present a significant risk to good governance and development. Technical assistance from the World Bank and IMF is based on the introduction of new regulations based on best international practices, their application by authorities in the financial sector, the establishment of legal frameworks by financial intelligence bodies, the development of capitation programmes and awareness-raising to address the concerns of the private and public sectors as well as co-operation with other organisations under multinational programmes and the development of training material.
In Resolution 1267 (1999), the United Nations Security Council established the "Sanctions Committee against Al-Qaeda and the Taliban". Its original purpose was to monitor the application of sanctions against Afghanistan, then largely under control of the Taliban regime which supported Osama bin Laden and his several hundred men strong Al-Qaeda group.
The sanctions regime has, especially since 2001, been modified and strengthened by subsequent Security Council resolutions. In this way sanctions were extended to individuals and entities associated with Al-Qaeda, Osama Bin Laden and the Taliban throughout the world. Those UN resolutions that have been approved under Chapter VII of the UN Charter require all member states to adopt a series of measures with respect to any person or entity associated with *Al-Qaeda*, Osama Bin Laden and the Taliban designated by the sanction committee. Among these measures are freezing their assets, preventing their members entry into a UN member states' national territory or transiting it, and preventing the supply, sale or transfer, direct or indirect, of military arms and equipment.
The primary responsibility for the application of these sanctions falls on the member states; its effective application is their obligation. The individuals and entities suspected of terrorism feature on the consolidated List of the Sanctions Committee it is periodically updated or revised. The List consists of four sections and contains 507 names (according to the update of 3 December 2009):

1. Individuals associated with the Taliban (142)
2. Entities and other groups or companies associated with the Taliban (none)
3. Individuals associated with *Al-Qaeda* (254)
4. Entities and other groups or companies associated with *Al-Qaeda* (111)

It is not necessary for charges to have been brought against an individual by a national court or a conviction in a trial in a court of law for a suspect to be added to the List because the sanctions are said to be of a preventative nature. States are obliged to disseminate the List fully to banks and other financial institutions, intelligence agencies, alternative money remittance services and charitable organisations amongst others. The Committee has a team tasked with providing analytical support for the sanctions; that team publishes progress reports periodically.

Although there has been significant progress, there remain systemic weaknesses in the application of the sanctions. The List contains imprecise and obsolete information, including the names of deceased individuals and defunct companies. On the other hand, some entities and individuals on the List have taken legal action in various countries to challenge their inclusion on the List. In other words, they challenge the Security Council's authority to impose sanctions based on dubious intelligence information only. Due to this, states are sometimes unable to put into practice decisions taken by the Security Council without contravening their own legislation. As a consequence, the international community is in such cases not fully able to apply co-ordinated measures against the financing of terrorism.

The international community has so far failed to discover or block many of the sources of financing of *Al-Qaeda*. The organisation headed by Bin Laden continues to have access to money through various channels at the margins of the formal financial system. It also makes intensive use of alternative remittance systems and sometimes simply sends money via couriers.

Al-Qaeda has succeeded in moving a large part of its financial activities through its associated groups to areas in Africa, the Middle East and South-East Asia where the authorities often lack effective CFT institutions and where individuals who feature on the Security Council's List can continue their financing activities by using companies and fictitious businesses to hide their transactions. The bottom line is that despite the Committee's powers, *Al-Qaeda*, the Taliban and the network's associates are in a position to continue to seek, obtain, gather, transmit and distribute considerable sums of money to support their ideological, logistical and operational activities.

Another international organisation taking action against terrorist financing activities is the Organisation for Economic Co-operation and Development (OECD). In October 2001, the OECD adopted a set of eight special recommendations to combat terrorist financing. In combination with the already existing forty recommendations of its Financial Action Task Force (FATF) to combat money laundering, these 48 recommendations form the basic international framework meant to prevent and suppress terrorist financing and terrorist acts.

Identifying Suspicious Operations

The current legislative framework for preventing the use of the financial system and other areas of activity for terrorist purposes based on the OECD's 48 recommendations is now in place in the majority of countries. The basic principles for combating terrorist financing have developed in a form essentially parallel to those regarding anti-money laundering measures. But there are some differences between the two issues. In money laundering, criminal elements generally need to deposit large amounts of money into the financial system. In financial transactions relating to terrorism, the amount of money used is considerably less and is usually consistent with the client's stated profile, which makes them look innocuous. All too often financial institutions are unable to separate suspicious transactions from those which are not.

Yet authorities often consider the financial sector to be in an ideal position to detect money laundering and terrorist financing activities. Reports of suspicious activities sent by financial institutions to national financial intelligence units form the basis of this preventative system. However, it is not easy for financial entities to detect suspicious terrorist financing operations. To qualify as a suspicious transaction, deviations from the client's profile and usual practices must be taken into account, which implies the application of a policy based on "know your customer". It is not enough to identify clients; it is necessary to know their usual practices and sources of income. When business relations are established, it is necessary to obtain information from the client about the nature of his professional or company business and establish beyond reasonable doubt the veracity of the information provided. In particular, it is necessary to pay particular attention to any operation that is complex, unusual or lacks an apparent financial or lawful purpose. In order that personnel of a financial institution or similar entity may detect suspicious operations when assessing transactions, it is the norm to use a number of

indicators according to the sector of activities in which the client is involved. These indicators come from experience compiled by various government agencies, international organisations and financial intelligence units in various countries.

The financial sector uses various IT programmes aimed at detecting suspicious operations to evaluate transactions made by customers. Each client is given a specific profile that describes the expected usual practice of the said client. In general, this includes the number of transactions and the amounts involved which are expected to take place over a particular period of time with an acceptable margin of deviation from the norm. When the client's transactions go beyond this margin, the IT programme issues an alert. Yet when submitted to closer scrutiny, many of these transactions result in "false positives". Given that there is no single effective set of indicators to detect suspicious transactions for countering terrorist financing, it is necessary to evaluate a high number of activities to come to responsible conclusions as to whether something significant is going on or not. This is an inconvenience, since submitting a high number of "false positives" to further investigation takes up time and money. In order to avoid an excessive number of "false positives" without adversely affecting the control of operations, it is necessary to maintain a current profile of clients, consider adequate tolerance ratios for each type of transaction, establish an adequate frequency for review according to the risk presented, and take account of the conditions of the time and the market which may affect the operations being carried out.

There is currently a general concern within financial institutions that most of the indications they receive are orientated towards money laundering rather than terrorist financing. However, it is a common complaint that they receive scant or no information about high-quality indicators that enable the detection of financing for terrorism purposes. Consequently, many of the reports of suspicious transactions are valuable only if these actually trigger an investigation by the authorities. There is a significant imbalance between the high volume of reports on suspicious activities generated by financial institutions throughout the world and the scant value of terrorist assets located or frozen as a result of these reports. In many cases, the reports are clearly defensive to protect the institution against possible sanctions from the authorities and focus on the type of client rather than the nature of the transaction, which makes them of little use to investigators. The large volume of suspicious transactions filed by financial institutions tends to overburden the financial intelligence units tasked to analyse them. Backlogs are common which reduces the amount of actionable intelligence gained from monitoring suspicious transactions.

Seeking a financial profile of terrorism

Banks and other financial institutions continue to ask the authorities what more they should be looking for to detect possible transactions associated with terrorism. Many of the mechanisms available to financial institutions to detect money laundering activities are not directly applicable to detecting terrorism. The 11 September 2001 operatives are an example of this. The nineteen hijackers formed a simple plan to disguise their transactions without revealing their intentions. Although the US authorities had information that several of the hijackers might be members of *Al-Qaeda*, the banking personnel where they held accounts never suspected that their clients were potential terrorists.

Financial institutions and governments have made a considerable effort to create a profile of "the terrorist". The FBI examined financial transactions made by the 9/11 hijackers focusing on the following: they visited the banks in groups, identified themselves as students, spent a large proportion of their income on pilot training schools and were financed to a large extent from money transferred from the UAE. Yet other terrorist cells such as the London attackers used the legal income of one of their members deposited in various bank accounts to finance the attacks.[43] In other words, profiles may be of some help to detect more or less identical types of attacks, but do not help much to warn of attacks developed in a different way.

Terrorist financing does not always follow clearly recognizable guidelines. This is especially true in cases of local cells whose members save or collect money to finance their own activities. These cells can use their own legally obtained funds but can then carry out illegal operations. In all cases, including the latter, it is difficult to detect a terrorist motive or even a purely criminal one. It is not an easy task to create a general profile of financing and using funds for terrorist purposes. For example, when an Islamic charity receives money from small donations and then makes periodic financial transfers to areas such as Afghanistan or Chechnya, this might be to finance terrorist operations or might constitute

humanitarian aid to a very needy population. Intelligence services and governments can hold information that may distinguish one use of funds from another, but it is unlikely that a financial institution would be capable by itself of determining the difference.

Conclusion

Our conclusion is that financial information alone is not sufficient to detect the financing of *Al-Qaeda* and its affiliates. However, when combined with other types of information held by intelligence services, it may help a financial institution to detect signs of possible suspicious activity. In this sense, the development of intelligence-led indicators based on the study of evolving terrorist operating methods and the exchange of information between public and private sectors should be one of the pillars for the development of a more risk-based focus which can improve the detection of terrorist financing operations.

About the Author: ***Juan Miguel del Cid Gómez*** *holds a PhD in Economics and Business and is Professor of Financial Economics and Accounting at the University of Granada, Spain. He is a member of the expert group of the EUDEFI-Project (European Union - Delivering Excellence in Financial Investigation) which aims to strengthen and standardize the financial crimes investigation in the European Union. He is Academic Director and tutor of the course 'Techniques for preventing and detecting money laundering,' organized by the Virtual Training Center at the University of Granada. Prof. Gómez has published "Blanqueo Internacional de Capitales. Cómo detectarlo y prevenirlo" ("International Money Laundering. How to detect and prevent"). Ediciones Deusto, 2007.*

The Pakistani Madrassah and Terrorism: Made and Unmade Conclusions from the Literature

by Nikhil Raymond Puri

Source: http://www.terrorismanalysts.com/pt/index.php?option=com_rokzine&view=article&id=130&Itemid=54

Abstract:
This paper revisits the relationship between Pakistani religious schools and terrorism. While much of the literature informs the enduring perception that madrassahs breed terror, some recent studies have begun to question the extent to which religious schools drive militancy. The analysis below balances these ostensibly incompatible positions – alarm and skepticism are equally misplaced. With a focus on evidence, and warranted and unwarranted conclusions provided by the literature, this paper seeks to establish what we do and do not know about the madrassah-terrorism relationship. In the process, it renders a preliminary mechanism linking the madrassah to the terroristic incident.

Introduction

Since 9/11, analysts have desperately combined estimates and educated guesses to maneuver the unknowns of Pakistan's madrassah landscape. For much of the last decade, the only certainty with regard to this elusive institution was its indisputable role in promoting terrorism. Yet recent scholarship questions the true threat posed by Pakistani madrassahs. Questions have evolved from how best to reform Pakistan's madrassahs to whether or not to do so. Concerns have shifted from the alarmist view that madrassahs are "weapons of mass instruction," to the skeptical position that the madrassah merely presents a "scapegoat" amidst other more worrying sources of radicalisation.

This paper reviews the literature on Pakistani madrassahs as discussed in the context of terrorism. Lest one get carried away by alarmist generalisation or skeptical vindication, it seeks to put in perspective the arguments housed by the literature. Towards this end, the paper is broken down into six sections:

- Section one uses counterfactual analysis to establish that madrassahs facilitating terrorism constitute important, yet far from exclusive, avenues of radicalisation.
- Section two addresses the prevalence of madrassahs in Pakistan and the proportion of Pakistani children enrolled in religious schools. It suggests that only a small minority of

Pakistani youth is exposed to militant madrassahs. Keeping these findings in mind, sections three to six explore the why, when, and how of the militant madrassah's contribution to terrorism.

- Section three studies the impetus for Islam in Pakistani politics – is it primarily top-down, or does it also respond to demands from below?
- Examining the history of internal and external patronage of Pakistani madrassahs, section four proceeds to show that top-down engineering was essential in generating the militant amongst Pakistan's madrassahs.
- Section five reconciles the alarmist's stance that madrassahs are "incubators of terrorism" with empirical observations that few militants come from religious schools. It shows that madrassah graduates are recruited as terrorists when alternative sources of militant supply are either undesirable or unavailable.
- Section six presents the main non-educational functions of the militant madrassah – radicalising to-be terrorists, providing a transit point for pre-radicalised visitors, and generating public support for extremist violence.

For the purpose of this discussion, a madrassah is defined as a religious school attended on a full-time basis. This definition stresses the institution's role as a substitute (not supplement) to Pakistan's mainstream public and private schools, thus differentiating it from *maktabs* (part-time religious institutions).

Probing the Counterfactual

The literature on Pakistani madrassahs suggests that the presence of a madrassah is an unnecessary and insufficient precondition for terrorism. With regard to necessity, the counterfactual – that the absence of a madrassah is accompanied by the absence of terrorism – fails to withstand empirical scrutiny. Ironically, the single event that most successfully brought madrassahs to the forefront of international attention – 9/11 – was executed by 19 men, none of whom graduated from a madrassah. Instead, they were educated in "Western-style institutions." Such evidence of "high quality" terrorists is not uncommon. In examining the profiles of 79 terrorists involved in "five of the worst anti-Western terrorist strikes in recent memory" (the 1993 World Trade Center bombings, the 1998 Africa embassy

bombings, September 11, the 2002 Bali nightclub bombings, and the 2005 London bombings), Peter Bergen and Swati Pandey find the average terrorist to be well educated. While 54 per cent of their sample had attended college, the authors point out that "only 52 per cent of Americans can claim similar academic credentials." Marc Sageman similarly observes a relatively strong correlation between educational achievement and terrorism. He samples 172 terrorists to find that a majority exhibit above-average educational qualifications with respect to the societies to which they belong. Surely the literature abounds with pairings of high-profile terrorists on one hand, and the respectability of their profession or alma mater, on the other: Omar Sheikh attended the London School of Economics, Ayman al Zawahiri was a pediatric surgeon, Mohammad Atta studied architecture, so on and so forth. Thus, as Christopher Candland notes, "there is no evidence that an education in the sciences [or any other non-religious subject] ensures students will not become militants."

The counterfactual has also been probed in a Pakistan-specific context. To the extent that the 9/11 Commission Report is correct in terming madrassahs "incubators of violent extremism," in Pakistan they do not operate alone. According to Andrew Coulson, "the presumption that Pakistan's state schools promote tolerance is mistaken." Instead, suggests Pervez Hoodbhoy, "Pakistani schools – and not just [madrassahs] – are churning out fiery zealots, fuelled with a passion for jihad and martyrdom." The Sustainable Development Policy Institute (SDPI) tells us that the public school curriculum exposes students to "material that is directly contrary to the goals and values of a progressive, moderate and democratic Pakistan." In a 2003 survey, Tariq Rahman compared "militancy and tolerance" among students of religious, Urdu-medium public, and English-medium private schools in Pakistan. Though based on a potentially unrepresentative sample, Rahman's findings suggest that public school graduates are only moderately more tolerant than the madrassah student. Asked whether Pakistan should prioritise taking "Kashmir away from India by open war," 40 per cent of public school respondents said "yes" compared to 60 per cent of madrassah students and 26 percent of private school students who shared this sentiment. Similarly, when asked whether they approved of taking "Kashmir away from India by supporting jihadi groups," 33 per cent of public-schooled respondents said "yes" compared to 53 per cent of madrassah students and 22 per cent of those in private schools.[10]

Another indication that non-religious schools conduce to militancy emerges from recent work on de-radicalisation. Project Sabawoon, aimed at "the de-radicalisation and de-indoctrination of captured young suicide bombers" in the Pakistani province of Khyber Pakhtunkhwa houses 84 young radicals, a majority of whom studied in government schools (not madrassahs) prior to their recruitment by militants. Coupled with the fact that only 54 per cent of Pakistanis are literate, such observations lead Rebecca Winthrop and Corinne Graff of the Brookings Institution to conclude that "Pakistan's low attainment ratios and poor quality of schooling in and of themselves" propel militancy across the country."

As part of its ongoing effort to remedy this situation, the U.S. committed $264.7 million for 2010 towards basic education in Pakistan. But some scholars express doubt in any reform programme targeted primarily at the public sector. They question the wisdom in promoting a public school system that has proven to be "sectarian, pro-jihad, and anti-minority." Even if their curricula were relatively neutral, a massive injection of funds alone may not be capable of reviving Pakistani public schools. Coulson warns that public schooling systems can fall short even in countries like the United States where the government spends "nearly $10,000 per pupil per year." Coulson encourages donors to shift their attention towards fee-charging private schools where parental oversight and adequate incentive structures are in place.

This discussion of proposed reform strategies is intended only to reinforce a central point of agreement that runs through the literature – one need not attend a madrassah to become a terrorist, neither in Pakistan nor anywhere else. If madrassahs constitute potentially useful ingredients in the manifestation of terrorism, they also exhibit some level of dispensability in its underlying (causal) mechanism. Their capacity to radicalise competes with other viable and arguably more prevalent avenues of indoctrination. It is important to note, however, that evidence towards dispensability by no means implies exoneration. While this section establishes only that madrassahs are not required for terrorism to take place, the following section considers the literature's treatment of an equally important fact – the minority of Pakistani madrassahs are involved in terrorism.

Counting Pakistan's Militant Madrassahs

Disagreement persists with regard to the headcount of Pakistani madrassahs as with the total population of students enrolled therein. A number of factors make it difficult to determine Pakistan's true madrassah population. For one, a chain of madrassahs run by a single trust is often registered as one institution. Conversely, an institution of religious learning (such as a *maktab*) that assumes only a subset of the responsibilities of the madrassah is often considered a full-fledged madrassah.[16] Most importantly, however, the voluntary nature of registration makes it very likely that a significant proportion of madrassahs remains invisible. Struggling to accept one guess over another, most scholars agree to disagree within a particularly broad (and generally unhelpful) range of 10,000 to 45,000 madrassahs.

Since the total tally of Pakistani madrassahs remains unknown, one cannot rely on "establishment surveys" (which add enrolment numbers for each individual institution) to determine total enrolment. Consequently, a World Bank study by Tahir Andrabi, Jishnu Das, Asim Ijaz Khwaja and Tristan Zajonc tries to achieve this task by relying on a combination of "household surveys" wherein each household is probed on the enrolment status of every child. Its assessment, which most scholars accept as fairly reliable, suggests that only about 0.3 per cent of Pakistanis aged five to 20 years attend madrassahs. Though districts bordering Afghanistan exhibit higher madrassah enrolment, Andrabi et al. argue, it never exceeds 7.5 per cent. Allowing for an annual enrolment growth rate of five per cent for every year since their last survey and including a further 15 per cent for orphans who evade any household survey, Andrabi et al. "arrive at a liberal estimate" of 475,000 madrassah students.

What do such estimates imply for the relationship between Pakistani madrassahs and militancy? Winthrop and Graff present the "fact that there are far fewer [madrassahs] in Pakistan as a share of all schools than previously thought" as partial refutation of "the argument that [madrassahs] are primarily responsible for the rise in militancy." That madrassahs constitute the "primary" force behind militancy, however, is a claim few scholars make. A brief examination (in section four) of the institution's top-down manipulation towards political objectives sufficiently demonstrates that the madrassah, to the extent that it is involved in militancy, functions as a tool – no more than an intermediate variable in causal terms. Winthrop and Graff's argument also implies that madrassahs are able to promote militancy by virtue of their market share in Pakistan's larger educational landscape. Such an assumption, however, is misplaced.

According to historian William Dalrymple, "it is not madrassahs per se that are the problem so much as the militant atmosphere and indoctrination taking place in a handful of notorious centers of ultra-radicalism." Lending a number to this problematic "handful," the literature presents us with the (admittedly unsubstantiated) suggestion that 10 to 15 per cent of Pakistan's madrassahs have militant affiliations. Working with Andrabi et al.'s "liberal" figure of 475,000 madrassah students, and assuming a uniform distribution of students across militant and non-militant madrassahs, a 10 percent "militancy rate" tells us that some 47,500 students attend Pakistan's militant madrassahs at any given time. Though Andrabi et al.'s estimate deflates by as much as 200 per cent, the pool of potential militant recruits, it is difficult to conclude, as Winthrop and Graff do, that 47,500 individuals "are too few to have a major impact on militancy across the country."

What can be deduced from the low market share of religious schools is that as a proportion of the population Pakistani madrassah students are fewer than initially thought and that as a consequence those exhibiting militant affiliations are still fewer. Evidence provided by the literature does not justify claims to the effect that this reduced prevalence coincides with a diminished motivation or capacity to influence militancy. The literature is certain that: 1) madrassahs are not required for terrorism to occur; and, 2) graduates of a majority of madrassahs will likely remain uninvolved in terrorism. With these points in mind, the remainder of this paper narrows its focus to discuss more strictly the minority of militant madrassahs that do help in promoting terrorism, and the manner in which they do so.

Islam in Pakistan – Instrumental or Primordial?

Reliance on Islam as a political tool has been a hallmark of Pakistan's leadership, whether civilian or military. The extent of this reliance has ranged from ad hoc "Islamic" postures to pervasive religious institutionalisation. Ayub Khan placed himself on the spontaneous end of the spectrum when he sought the support of the *ulema* (clergy) to discredit Fatima Jinnah in her presidential bid. Similarly, Yahya Khan backed Islamist parties in East and West Pakistan when challenged by Zulfikar Ali Bhutto and Mujibur Rahman. Bhutto continued in this tradition of insincere religiosity when faced with pressure from

the Jamat-e-Islami (JI, Islamic Party), Jamiat Ulema-e-Islam (JUI, Islamic Party of Religious Leaders), and Jamiat Ulema-e-Pakistan (JUP, Party of Religious Leaders of Pakistan). He declared Pakistan an Islamic state, banned liquor shops, declared Friday a weekly holiday, embarked on his pet projects of "Islamic socialism" and the "Islamic bomb," and declared Ahmadis non-Muslims. If these leaders used Islam in an ad hoc and blatantly instrumental manner, Gen Zia-ul Haq gave people more reason to trust his sincerity. A practicing Muslim, Zia sought to establish an Islamic society and economy. Concrete steps in this direction included the Zakat and Ushr Ordinance, the Hudood Ordinance, and instructions towards regular observance of prayers.

But underlying Zia's religiosity was a well-calculated political logic. In surveying the nature and content of Islamisation measures, Hina Jilani finds that Zia implemented Islam only in those areas where he sought to curtail rights. Omar Noman tells us that in the political domain Zia's Islamisation measures were intended to legitimise military supremacy while in the social realm they were aimed at extending state control to individuals' personal lives – an effort manifest in his instructions on daily prayer. Hassan Gardezi also agrees that Zia's version of S*haria* (set of rules derived from the Quran and the Sunnah, or compilation of Prophetic traditions) was limited to those aspects that extended the coercive apparatus to the individual's private domain. These observations give David Taylor reason to believe that Islamisation under Zia was "concerned only with the husk and not the core of Islam." Thus even at its most pervasive, Islam was not implemented in its totality, but only to the extent that it served to consolidate and sustain political power.

How then does Islam relate to Pakistani politics? Paul Brass draws a distinction between two ways of viewing Islamic ideology: the instrumentalist approach and the primordial approach. The instrumentalist approach sees Islamic ideology as a convenient means employed towards political objectives. The primordialist approach, on the other hand, "stresses the innate mobilizing and inspiring strength of the appeal of Islamic values and norms." Mustapha Kamal Pasha describes the same pair in terms of "official Islam" on one hand, and "popular Islam" on the other. An instrumentalist reading would suggest that the apparent prominence of Islamic political parties exaggerates their real popularity. This distortion, according to Mohammad Waseem, arises as the military makes it possible for religious parties to remain visible in the public realm, while disallowing other sections of society the same extent of participation. Agreeing with this analysis, Stephen Cohen believes that the power of religious parties lies primarily in their underlying state patronage and in their nuisance value. This view of religious party

as spoiler lends credence to the instrumentalist position, as it resolves the apparent paradox between the visible extent of Islamisation in Pakistani society and the continued failure of religious parties to perform at the polls.

The literature in turn provides a relatively weaker case against Islam as a purely instrumentalist force. According to Pasha, an instrumentalist reading overlooks the fact that leaders have often used religion in response to the religious consciousness of a particular constituency. In Zia's case, for instance, he was aware that his policies would appeal to a large section of the *petite bourgeoisie.* Pasha believes the entire project of Islamisation to be driven by an element of duality: Zia's hypocrisy (supply of religious ideology) was accompanied by the presence of willing consumers (demand for religious ideology). This position is consistent with Taylor's observation that both Pakistan's founder Mohammad Ali Jinnah and Bhutto perceived a general Islamic consciousness amongst Pakistan's masses. But what lies behind this consciousness? According to Gardezi, groups with an ambiguous position with respect to relations of production stand to benefit from extending their control over the religious sphere. Thus to the extent that Pakistan's rising middle classes have supported Islamic parties and policies, he suggests, they have done so to bolster their material interests. Pasha explains Islamic consciousness differently. Capitalist expansion, according to Pasha, yields uneven development. While it causes some to embrace it fully and westernise, others are willing only to accept its material components. Disillusioned with its accompanying "cultural haemorrhage," these latter sections find solace in Islam. Dalrymple would likely append to this list of theories his belief that religiosity in Pakistan cannot be divorced from American foreign policy and its impact on South Asia.

This issue of primordialism is also informed, albeit indirectly, by Andrabi et al.'s aforementioned study of schooling choice. Amongst households sending a child to a madrassah, Andrabi et al. find that "less than 25 per cent send all their children to [madrassahs]." Instead, the authors suggest, "50 per cent send their children to both, madrassahs and public schools, and another 27 per cent use the private school option." Based on this finding, they conclude that arguments citing religiosity as a determinant of madrassah enrolment cannot overcome this "substantial variation within households." But this preference for mixed schooling options may confirm little more than Clifford Geertz's observation that the mosque and the market often coexist. It could be that by sending one child to a madrassah and the other to a private school, parents retain their religiosity while simply complementing it with a rational desire to mitigate risk. The continued symbiosis between instrumentalism and primordialism inevitably makes it difficult to assign either tendency independent weight as a determinant of developments in Pakistan. That being said, a closer look at the evolution of madrassahs since the late 1970s suggests that the machinations of willing patrons have been indispensable in making Pakistan, by some measures, the most dangerous place on Earth.

Patronage, its Effects and their Persistence

Pakistan's madrassah landscape provides a good showcase for the continued symbiosis between instrumentalist and primordial tendencies. In the late 1970s, a number of domestic and international factors combined to make the madrassah a hot commodity for internal and external patrons alike.

According to Coulson, "until the late 20th century, it was unusual for a government to harness the schools of another sovereign nation to achieve its own ends." All this changed with the onset of the Iranian Revolution and concurrent American concerns over the Soviet invasion of Afghanistan. The Iranian Revolution in 1979 had a tremendous impact on Pakistani madrassahs. Fearful that Shia ascendance might radiate outward, Sunni states, including Saudi Arabia and Iraq, sought to curtail Iran's influence. These geo-strategic concerns coincided with Zia's own home-grown troubles. As Vali Nasr explains, Pakistani Shias became increasingly disenchanted with Zia's Islamisation policies, which were based on a narrow Sunni interpretation of Islam, and dismissed by Shias as mere "Sunnification." Eager to pre-empt an externally-inspired challenge to his authority, Zia was happy to join hands with his Arab friends. Before long, Nasr suggests, a "Sunni wall" was built along Pakistan's border with Afghanistan and Iran. Thus, Pakistan's Sunni and Shia madaris became proxies in the larger "battlefield for Arab-Iran disputes." Nasr views this external patronage, particularly from Saudi Arabia, as a necessary stimulus for the proliferation of madrassahs:

In order to have terrorists, in order to have supporters for terrorists, in order to have people who are willing to interpret religion in violent ways, […] you need particular interpretations of Islam [that] are being propagated out of schools that receive organizational and financial funding from Saudi Arabia. In

fact, I would push it further: that these schools would not have existed without Saudi funding. They would not have proliferated across Pakistan […] without Saudi funding. They would not have had the kind of prowess that they have without Saudi funding, and they would not have trained as many people without Saudi funding.

It is important to note that the madrassahs employed towards these ends were carefully selected. As one commentator points out, Zia's administration was unwilling to back just any Sunni madrassah – "the military government invariably favoured the Deobandis." Such patterns may help explain why Barelvis, who make up a majority of the country's population, run only 25 per cent of its madrassahs while Deobandis, who account for around 15 per cent of the population, disproportionately operate over 60 per cent of the country's madrassahs.

Around the time Sunni quarters became watchful of developments in Iran, the US grew increasingly pre-occupied with the Soviet presence in Afghanistan. Recognising that any American plan to drive the Soviets out of Kabul required Pakistan's cooperation, Washington was eager to bring Zia on board. In 1980, Jimmy Carter sought to entice Zia with an offer of $400 million over two years. Cognizant of his indispensability, Zia compelled Washington to revise its meager offer, calling it "peanuts". The following year, the Reagan administration more generously offered to supplement its covert funding with a five-year, $3.2 billion package. Having signed the deal, the US and Pakistan embraced "Operation Cyclone," to purge Afghanistan of its Soviet presence. The modus operandi: to promote a jihadi culture and its most "pliable" vehicles – an army of Mujahideen. In this cause, says Coulson, "American taxpayers [underwrote] ... the publication of textbooks inciting holy war on Soviet troops." USAID invested over $51 million to publish and distribute "textbooks [13 million volumes] that gave religious sanction to armed struggle in defence of Islam." These books ensured that students learned only as much as their (politically dictated) cause demanded of them. A fourth-grade mathematics text informs students that "the speed of a Kalashnikov bullet is 800 meters per second." Equipped with this cue, they are then asked to solve the rest of the problem:

If a Russian is at a distance of 3,200 meters from a mujahid, and that mujahid aims at the Russian's head, calculate how many seconds it will take for the bullet to strike the Russian in the forehead?

The benefit of hindsight prompts Coulson to conclude that "any US strategic gains from funding militant Islamist education during the 1980s were negligible compared to the long-term harm wrought by that policy." When America pulled its money and interest out of Pakistan in the late 1980s, however, such a proposition seemed ridiculous. Consequently, Pakistani leaders chose to retain what they considered a high-yielding strategy:

The success of the mujahideen in driving out the Soviets and the Taliban in capturing the Afghan state created an illusion among a section of the Pakistani policy-makers that similar success could be achieved in Indian-held Kashmir.

In fact, Pakistani leaders have seen in Islam a potent foreign policy instrument. As Veena Kukreja points out, the Pakistani establishment has consistently used jihad as a tool to check India and Afghanistan. In this effort, Pakistan's premier spy agency, Inter-Services Intelligence (ISI), and political parties under its wing – including the JI – have extended support to militant outfits in Kashmir. This point speaks to the state's geo-strategic calculus: weaken India and undermine disagreeable governments in Afghanistan. According to Oliver Roy, "while US policy-makers can indeed be credited as the mid-wife of this retrograde band of armed madrassah students, the Pakistani military and politicians deserve the distinct honour of being their guardian." Cohen agrees that the Pakistani army has godfathered many a militant tendency:

Pakistan's radical groups are a mixed lot. Some are criminals trying to wrap themselves in the mantle of divine justice. Some have modest, Pakistan-related objectives. Some are seized with sectarian hatred. A few are internationalist apocalyptical terrorists in tune with the al Qaeda philosophy. The rise of all radical groups to prominence, however, can in large part be attributed to the patronage they have received from the Pakistan army.

There is little indication that such patterns of patronage are history. Recent evidence suggests that military and non-military leaders continue to tolerate, and even actively support, known militant groups and their networks of militant madrassahs. As a number of scholars note, it is likely that Pakistani intelligence officials know which amongst Pakistan's madrassahs are militant. Yet, strategic calculations and an incessant quest for political legitimacy keep Pakistan's leadership from lifting a finger against religious political parties, militant outfits, or madrassahs. As a result, Dalrymple points out, "not even

one militant madrassah has yet been closed down." More worrying still, Maulana Sami-ul Haq, director of the infamous Madrassah Haqqania, is confident that any official promise to crackdown on radical madrassahs "is for American consumption only." In fact, this madrassah has only been "forced" to shut down on one occasion – when in 1997 it deployed its entire student body to support a stalled Taliban offensive across the border.

In September 2003, a number of Southeast Asian students were arrested from Karachi's Jami'at al-Dirasat al-Islamiyya. Though "authorities swooped down on [the madrassah's] Malaysian and Indonesian students," they did little to address a more concerning aspect of their visit. On the day of the arrests, Hafeez Muhammad Saeed, leader of the Jamaat ud Dawa (an organisation known to be linked, if not synonymous, with the banned Lashkar-e-Taiba), was in attendance as the chief guest. His presence, however, was blatantly tolerated. More recently, in April 2010, Rana Sanaullah, Punjab's law minister, visited a madrassah run by the banned sectarian group Sipah-e-Sahaba Pakistan (SSP). He was later seen sharing a car with the madrassah's leader. Three months later, the PML-N government in Punjab, headed by Nawaz Sharif's brother, Shahbaz Sharif, provided the Jamaat ud Dawa a $950,000 grant for its educational activities. In July 2010, Wikileaks belatedly revealed documents suggesting that in 2006 Lt-Gen Hamid Gul (retd) and other ISI operatives visited madrassahs in Khyber Pakhtunkhwa in an effort "to recruit new fodder for suicide bombings."

As Christopher Blanchard notes, "channels of responsibility between donors and recipients for curricular development and educational control are often unresolved or unclear." Consequently, it becomes difficult to corner either patrons or clients as bearers of greatest culpability. Nevertheless, in the context of the instrumentalism versus primordialism debate, it is important to recognise that "traditionally, jihadi texts are not a part of the normal curricula of [madrassahs]." Though patronage cycles and their ephemeral goals are never long in vogue, the consequences of such manipulation have proven to be more enduring. "The absence of US support for [madrassahs] in the 1990s," says Ali Riaz, "did not bring an end to the proliferation of madrassahs." As a 2002 International Crisis Group report suggests, even when patronage ceases, its propaganda persists "develop[ing] a dynamic independent of its original patrons." Left to primordial tendencies alone, however, Pakistan's madrassahs would likely have evolved along a different trajectory. This brief account of Pakistan's history since the late 1970s lends support to the verdict that instrumentalist tendencies (on the part of internal and external sponsors) were essential in generating and promoting the more "militant" amongst Pakistani madrassahs. By itself, the presence of a madrassah is an insufficient condition for terrorism to occur.

The Madrassah and its Latent Utility to Terrorist Organisations

To understand the relationship between militant madrassahs and terrorism, some scholars suggest it may be useful to work backwards in the causal mechanism. Rather than treat "terrorism" as a uniform concept, they disaggregate it into discrete categories, asking how each type relies on madrassahs differently. The main lesson gleaned from this section of the literature survey is that a madrassah's capacity to contribute to terrorism depends heavily on the type of terrorism in question.

Qandeel Siddique divides violent extremism in Pakistan into four categories or types of jihad on the basis of target choice: Type I jihad, representing "global jihad" targeted primarily at the West; Type II jihad, involving cross-border terrorism executed against India and Afghanistan; Type III jihad, involving violence directed at Pakistan's government and security forces; and, Type IV jihad, representing sectarian violence. Though he discerns "weak to strong bonds" between madrassahs and type II, III and IV jihad, Siddique suggests that "there is little evidence supporting a connection between" madrassahs and type I terrorism. This finding reaffirms Dalrymple's opinion that "militant [madrassahs] are [...] likely to create more problems for Pakistan's internal security than for the safety of Western capitals." In fact, Bergen and Pandey contend that with regard to the security of Western interests, the madrassah merely presents a "scapegoat." They consider "misguided" a "national security policy focused on [madrassahs] as a principal source of terrorism."

Such conclusions build on the assumption that "perpetrating large-scale attacks requires ... a facility with technology" that "is simply not available at the vast majority of [madrassahs]." The logic here is that madrassahs fail to supply the human material required to successfully execute a terrorist attack. In other words, the supply of motivation is unaccompanied by an equally important supply of capacity. But in their disproportionate focus on "militants who successfully executed an attack or who were caught in the

act," Bergen and Pandey fail to consider that the capacity of madrassah graduates to execute type I jihad may only be veiled by a ready supply of more capable alternatives.

Christine Fair's work on militant recruitment posits that the low representation of madrassah students "in the ranks of the observed militants" is likely attributable "to the efforts of *tanzeems* [militant groups] to select for quality among their operatives." "Even if [madrassah] students are more inclined towards jihad," says Fair, "a given militant group may not select [madrassah] students if the group has other, more desirable candidates to recruit." To understand what engines such a quality-driven demand for recruits – what makes one recruit more "desirable" than the other, Fair looks at "the objectives, tactics, theatres, and 'quality of terror' produced" for each particular *tanzeem*. Thus shifting the unit of analysis from the individual recruit to the recruiting entity, Fair makes her case by comparing the operations of two Pakistani *tanzeems* – Lashkar-e-Taiba (LeT) and Lashkar-e-Jhangvi (LeJ).

LeT concerns itself primarily with type II jihad, a commitment most evidently displayed through a host of high-profile anti-India terrorist operations – the 2001 attack on the Red Fort in New Delhi, the 2006 express train bombings in Mumbai, and the 2008 terrorist assault on Mumbai commonly known as 26/11. In order to successfully "engage hard targets in demanding high-risk missions," LeT inevitably demands that its recruits meet a minimal standard of quality. As Fair points out, carrying out "operations deep within India" requires not only that cadres be able to navigate the "high-altitude Line of Control" separating Pakistan from Indian-administered Kashmir, but also that they possess the linguistic talent to "carefully evade the extensive Indian counter-insurgency grid." Moreover, LeT prefers recruits who are "literate, numerate, and capable of working out mathematical proportions," prerequisite skills for competently "building improvised explosive devices."

Unlike LeT, LeJ devotes most of its activities to type IV jihad, targeted domestically at sectarian (in this case Shia) foes. "In general," says Fair, "LeJ attacks soft or low-value targets and conducts operations for which opportunity costs of failure are low." Furthermore, unlike LeT, LeJ faces few difficulties in "getting to the theatre." A preference for "low-end tactics such as grenade tosses" also ensures that LeJ is easily contented with low quality recruits. Thus, given the "kinds of operations" for which LeT and LeJ are known, one can assess the utility of the madrassah student for each group. While knowledge of current target preference and operational sophistication "suggests that few LeT operatives are [madrassah] products," the opposite is true for LeJ. In Fair's assessment, "given LeJ's sectarian mission, students with some [madrassah] background may be preferred to those without [madrassah] experience, all things being equal."

But Fair recognises that changed conditions and "repurposed" *tanzeems* are not unheard of. Consequently, she contends that is problematic to "conclude that madrassahs are exculpated because their students fail to be accepted by *tanzeems* under current recruitment conditions." Surely, scholars and policymakers are increasingly cognisant of the overlap between different types of terrorism. According to Ashley Tellis, coordination between *tanzeems* "through the entire spectrum of jihadi groups" makes them "much more flexible in their cooperation now than they ever were historically." Though Hafeez Mohammad Saeed and the Jamat ud Dawa (JuD) are primarily associated with type II jihad, evidence suggests that Saeed's purpose is less restricted. In 2007, Saeed emphasised the virtues of jihad against the "US and its agents." He also harbours an expressed desire to extend the writ of Islam to New Delhi, Tel Aviv, and Washington. Lending credibility to his rhetoric, the LeT was behind a foiled 2009 plot to attack the American, British, and Indian embassies in Dhaka. According to Stephen Tankel, "fighting the West remains a secondary concern for Lashkar, but one to which it has committed increasing resources during the past several years." Thus, accompanying Saeed's primarily type II jihadist mindset and activities is a proven readiness to contribute to type I jihad. Masood Azhar is known to be the prime beneficiary of the 1999 hijacking of flight IC 814 (Indian authorities released him in exchange for all passengers), and as the leader of JeM, a militant group avowedly committed to type II jihad. Nevertheless, Azhar advocates a jihad that involves breaking both Indian and American legs. The Sipah-e-Sahaba Pakistan (SSP) is a sectarian group best known for its type IV sectarian activity against Pakistan's Shia minority. Yet, the organisation's former leader, Azam Tariq, ardently supported type II jihad in Kashmir, resolving to send "500,000 militants to Jammu and Kashmir to fight Indian security forces." The LeJ, also a group committed to type IV jihad, has supplemented its anti-Shia activities by sending suicide terrorists nearer to the Durand Line to fight Pakistani security forces in Federally Administered Tribal Areas (FATA) – a symptom of type III jihad. Thus one does well to heed Cohen's

advice that "an American policy designed to curb existing terrorism in Pakistan should deal with all [forms of terrorism]."
More importantly in the context of this paper, all militant groups in Pakistan – LeT and JeM (primarily tied to type II jihad), SSP and LeJ (at the forefront of anti-Shia type IV jihad), the Tehrik-e-Taliban Pakistan (TTP, an emergent leader in type III jihad against the Pakistani state), and more immediately anti-American entities (such as the Haqqani network) – inevitably enjoy close associations with madrassahs. Though Fair succeeds in explaining why different types of terrorism (and *tanzeems* thereto devoted) should rely differently on madrassahs, she does not tell us why all *tanzeems* tirelessly continue to promote madrassahs. The persistent proximity between *tanzeems* and madrassahs beckons the question: do the aforementioned arguments adequately consider the full range of functions madrassahs provide to *tanzeems* and their operations? Do madrassahs present more than a reserve recruit base? Might they less visibly (though no less significantly) contribute to the execution of a terrorist attack?

The Madrassah and Its Contributory Roles

The previous section shed light on the diversity of purpose exhibited by Pakistani madrassahs. But madrassahs can also assume different contributory roles in the build-up and execution of a particular terrorist event. A few such functions alluded to in the literature include: 1) radicalising to-be terrorists, 2) providing transit and hospitality to pre-radicalised individuals, and 3) generating support for terrorism. While supply-side explanations profile the individual militant, and the *tanzeem* approach focuses on the needs of a particular militant group, this section treats the madrassah as its unit of analysis.

Radicalisation

According to Kalsoom Lakhani, the madrassah is able to indoctrinate by severing and replacing connections with home. A young and malleable child is pulled away from his parents, detached from his origins, this child finds a new surrogate in the shape of the madrassah. Insulation from opportunities of critical thought, plus reverence for an acquired parent prompt the child to accept sermons without question or doubt.[98] This process speaks to the grassroots component of militant madrassahs. The madrassah radicalises young entrants into aspiring terrorists who graduate into *tanzeems* before making a more tangible contribution to terrorism. A number of JI madrassahs – including Markaz Uloom-e-Deeniya's Alfalah Academy, Jamiatul Ikhwan, and Jamia Darul Islam – have adopted this formula by directing students towards martyrdom via militant outfits like Hizbul Mujahideen.[99] According to Siddique, such collusion between madarssahs and *tanzeems* is widespread. When the JeM organised a conference in the Pakistani city of Bahawalpur in 2008, he points out, "some madrassah managers to figure prominently" in the audience included Maulana Sher Bahadur of Darul Uloom Hijra Attock, Mohammad Shah Saleem of Darul Bannu, and Maulana Qari Khalil Ahmad Bandhani of Jamia Ashrafia Karachi. Also present (as guest speaker) was Maulana Jalandhry who heads the Wafaq-al Madaris – the umbrella of Deobandi madrassahs in Pakistan – in addition to his own madrassah (Khair-i-Madaris in Multan). The close affiliation of these madrassah managers to an overtly militant group all but ensures that the students enrolled in their madrassahs are exposed to ideas that converge with their own. Qari Hussain, a Taliban commander commonly referred to as "Trainer of Suicide Bombers," justifies the radicalisation taking place at many madrassahs: "Children are tools to achieve God's will. And whatever comes your way, you sacrifice it." Thus, treating all children as sacrificial lambs, the militant madrassah is able to radicalise innocent children towards their own violent ends. But to the extent that a militant madrassah contributes to terrorism, it does not always constitute a (lone) site of radicalisation.

Transit and hospitality

According to terrorism analyst B. Raman, Western Muslim youth "of Pakistani origin studying in the [madrassahs] of Pakistan fall into two categories – those who are sent by their parents in order to dilute the Western cultural influence on them and those who come on their own in order to contribute to the cause of their religion." In 2004, 21-year old Shehzad Tanweer, one amongst the four men who carried out the 2005 London bombings, spent four months in a madrassah in Lahore. As Bergen and Pandey see it, Tanweer "made a conscious decision to travel halfway around the globe to attend [a] radical Pakistani [madrassah] after [he] had already been radicalised in [his] hometown of Leeds in the United

Kingdom." In Raman's terms, Tanweer corresponds to that category of individuals who "are already strongly anti-West before joining the [madrassah]." But why bother to visit a madrassah when the task of radicalisation is a fait accompli? Unable to do more, suggests Siddique, militant madrassahs supportive of type I jihad might "allow their [madrassahs] to be used as transit points, brief visitations or as safe havens." A madrassah in Rawalpindi served as a transit point to Hamid Hayat (the teenager from Lodi, California, arrested in 2005 for his affiliation with Al Qaeda) before directing him towards a jihadi training camp. Similarly, a madrassah in Peshawar hosted Bryant Neil Vinas "on his way to join Al Qaeda in waging holy war against US troops." Insofar as it serves as a transit point, the madrassah thus presents a promising destination for a small population of pre-radicalised elements with lofty goals but minimal connections.

Generating support

Radicalisation of the "sacrificial lamb" and hospitality towards the pre-radicalised tourist are roles reserved for the militant madrassah. With regard to both functions, one can employ binary terms to qualitatively distinguish Pakistan's militant from its non-militant madrassahs. Either a madrassah deliberately radicalises young boys towards violent ends or it does not. Either a madrassah is willing to act as a transit point for the budding terrorist or it is not. Insofar as the generation of support for terrorism goes, however, it is more difficult to locate a clear divisor between militant and non-militant contributions. Any differences will inevitably be quantitative in nature. While the capacity of militant madrassahs to generate support for extremism requires little elaboration, the literature suggests that most Pakistani madrassahs (militant and non-militant alike) "sow the seeds of extremism in the minds of […] students." As mentioned earlier, Rahman's survey of attitudes towards extremism and militancy reveals that madrassah students are more intolerant than students from public and private schools. In addition to their strong support for militancy against India, sampled madrassah students also exhibit greatest resistance to equal rights for Hindus, Ahmadis, and women. Dalrymple tells us that while "only a small proportion of [madrassahs] are militant," the rest also "tend to be ultra-conservative." Such evidence prompts Fair to conclude that "even if they may not contribute significantly to the pool of observed militants, Pakistan's [madrassahs] may foster support for terrorism within families and communities." Thus in the marketplace of ideas, both militant and non-militant madrassahs make quantitatively different contributions towards the legitimacy and viability of violent groups and their activities.

Conclusion

This article has focused on the literature's role in illuminating the relationship between militant madrassahs and terrorism (See Figure 1). In addition to its obvious merits, however, the literature also exhibits room for further research. The literature effectively employs different units of analysis: terrorists in supply side studies; militant groups in Fair's *tanzeem* approach; and, the madrassah, or its lead representative, in analyses of the madrassah's varied roles and functions. In addition to these approaches, it might be useful to study more closely the larger family to which madrassahs belong. In other words, as a unit of analysis, one may consider treating as one, admittedly amorphous, entity the cumulative interactions between madrassahs, *tanzeems*, and patrons in search for identifiable patterns. Does this family possess borders? Are they permeable? What causal mechanisms are at work within such families of interaction? What provisions are there for sustenance in absence of continued patronage? At present, evidence of the nexus between madrassahs and militant groups is isolated. The literature tells us that particular patrons prefer particular madrassahs, and that particular madrassahs associate with particular *tanzeems*. But the nature of interaction between these parties remains insufficiently understood.

In its treatment of the madrassah as a variable, the literature commits some level of conceptual stretching. Clearly, madrassahs serve different roles, to different extents, towards different ends, and with varying levels and sources of inducement. Yet, most studies are content with the binary distinction between madrassahs and militant madrassahs. If militant groups constitute a heterogeneous lot, and scholars accept that terrorism has its sub-types, one can likely do better than assume homogeneity within the category of militant madrassahs. The same goes for Pakistan's non-militant madrassahs. Rather than sanctify boundaries of categorisation, it might be useful to employ means of analysis that reflect differentiation within extant categories. As an elementary example, a madrassah that has "no"

role in terrorism could more usefully be described as one where most students exhibit little, if any, support for the most benign form of involvement in terrorism – e.g. impersonal sympathy for terrorist groups and their associated inclinations. Conversely, a madrassah that is heavily involved in the operations of a terrorist organisation could be described as one where most students manifest a strong desire to engage personally in the execution of a terrorist attack. The Figure below tries to capture some of the influences at work.

The changing interests and fluid patterns of patronage influencing Pakistani madrassahs are better accommodated by a rubric that captures subtlety – future scholarship ought to deepen current categorisations.

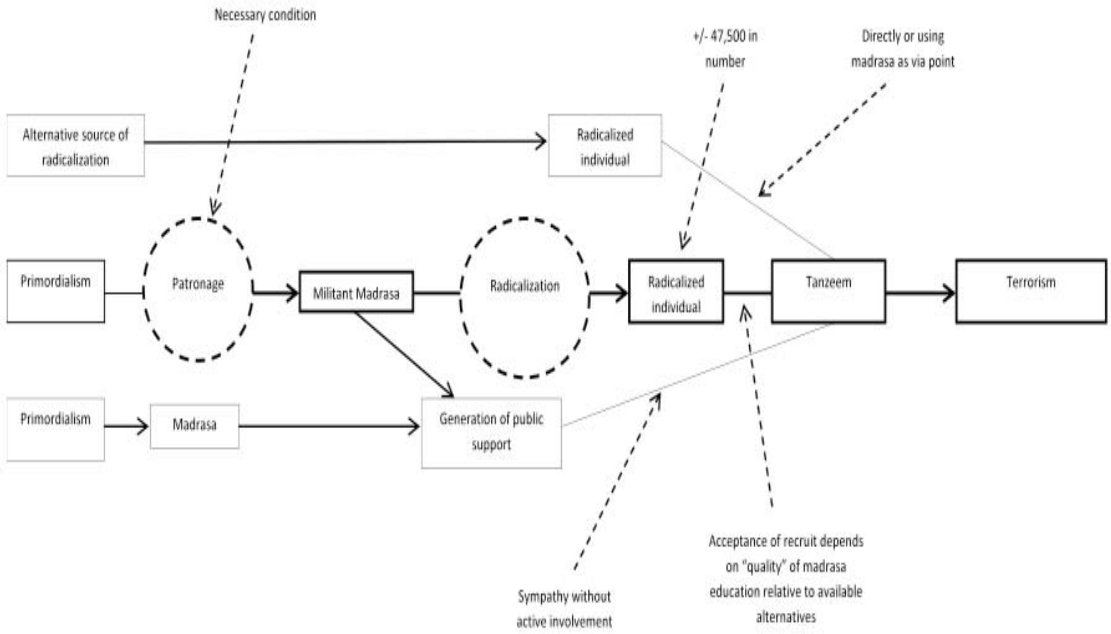


Figure 1: The relationship between Pakistani madrassahs and terrorism

About the Author: ***Nikhil Raymond Puri*** *recently completed an MPhil in Politics from the University of Oxford. His thesis, which was awarded a distinction, focused on madrassah reform in the Indian state of West Bengal. A member of Phi Beta Kappa, Puri also holds a BA in South Asian Studies from the University of Virginia. He currently serves as Research Assistant at the Terrorism Research Initiative (TRI).*

New Super Microphone Can Hear You in a Crowded Stadium

Source:http://singularityhub.com/2010/10/13/new-super-microphone-can-hear-you-in-a-crowded-stadium-video/

I have an uncanny knack for making a fool of myself when I'm in a crowd, and it always seems like everyone goes silent right when I'm saying the most embarrassing thing. Now all of you can enjoy the same feeling, thanks to AudioScope. Developed by two physicists from the University of Norway, the new super microphone can pick out single voices in a mob of people. Watch the video below to see how the technology listens in to basketball players in a full stadium. AudioScope is being actively marketed towards bringing a new intimacy to athletic events everywhere, and it may not be too long

before it singles you out of the masses as well.

What makes a microphone super? Multiplication. AudioScope is actually hundreds of smaller

microphones collected together in the same carbon fiber disk. Measuring about a meter across, the AudioScope array contains 300 individual mics and a camera with wide angle lens. Visual cues from the camera help the system estimate distances, which allows it to precisely time when sounds should arrive at each microphone. “Sophisticated signal processing algorithms” then combine the hundreds of feeds into one audio stream. With pinpoint targeting, AudioScope can listen to specific areas in its field of view, amplifying quiet sounds to audible levels. In the example shown below, the voices of players, referees, and coaches in a LA Lakers game can be heard clearly despite the noise of the stadium. It’s pretty amazing.

Developers Morgan Kjolerbakken and Vibeke Jahr have formed a new company, Squarehead Technology, to market the AudioScope across a variety of applications. The system could be used to improve video conferencing or public meetings, but the first place we’ll see it is probably in televised sports. Soccer and basketball teams (like the LA Lakers shown above) have tested the device with great success. AudioScope offers a clear advantage over traditional directional microphones: a single operator can quickly change the target area via a central control system. One AudioScope, or a few acting in concert, could cover an entire arena, allowing a television broadcaster to zoom in on a player, coach, or fan in rapid succession. In the future, sports audiences at home will be able to hear all the gritty details normally reserved for those with seats on the edge of the field.

The AudioScope's array of hundreds of mics can listen to conversations anywhere in a crowd. An easy control system (right) lets an operator quickly choose where to listen to inside the wide angle view of the camera.

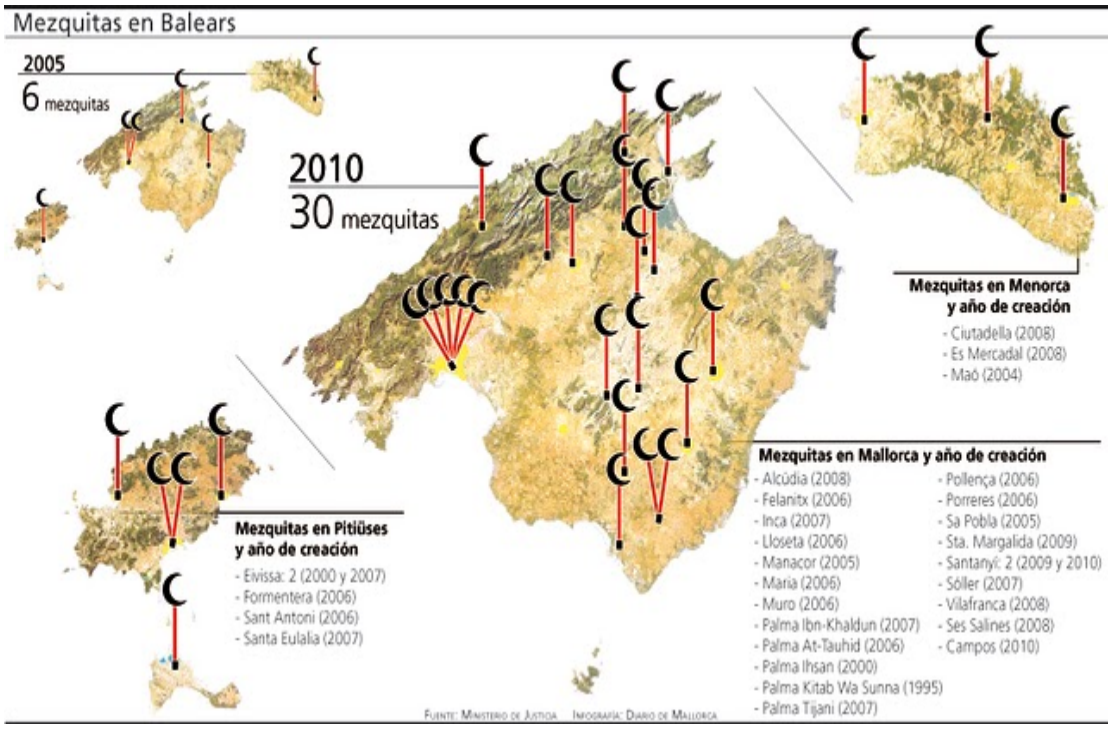
As cool as that scenario may be for fans, I’m not sure players would really appreciate it. We could all share that sentiment soon. With AudioScope, businesses and governments have been handed a perfect device for spying on people in crowds. Listening to a conversation in a packed auditorium, or bus

station, or airport would be simple. Operators at a central location could quickly move the focus of the device through crowds and monitor them for safety. Or for whatever. We've already seen how audio filtering technology will be able to take massive numbers of audio recordings and extract valuable information about how we feel about ideas, products, or people. When combined with AudioScope, such sentiment analysis technology could become much more powerful.

We've already become accustomed to the 'eye in the sky' cameras that monitor public places for security. Now, AudioScope is likely to provide similar capabilities for audio. If we are comfortable knowing that anyone could be watching us when we're at the store, airport, or sports stadium, it shouldn't be that disconcerting to know they may be listening as well. We'll have to adjust to a future where the crowd can't hide our personal conversations. Whether actively scrutinized by security guards or passively processed by corporations looking to understand their market, the things we say out loud are about to become fair game. Privacy simply isn't what it used to be.

Spain: Mosques have increased by five in the Balearic Islands

Source:http://tea-and-politics.blogspot.com/2010/10/spain-mosques-have-increased-by-five-in.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TeaAndPolitics+%28Tea+and+Politics%29&utm_content=Yahoo!+Mail



The number of mosques has increased fivefold in the Balearic Islands in recent years. In 2005 there were only six mosques in the islands and is now accounted for 30, as shows the registration of religious communities in the Ministry of Justice. The most important municipalities of the Balearic Islands have already a temple to practice Islam and Islamic groups now want also to have cemeteries to bury their dead by Muslim rites. For this reason, they plan to apply for land to the municipalities.

The real expansion of mosques has occurred since 2006, being the year 2008 when opened more Islamic centers were opened in the islands, especially in Mallorca. In most cases the faithful themselves have decorated the places with Arab tapestries. The faithful have also chosen a magnet in order to fulfill their religious obligations every Friday, the day of worship.

The reasons that Islamic groups give for the significant increase of places of worship in the municipalities is that gradually and over the years, Muslims have settled and integrated, losing the fear

of showing religious affiliation. Many of the faithful flocked to nearby towns or Palma to pray, but over the years they have decided to launch their own temples in the towns where they reside.
Francisco José Giménez, president of Mallorca's Lliga Musulmana and representative of the Islamic Platform states that "*Muslim groups of municipalities were reluctant at first to set up their mosques, but once you have settled have changed their way of seeing things and even people of Mallorca has helped offering some places*". Islamic organizations complain that at a regional level there is no a group that unites the entire Muslim community.
In 2005, on the island of Mallorca, there were only two mosques in Palma, one in sa Pobla and another in Manacor. Now there are centers of Islamic worship in Inca, Lloseta, Pollença, Alcúdia, Felanitx, Maria de la Salut, Muro, Santa Margalida, Soller, Vilafranca, Ses Salines, Inca, Santanyi, Porreres or Campos.
The Lliga Musulmana and the Islamic Council of Islands, who is chaired by Lounis Meziani, think one step further. Since mosques are already implemented in most counties, they have decided to ask the councils to provide land for the construction of Islamic cemeteries. It turns out that the Police Act which governs Islands' Mortuaries prohibits the burial of the deceased without coffins. Muslims do not use them and their religion requires burial in contact with soil, incineration is considered an act of selfishness. Mallorca cemeteries are not eligible to meet this ritual.
At the moment, they only have an area within the municipal cemetery in Palma for about 40 corpses. The municipality of the capital and has informed them that it has no more land to expand this space. In this situation, they are thinking of going through the villages of the islands with the aim they are assigned to build enclaves where Muslim cemeteries.

Study predicts women in power, Muslims heading West

By Karin Zeitvogel (AFP)

Source:http://www.google.com/hostednews/afp/article/ALeqM5iR9JqqEyu833mBTtmOmf8PirHj0g?docId=CNG.39d86b87288610357aedef0bdb96a13e.d51

In the next 40 years, an unprecedented number of women will be in positions of power, Muslim immigration to the West will rise, and office workers will be unchained from their cubicles, a report released last week says. South America will see sustained economic growth and the Middle East will become "a tangle of religions, sects and ethnicities," says the report by Toffler Associates, a consultancy set up by the author of the 1970s blockbuster "Future Shock." Toffler Associates released its predictions for the next 40 years to mark the 40th anniversary of "Future Shock," in which author Alvin Toffler studied the 1970s to see what would happen in the future. His prognosis 40 years ago was that technology and science would develop at such an accelerated pace that many people would be unable to process the enormous amounts of new information available and would disconnect from life. Some of "Future Shock's" prognoses have come true, including that news would travel around the world instantly, that same-sex couples would wed and raise families, and that violence and environmental disasters would increase and have broad consequences -- like the BP spill in the Gulf of Mexico. So it might be worth paying heed to what Toffler Associates foresees for the next 40 years, including container ships getting larger to meet increasing demand for faster, cheaper delivery of goods, and the Suez and Panama Canals being "improved." They envision more and more people growing their own food to reduce their dependence on large manufacturers and distributors, and the proliferation of high-speed Internet and low-cost video-conferencing freeing office workers from their cubicles and working from anywhere in the world. Only a very small number of states will continue to behave as "rogue" nations, Toffler Associates says, naming

North Korea and Iran. "A true test for political leaders will be in how they handle relationships with these nations and to what extent they allow them to control geo-political agendas," the consultancy says. China will position itself as a global economic power, allying with Brazil and India to influence currency use and with Venezuela and African nations to ensure its energy needs are met. The United States, meanwhile, will depend on China for 17 rare earth metals that are essential to produce everything from weapons components to radars to wind turbines and hybrid cars. The development of alternative energy forms will create "losers in a post-petroleum world" including Saudi Arabia, Iran, Iraq, several Gulf states, Russia and Venezuela, the report says. Christianity will rise rapidly in the global South, while Muslims will migrate in increasing numbers to the West, where their presence will reshape public attitudes and government policies. Climate change will fuel conflict as melting sea ice exposes mineral wealth and oil fields in the Arctic and as rising sea levels force large populations from their homes. An aging population will cause spending on long-term care services for the elderly to nearly quadruple by 2050, and social security and Medicare, the US health insurance for the elderly, will cease to "exist as we know them," Toffler managing partner Deborah Westphal told AFP. "We don't know what will replace them; we just know that we will be in a different type of society with different types of people and different needs," she said. As for women, they will take on leadership positions around the globe at a never-before-seen rate, as countries realize "you can't be successful with just 50 percent of the population participating in decision-making," Westphal said. And in the next 40 years, information-gathering will speed up even more as the world enters the Petabyte Age, Toffler Associates predicts. Petabytes -- which are 10-to-the-15th-power bytes, or measures of computer files, hard disk space, and memory -- are used today only to measure the storage space of multiple hard drives or collections of data. Between now and 2050, measuring data in petabytes will become the norm, and so will data saturation, Toffler Associates predicts.

Top 10 smart surveillance systems from Israel

Source: http://homelandsecuritynewswire.com/top-10-smart-surveillance-systems-israel

Video surveillance systems have become an important tool in enabling authorities to trace criminals and terrorists; Israel is one of the leading players in the field of intelligent surveillance; here is a list of the Top 10 video security technologies from Israel; these companies offer solutions that range from "seeing"

through walls to reducing twenty-four hours of video to a few (indexed) minutes to detecting subtle changes in the landscape to offering high-resolution under-water images, and much more. The attempted bombing in New York's Times Square highlighted, if such highlighting was necessary, the significance of video surveillance systems. Within hours of the car being discovered, police had used surveillance camera footage in a nearby shop to identify a suspicious looking man seen near the vehicle. In the London bombings in July 2005, in which fifty-two were killed and 700 wounded, police officials, using dozens of surveillance cameras placed on the streets and in railway and tube stations, were able to trace almost the entire journey of the four bombers as they prepared for the attacks. For crime too, police today turns to surveillance cameras to try to discover what took place. *Israel21*'s David Shamah writes that it is no surprise that Israel is a world leader in this field. With its ongoing national security problems, the country relies heavily on advanced video security technology to keep Israelis safe. Using expertise gleaned from the Israel Defense Force, Israeli

companies have moved quickly into the field, responding first to the needs of the local market, and then using this as a base to access the rest of the world. Today, Israeli video security companies provide some of the most advanced solutions in the world, selling to law enforcement and military authorities in Europe, the United States, and Asia. The most common innovation these companies share: smart video surveillance systems that not only observe, but also analyze, alert, and make security personnel more effective. Here is a list of the Top 10 Israeli video security companies;

1. MATE Intelligent Video. Mate's video analytics system can detect changes in the landscape. One of the biggest problems facing security organizations is worker boredom. Monitoring large banks of monitors hour after hour has a debilitating effect on the people doing the observing, and that fatigue can be exploited by those bent on breaching security. In addition to fatigue, continuity of observation is an important issue. When guards change shifts, continuity is lost, so that terrorists, if they time it right, could place a bomb hidden in a bush next to an electrical plant or in the path of a security patrol. The bush would look as if it belonged there, and no one would realize anything was out of place until it was too late. Shamah writes that to combat these two problems, MATE developed a video analytics system that can detect changes in surroundings and landscape, indicating whether anything has changed in a camera's field of observation — such as if someone or something appearing that had not been there before. When such unauthorized changes are detected, the system alerts security personnel, pinpointing the problem and allowing them to deal efficiently with the situation before it gets out of hand. MATE's technology can be used for anything from detecting suspicious activities or behavior to counting people and cars, tracking objects, or even detecting tailgating or piggybacking through access-controlled doors.

2. Adaptive Imaging. The devil, as they say, is in the details — but most video surveillance systems are weak on picking up small details in images in real time. Security personnel watching a situation develop are often missing crucial information — such as whether a potential subject is holding a weapon. Arresting an individual before the time is right could compromise an investigation months in the making — or sow unnecessary and economically damaging panic. To keep track of the details, security agencies can use a unique "panoramic telescope" developed by Yokneam-based Adaptive Imaging Technologies. The company won the Most Promising Startup award at last year's Global Security Challenge, and has received a grant from the U.S. Department of Defense. It has developed a camera with a full gigapixel (1,000 megapixels) of raw resolution. With its telescopic lens, the camera can take in a very wide field, one which would usually require a much larger number of individual cameras. Thanks to the innovative software that accompanies the camera, security personnel can focus in on a target and receive a remarkably clear picture, de-emphasizing less critical parts of a scene. The result: security personnel can zoom in on the important details, giving authorities the information they need to deal with a crisis as effectively as possible.

3. Vigilant Systems. Vigilant offers a turnkey networked video management solution. After 9/11, installing and managing video surveillance systems became a priority for city, regional, and national governments around the world. While many solutions were already on the market, managers and government officials needed a system they could deploy quickly and efficiently, that would also supply the necessary recording, analysis, and storage capabilities — and all this in a framework that would allow maximum flexibility and be able to integrate existing equipment. Many managers, especially in the United States and the United Kingdom, found that Israel's Vigilant Systems could supply those solutions. Vigilant specializes in turnkey networked video management and recording solutions, streaming high quality images over robust wireless networks, and recording them for analysis. Video from a wide variety of cameras is streamed to a single control room, where security personnel can keep an eye on a wide area, with the ability to focus in on detailed scenarios in high resolution. Vigilant's solutions have been installed in dozens of city centers and shopping malls in the United States and the United Kingdom — where there are more video surveillance cameras per head than anywhere in the world, with managers saying that the systems have been integral elements in ensuring or restoring safety.

4. Briefcam. Twenty-four hours reduced to a few minutes. Cameras are everywhere these days — but what happens to the footage they record? Often nothing happens, because there is no one to sit and sift through the endless hours of video. It is usually only after a major disaster or attack that officials check the video, hoping to get clues as to whom or what caused the problem. Briefcam's solution is its Video Synopsis product. Instead of watching the entire video, a viewer can see a synopsis — with the option of focusing in on objects or people of interest from a 24-hour period within a few minutes. If viewers notice something odd in the behavior of an individual, they can focus in on that individual, and receive an index of all his or her movements in the entire range of footage. With Briefcam VS, security personnel have a more efficient way to watch and analyze footage, making it more likely that they will catch problems before they occur.

5. Sea-Eye Underwater Technology. Not all dangers are visible to the roving camera's eye; some are hidden away, underwater. Israel has experienced several attacks at the hands of scuba-diving terrorists, and underwater pipes and other installations may also be at risk. Cameras would be useful as aids in underwater security, but the limitations on video in underwater situations — transmission of very low-resolution pictures via cameras that have to be tethered to a ship console — make underwater video impractical for security purposes. Shamah writes that the underwater video system perfected by Sea-Eye aims to overcome previous limitations by combining new advances in signal processing and video compression. A featured part of the system is a modem that allows data transmission at rates that are much more robust than in most other systems. In addition, Sea-Eye has developed algorithms to cope with underwater signal transmission problems such as multi-path reflection and Doppler effects, enabling streaming video or voice broadcasting to proceed unimpeded. The result - clearer underwater pictures with more detail - granting security services better tools to protect underwater installations.

6. AgentVI. Large facilities like airports, shopping malls, or stadiums are nowadays equipped with cameras that allow security personnel to view nearly every square inch of the facility. What is it, though, that security personnel are seeing? How can they differentiate between individuals or groups out for good clean fun, and those with crime — or terrorism — on their minds? One innovative way is by using the video analytics system developed by Agent VI (formerly Aspectus), with research facilities in Rosh Ha'ayin, in central Israel. The company's VI-System compares video to a database of behavior patterns. When a pattern is detected that indicates trouble, an alarm is sounded, alerting personnel. The alarms could be set off by images ranging from someone dropping a gym bag in the corner of a busy downtown intersection, to someone reaching behind an unattended jewelry counter in a department store. Those guys are likely up to no good — and with Agent VI's technology, the chances that security personnel can nip a crime or attack in the bud are greatly improved.

7. Magal Security Systems. Some of the softest, most vulnerable targets for terrorists are the ones where they can operate uninterrupted and unobserved. Take a reservoir, for example — a body of water that sits relatively unattended and unprotected (except for a perimeter fence), but upon which millions of people depend. Even placing a battalion of soldiers there would not necessarily be sufficient to protect such a large facility — not that governments can afford to allocate those kinds of resources anyway. One solution that has proven successful has been perimeter detection, a specialty of Magal Systems, based in Yehud in central Israel. Magal is one of the largest outdoor, major-installation security companies in the world, with offices in dozens of countries, which claims 40 percent of the worldwide market for Perimeter Intrusion Detection Systems. Using a range of tools — from video cameras to lasers to microwave sensors and more — all controlled by automated software that can instantly alert those in charge, Magal is keeping safe thousands of sensitive sites and tens of millions of people.

8. NICE Systems. To be effective, a surveillance system has to be nimble. At large facilities, security personnel must watch out for numerous threats, and any system that can ferret out the unnecessary information, delivering only the required data, is most welcome. NICE System says that this is one of the strengths of its NiceVision technology. Along with a robust network that can deliver high-quality images and simplified, unified management capabilities, NiceVision also features distributed video analysis, which streams video only when an event is detected. This ensures that security personnel see

what they need to see, while allowing them the flexibility of dealing with tasks other than observing video feeds. Currently, NiceVision solutions record, analyze, and manage video data from over 200,000 cameras deployed around the world, at airports, highways, railways, hotels, cruise lines, public facilities, schools and many other sites.

9. Camero. While security cameras — both stationary and roving — are useful in observing open areas and perimeters, they are far less useful in urban settings. Buildings and other large objects abound, providing terrorists or criminals with the cover they seek to avoid authorities — and stay out of view of cameras. Camero, with R&D facilities in central Israel in Kfar Netter, has developed a unique camera that can "see" through walls, that denies the bad guys the advantages provided by urban environments. The Camero Xaver system uses 3D image reconstruction algorithms in conjunction with sophisticated, patented signal processing techniques and a unique proprietary Ultra-Wideband (UWB) sensor design with extremely high bandwidth and a very high dynamic range. The result is an ability to generate 3D images of objects concealed by solid barriers such as walls, made from a variety of known materials including ement, plaster, bricks, concrete and wood. With the system set to receive FCC (U.S. Federal Communications Commission) certification this year, Camero will be ready to install systems throughout the US in the coming months.

10. Bynet. In an enclosed area, cameras using some of the technologies outlined above can be used to effectively stop and catch suspects. What if the suspect gets into a vehicle? At that point, cameras can no longer track the suspect, and important information that could help defuse the situation is lost. Shamah writes that the problem can be countered with the high-resolution mobile video surveillance system from Bynet, Israel's largest hardware, software, and technology integrator. Along with advances in video surveillance, Bynet partners have developed technology that enables the company to offer a unique solution for border patrols, police and other law enforcement agents. The central feature of the technology is a communication system capable of transmitting live, real-time video, data and voice communications via a single broadband connection, using a fast, secure, private network. The key to the system is the high-speed wireless network, which allows fast transmission of high-resolution video and audio without any effort required on the part of the driver. The vehicle continues on its rounds or pursues a suspect, and the camera focuses, with an individual in the control center able to enhance the picture to see inside a vehicle even hundreds of meters Away. Add to that Bynet's unique video correction system, and security and law enforcement officials won't miss a move suspects make

USS Cole: 10 years on

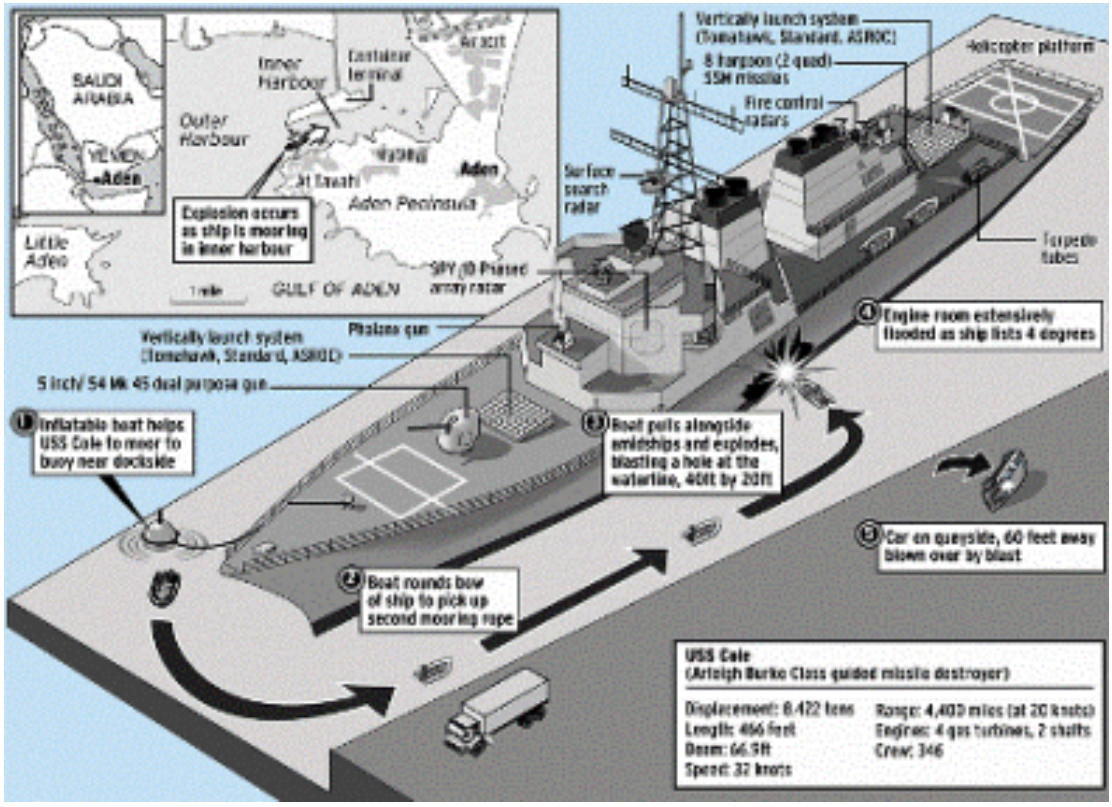
Cole's legacy: a different U.S. Navy

Source: http://homelandsecuritynewswire.com/coles-legacy-different-us-navy

The terrorist bomb attack on the destroyer Cole on 12 October 2000 was a watershed moment in modern Navy history; it was also a wake-up call on the need for better force protection, damage-control training, intelligence sharing, shipboard equipment, and mass-casualty response

Waterline damage to the Cole after the attack of 2000 // Source: whereistheoutrage.net

The terrorist bomb attack on the destroyer Cole on 12 October 2000 was a watershed moment in modern Navy history. It was also a wake-up call on the need for better force protection, damage-control training, intelligence sharing, shipboard equipment, and mass-casualty response. Significant strides forward in these elements have been made in the past ten years, officials say — some of the steps prompted by changes mandated in the Pentagon's 2001 Cole Commission Report, others by debriefs and after-action reports. William H. McMichael writes in *Navy Times* that no area has advanced more than force protection, both in port and in transit. He quotes Capt. Sam McCormick, the anti-terrorism/force protection officer for Fleet Forces Command to say that "There's been a huge amount of change." Doctrine, organization, materiel, logistics, facilities and personnel requirements have been modified and training has been "totally revamped," McCormick said. Afloat training groups train ships' reaction forces in basic and advanced techniques, and train their trainers as well. Ships cannot deploy without passing strike force certification training on anti-terrorism force protection, or ATFP. Ships in



port employ protective zones, security barriers and harbor security patrols. High-value units are escorted in and out of port, often by the Coast Guard, which has law enforcement capability. Gate sentries get specialized training. The master-at-arms force has increased fivefold since 2001. In addition, the rules of engagement around the world have "been thoroughly reviewed and amended as appropriate," McCormick said. The standing rules are defined by the Joint Staff. In high-threat areas such as 5th Fleet, he said, those rules are modified by the combatant commander, who has sole responsibility for setting the threat level in his area. Ship commanders formerly had wide latitude in how they handled ATFP but set their own force protection postures based on the threat level, he said. Cmdr. Amy Derrick-Frost, 5th Fleet spokeswoman, said commanders also coordinate extensively with host nation officials and U.S. Embassy country team officials and consider active intelligence and current threat assessments. "One of the biggest pieces that came out of the attack on the Cole was truly a mindset change in the Navy," McCormick said. "When you have a successful attack in which, tragically, 17 sailors were killed and a billion-dollar warship was significantly damaged, that changes the psyche of the Navy." When ship crews arrive in theater, he said, "They are leaning forward in their boots, they are vigilant to the extreme. Everything is possible. And we have to be prepared. We have to be on task, 24-7-365, when we're in the combat zone." In addition, he said, the defensive concept of anti-terrorism operations applies globally. Guidance is aligned all down the line. Citing security concerns, 5th Fleet reveals little about operational changes in the region, but said the rules for ships pulling into ports have been changed "to mitigate possible attacks." Multiple factors, such as threat assessments and host

nation resources, go into deciding whether to enter a given port, Derrick-Frost said. Asked whether Navy ships still stop in Yemen's Aden Harbor to refuel, Derrick-Frost replied, "U.S. Navy ships have not actively visited the port of Aden since the Cole tragedy." The Pentagon report called for better rapid incident response. All Navy regional operations centers are now connected by a command-and-control network, McCormick said. From his base in Norfolk, Virginia, he said he can dial one number and be simultaneously connected to all six Navy regional operations centers in the United States, both Navy numbered fleets, Navy Installations Command and the Naval Criminal Investigative Service. "So if something happens on the West Coast, and we're alerted, I can immediately tell everyone in the nation," McCormick said. Overseas, combatant commanders' Maritime Operations Centers are similarly linked to the system, he said. He added, that, that "At the end of the day, it's still those sailors on the ship that make the difference. … If they're doing their job to the best of their ability, they're going to beat them." McCormick emphasized the importance of U.S. forces remaining nimble enough to keep ahead of an elusive insurgent enemy. "We've closed all the gaps that enabled Cole to happen, let's say," McCormick said. "But you know, we're up against a highly dynamic, innovative and adaptive enemy, who now has increased what they can do. Have we matched up to that? I'll be very honest with you: We found that we still have some work to do." McMichael writes that the Cole plays a highly visible role in Navy damage-control training, which begins in boot camp with the pre-graduation Battle Stations event. One of the improvements, and seminal events, that takes place aboard the realistic destroyer mock-up housed inside a building at Naval Station Great Lakes, Illinois, is called "The Cole Scenario." The room's mess decks have collapsed onto a berthing area — the opposite of what happened on Cole, but real-enough looking, officials say. There are dummy bodies and body parts scattered about the torn metal, and groups of recruits are sent down with stretchers to look for those who can be "saved," triage them and, if savable, carry them via stretcher back to a battle dressing station. The dummies make noise via built-in MP3 players, and trainers employ other special effects and lighting. "We drive home to the recruits that the things they're learning here at boot camp, they need to take them to heart," said Chief Gas Turbine Systems Technician (Mechanical) (SW/AW) Karl Hacker, Battle Stations operations chief. The scenarios, he said, "all really happened in naval history. Real sailors lost their lives. We want to prepare them … so if this happens to them out in the fleet, it won't be the first time they've seen it." The Cole simulator was launched in 2007, but Battle Stations began 10 years earlier. The former executive officer of the Cole, now-Capt. Chris Peterschmidt, said younger sailors on the Cole performed "phenomenally well" after the attack. When interviewed afterward, the sailors told officials, "We saw this before" — referring to their more-intense basic training. The new training center, Peterschmidt said, is the "crown jewel" of Navy damage control training. "In a way, every sailor coming into the Navy walks a little bit in the shoes of the sailors of the Cole," said Peterschmidt, now the operations officer for 3rd Fleet, who visited the mock-up in May. "Unfortunately, they only go through it once. They never go back to it again, and there's nothing like it, comparably, in any of the fleet concentration areas." That training in damage control and mass-casualty response, as well as in other vital areas, gets reinforced out in the fleet by the afloat training groups — although one retired skipper said the philosophy of training the trainer neglects vital team-building. Retired Cmdr. Bryan McGrath, who commanded the destroyer Bulkeley from 2004 to 2006, maintains that the "dirty little secret" of this approach is that the trainers are a ship's very best watchstanders. "For a good portion of the time … they train your more junior people," McGrath said. "Your absolute varsity, your very best people, almost never get trained operating as a unit, together. Your junior people definitely become better trained. Your No. 1 [group] never drills together, and never gets drilled. Because who do you use to evaluate them? Your second team?" ATG damage control training, he said, "was satisfactory, it was good. They concentrated on the right things, the basics. I never felt like I could have enough of it. But it was probably among some of the better training that I thought ATG gave." Equipment and gear changes, many quite small, were prompted by the Cole attack. Every surface warship and command ship now carries a "Cole Lessons Learned Kit," with items that came as a pleasant surprise to Peterschmidt when, in 2006, he took command of the destroyer Pinckney in San Diego. "I noticed right away— oh, they fixed that!" Peterschmidt said, noting fixes as simple as adding fluorescent markings in the escape trunks to more accurately assess dewatering efforts in a darkened space.

Giant blimps to ferry hospitals, buildings to disaster zones

Source: http://homelandsecuritynewswire.com/giant-blimps-ferry-hospitals-buildings-disaster-zones

Giant airship will be able to lift up to 150 tons -- more than seven times the weight that helicopters are able to carry; the airship, which will be able to move aid -- or even portable hospitals and entire buildings -- to remote areas or disaster zones, harnesses aerostatic lift, meaning it is able to fly using lighter-than-air (LTA) gases that keep it buoyant rather than aerodynamic lift

Photo-rendering of SkyLifter-delivered hospitals on Mt. Everest // Source: skylifter.com.au

Aussie company SkyLifter is developing a giant flying saucer that can transport buildings for long distances anywhere in the world. The airship, dubbed the "SkyLifter," would be able to lift up to 150 tons — more than seven times the weight that helicopters are able to carry. The *Sydney Morning Herald*'s

Glenda Kwek writes that the designers of SkyLifter, English-Australian Jeremy Fitton and Englishman Charles Luffman, hope to power it using bio-diesel fuel and solar panels. "There is a massive need for this," SkyLifter's investor relations partner Sam Mokhtari told Kwek in a phone call from London.

Potential uses for a successful commercial model of the SkyLifter include moving aid or even portable hospitals to remote areas — such as rural regions or disaster zones — which have limited or no available infrastructure such as roads, Mokhtari said. The company hopes it will one day also become part of the tourism market, where travelers can fly slowly above landscapes from one destination to another, as they currently do on cruise ships. "One hundred years ago, airships were the rage. [This technology] needs to be brought up to date. People want a greener product and … we are looking at alternative forms of transport." Mokhtari said the company had so far built Betty, a three-meter mini-SkyLifter, and Vikk,i, an 18-meter-wide tethered version of the airship, and plans to construct an unmanned aerial vehicle (UAV) prototype in the next two to three years. Lucy, the 150-meter prototype, is expected to be completed in about six to seven years, he said. Kwek writes that the airship, which will be made using "strong laminated fabric," harnesses aerostatic lift — meaning it is able to fly using lighter-than-air (LTA) gases that keep it buoyant — rather than aerodynamic lift. Unlike heavier-than-air (HTA) fixed or rotary-wing aircraft such as aircraft and helicopters that use aerodynamics to fly, the SkyLifter would be able to move using propellers attached to a small control pod suspended from a rod below the main saucer-like blimp. Its top speed is expected to be about 45 knots for a maximum travel distance of about 2,000 kilometers. Mokhtari would not speculate on the cost of building such airships, but added that, while it has been a "slow process of building the case" of the SkyLifter, the company had "made miracles happen in a year" and had many interested parties keen to invest in the technology. Aerostat technology featured in the headlines last week after a $8.9 million helium balloon was used during the opening ceremony of the Commonwealth Games in Delhi, India.

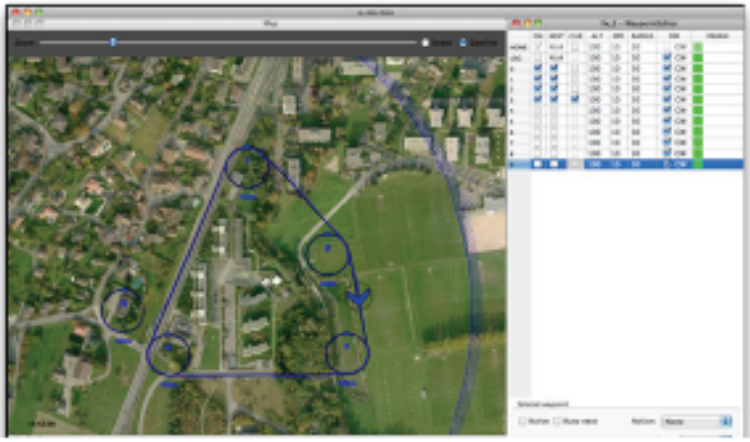
Kwek notes, though, that commercial uses for aerostat craft have not always taken off. In the mid-1990s, a German company tried to build a heavy-lift airship called the Cargolifter, but fell into insolvency in 2002, leaving behind millions of dollars of debt and a massive hanger in Brandenburg that was converted into an artificial indoor tropical resort. The first rigid airship that became commercially successful was the Zeppelin, built by Count Zeppelin in the early twentieth century and used by the Germans for military missions during the First World War. Passenger-carrying airships using both helium and hydrogen were developed in the following years, although the explosion of the hydrogen-filled Hindenburg airship in the United States in 1937 eventually ended such modes of travel. Today, airships are more likely to be used as an alternative form of aerial advertising. Kwek writes that the U.S. government is also reviving its interest in airships as surveillance tools, with the department of defense reportedly investing about $1.7 billion into researching and developing unmanned aerial vehicles last year.

You don't need to be a pilot to fly the *swinglet* CAM.

With the easy of a bird the swinglet CAM takes off in the sky. Thanks to its integrated autopilot: it starts, flies and silently land by itself.
With the help of the software "e-mo-tion" you can define a whole flight path for the swinglet CAM and direct it where to make the pictures. Once the swinglet CAM landed you can download those pictures from the photo camera.

Feature	Advantage
Very light	Inherently harmless
Electrically powered	Low noise level
Miniature autopilot	Flies autonomously
Intuitive control and monitoring software	Very easy to use
High autonomy	Covers big areas or long distances

If you have basic computer skills, then you will be easily able to operate the flight programming software "e-mo-tion." With simple drag & drop functions it is possible to pre-program, and update during flight, the position, altitude and behavior of the swinglet.



If you want a turn-key solution opt for the swinglet CAM Pro. It comprises an additional ground station. The swinglet CAM Pro is immediate ready to be operated.

Size	80 cm of wingspan
Weight (typ.)	500 g
Battery	Lithium-Polymer
Endurance (typ.)	30 minutes
Range	Up to 20 km
Propulsion	Electric brushless motor
Flight speed	30-50 km/h
Communication link	For remote control: 35 MHz
Navigation	Up to 20 waypoints
Control and monitoring software	Drag and Drop flight planning, mission reprogramming during flight
Digital Camera	12 MP, electronically integrated
Ground station	Notebook; preconfigured hard- and software

Do you want to take off and fly?
Order you swinglet CAM or CAM Pro: info@senseFly.com

senseFly – chemin de la Raye 13 – 1024 Ecublens – Switzerland – www.sensefly.com

S. American states among money launderers

Source: http://www.upi.com/Business_News/Security-Industry/2010/10/21/S-American-states-among-money-launderers/UPI-58131287661733/

Costa Rica, Cuba, Honduras and Nicaragua are among nations that pose rising risks in the global fight against money laundering and related security threats, a new survey indicated. The latest version of Anti-Money Laundering Atlas produced by Promontory Compliance Solutions rated countries of the world according to perceived risk of money laundering and terrorist financing. The latest AML Atlas released by the company incorporates Transparency International's Corruption Perception Index but also includes feedback and data from a network that shared its on-the-ground experience with high-risk countries. Transparency International Corruption Perception Index ranks 150 countries in terms of perceived levels of corruption, as determined by expert assessments and opinion surveys. Included in the assessment is the recently released Presidential Determination on Major Illicit Drug Transit or Major Illicit Drug Producing Countries for Fiscal Year 2011, changes to World Bank Governance Indicators, new information from the Financial Action Task Force and updates to several other anti-money laundering related indicators. Promontory said its anti-money laundering atlas continues to rate Iran, Myanmar and Cuba as among the riskiest countries, considering the U.S. and multinational sanctions against them. It identified several other countries, including the Cook Islands, Costa Rica, Eritrea, Honduras and Nicaragua as presenting rising risks. "Fighting money laundering, terrorist financing and financial fraud remains a high priority for governments around the world, and AML Atlas is a proven tool for helping financial companies comply with complex rules," said Eugene A. Ludwig, chief executive officer of Promontory Compliance Solutions. In September the U.S. Financial Crimes Enforcement Network issued an Advance Notice of Proposed Rulemaking that could result in a dramatic expansion in reporting requirements for cross-border transactions. The atlas was launched in 2005 as a geographic risk assessment tool rating countries according to their perceived risk of money laundering and terrorist financing. Promontory Compliance Solutions is an affiliate of Promontory Financial Group, a global financial services consulting firm. Increased risks of linkage between money laundering and terrorism have widened a term originally applied to financial transactions related to organized crime. The U.S. Office of the Comptroller of the Currency includes in money laundering any financial transaction that generates an asset or a value as the result of an illegal act, including tax evasion and false accounting. Money laundering activities in Latin America have been linked to an extensive narcotic trade involving Colombia, Mexico and Venezuela. Recent police reports also cited money laundering connections between Central and South America and the Middle East and Africa.

View the interactive world atlas at: http://www.promontorycs.com/atlas.shtml

Al Qaeda Leader Dined at the Pentagon Just Months After 9/11

Source: http://www.foxnews.com/us/2010/10/20/al-qaeda-terror-leader-dined-pentagon-months/

Anwar Al-Awlaki may be the first American on the CIA's kill or capture list, but he was also a lunch guest of military brass at the Pentagon within months of the Sept. 11, 2001, terror attacks, Fox News has learned. Documents exclusively obtained by Fox News, including an FBI interview conducted after the Fort Hood shooting in November 2009, state that Awlaki was taken to the Pentagon as part of the military's outreach to the Muslim community in the immediate aftermath of the attacks. The incident was flagged by a current Defense Department employee who came forward and told investigators she helped arrange the meeting after she saw Awlaki speak in Alexandria, Va. The employee "attended this talk and while she arrived late she recalls being impressed by this imam. He condemned Al Qaeda and the terrorist attacks. During his talk he was 'harassed' by members of the audience and suffered it well," reads one document. According to the documents, obtained as part of an ongoing investigation by the specials unit "Fox News Reporting," there was a push within the Defense Department to reach out to

the Muslim community. Terrorist dined with military brass? "At that period in time, the secretary of the Army (redacted) was eager to have a presentation from a moderate Muslim." In addition, Awlaki "was considered to be an 'up and coming' member of the Islamic community. After her vetting, Aulaqi (Awlaki) was invited to and attended a luncheon at the Pentagon in the secretary of the Army's Office of Government Counsel." Awlaki, a Yemeni-American who was born in Las Cruces, N.M., was interviewed at least four times by the FBI in the first week after the attacks because of his ties to the three hijackers Nawaf al-Hazmi, Khalid al-Mihdhar and Hani Hanjour. The three hijackers were all onboard Flight 77 that slammed into the Pentagon. Awlaki is now believed to be hiding in Yemen after he was linked to the alleged Ft. Hood shooter Major Nidal Malik Hasan, who e-mailed Awlaki prior to the attack. Sources told Fox News that Awlaki, who is a former Muslim chaplain at George Washington University, met with the Christmas Day bomber Umar Farouk Abdulmutallab in Yemen and was the middle-man between the young Nigerian and the bombmaker. Awlaki was also said to inspire would-be Times Square bomber Faisal Shahzad. Apparently, none of the FBI's information about Awlaki was shared with the Pentagon. Former Army Secretary Tommy White, who led the Army in 2001, said he doesn't have any recollection of the luncheon or any contact with Awlaki. "If this was a luncheon at the Office of Government Counsel, I would not necessarily be there," he said. The Pentagon has offered no explanation of how a man, now on the CIA kills or capture list, ended up at a special lunch for Muslim outreach. After repeated requests for comment on the vetting process beginning on October 13th, an Army spokesman insisted Wednesday that the lunch was not an Army event. "The Army has found no evidence that the Army either sponsored or participated in the event described in this report," spokesman Thomas Collins said. Collins also noted that the FBI document referred to the “Office of Government Counsel” but should read “Office of General Counsel.” Collins said he believed the event was sponsored by the office of the Secretary of Defense. A spokeswoman there said she would look into it and get back to Fox News. A former high-ranking FBI agent told Fox News that at the time Awlaki went to lunch at the Pentagon, there was tremendous "arrogance" about the vetting process at the Pentagon. "They vetted people politically and showed indifference toward security and intelligence advice of others," the former agent said.

Tunnels, boats used to defeat stronger border security

Source: http://homelandsecuritynewswire.com/tunnels-boats-used-defeat-stronger-border-security

As border fences along the U.S.-Mexico border get stronger, smugglers are attempting to dodge increased security by tunneling and sailing their way into the United States; tunneling activity has increased 65 percent in the past two years, and a multi-agency team has already made 786 sea smuggling arrests, up from just 400 last year.

Drug smuggling tunnel discovered in Nogales, Arizona // Source: news.sky.com

As violence along the United States-Mexico border continues to escalate, the U.S. government is beefing up border security. On Monday, DHS secretary Janet Napolitano touted the success of

those efforts. In fiscal years 2009 and 2010, criminal arrests along the border — three-quarters of which were for drug or human smuggling — were up 12 percent compared to the two previous years. Meanwhile, apprehensions for illegal border crossings are falling, suggesting fewer people are attempting to enter the U.S. illegally ("Illegal immigration into U.S. continues to decline. Brandon Scott reports for CBS News that border authorities are facing a troubling — and growing — problem. As border fences get stronger, smugglers are attempting to dodge increased security by tunneling and sailing their way into the United States. Since 2001, 111 tunnels have been discovered along the southern border, with tunneling activity increasing 65 percent in the past two years. One tunnel, discovered thirty feet below the surface in Tijuana, is an elaborate passageway complete with electricity and ventilation, upwards of six feet tall, and wide enough for two people to walk side-by-side. Uncovering the tunnels is a challenge, according to Tim Durst of U.S. Customs and Border Protection (CBP). Durst said the effort to find and shut down border tunnels is "baby steps at this point." "It's basically the cartel and smuggling organizations' mechanism to go around the increased presence along the port of entries," Durst said. Durst heads a Tunnel Task Force, and he and his team have been busy trying to find tunnels before smugglers can reach the United States. Scott writes that if it is tough to find smugglers underground, it can be an even bigger challenge on the open water, along the U.S.-Mexico coastline, where there are no border checkpoints, no border crossings. Coast Guard Lt. Jamin Stortz, who patrols the Pacific coast, said, "Smugglers are exploiting the coastline," often hiding in plain sight on sailboats and luxury yachts. This year a multi-agency team has already made 786 smuggling arrests, up from just 400 last year. "A new wave of challenges — that fences can't contain," Scott notes.

U.K. revives sweeping digital surveillance scheme

Source: http://homelandsecuritynewswire.com/uk-revives-sweeping-digital-surveillance-scheme

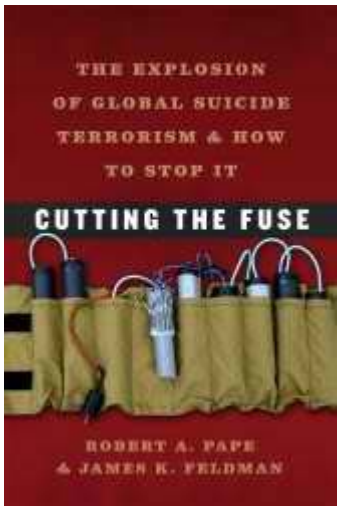
The U.K. government has revived a sweeping surveillance scheme killed by its Labor predecessor last December; the scheme will require that every e-mail, phone call, and Web site visit be recorded and stored, allowing the security and police authorities to track every phone call, e-mail, text message, and Web site visit made by the public if they argue it is needed to tackle crime or terrorism; the information will include who is contacting whom, when, and where -- and which Web sites are visited, but not the content of the conversations or messages. The U.K. government has revived a digital surveillance which will require that every e-mail, phone call, and Web site visit be recorded and stored. The scheme will allow security services and the police to spy on the activities of every Briton who uses a phone or the Internet. Moves to make every communications provider store details for at least a year will be unveiled later this year sparking fresh fears over a return of the surveillance state. The plans were shelved by the Labor government last December, but the Home Office is now ready to revive them. The *Telegraph*'s Tom Whitehead writes that it comes despite the Coalition Agreement which promised to "end the storage of Internet and e-mail records without good reason." Any suggestion of a central "super database" has been ruled out but the plans are expected to involve service providers storing all users details for a set period of time. This will allow the security and police authorities to track every phone call, e-mail, text message, and Web site visit made by the public if they argue it is needed to tackle crime or terrorism. The information will include who is contacting whom, when, and where — and which Web sites are visited, but not the content of the conversations or messages. The move was buried in the government's Strategic Defense and Security Review, which revealed: "We will introduce a program to preserve the ability of the security, intelligence

and law enforcement agencies to obtain communication data and to intercept communications within the appropriate legal framework". This program is required to keep up with changing technology and to maintain capabilities that are vital to the work these agencies do to protect the public. Communications data provides evidence in court to secure convictions of those engaged in activities that cause serious harm. It has played a role in every major Security Service counterterrorism operation and in 95 per cent of all serious organized crime investigations. We will legislate to put in place the necessary regulations and safeguards to ensure that our response to this technology challenge is compatible with the Government's approach to information storage and civil liberties. Isabella Sankey, director of policy at Liberty, said: "One of the early and welcome promises of the new Government was to 'end the blanket storage of internet and email records.' Any move to amass more of our sensitive data and increase powers for processing would amount to a significant U-turn. The terrifying ambitions of a group of senior Whitehall technocrats must not trump the personal privacy of law abiding Britons." Guy Herbert, general secretary of the No2ID campaign group, said: "We should not be surprised that the interests of bureaucratic empires outrank liberty. It is disappointing that the new ministers seem to be continuing their predecessors' tradition of credulousness."

New Book: How To End Suicide Bombings

Source: http://www.medicalnewstoday.com/articles/203715.php

To put an end to suicide bombings, the United States needs a new strategy that would reposition troops and work with local allies to boost their fighting capacity, contends Robert Pape, a political scientist at the University of Chicago and one of the nation's leading experts on suicide terrorism.



Despite a popular belief that suicide terrorism is the result of religious fanaticism, such bombings are really a calculated response to occupations by outsiders, according to research in a new book, Cutting the Fuse: The Explosion of Global Suicide Terrorism and How to Stop It. The book examines exhaustive data on suicide attacks since 1980 in the Middle East, Chechnya, Sri Lanka and around the world. The data show that the best way to reduce suicide bombings in Afghanistan or Iraq is not to condemn Islamic extremism, but to end foreign occupations as quickly as possible, Pape claims. Pape's co-author is James Feldman, a former professor of decision analysis and economics at the Air Force Institute of Technology and the School of Advanced Airpower Studies. The book is published by the University of Chicago Press. Their work shows that the suicide terrorism threat to America is growing, despite military efforts in Iraq and Afghanistan as well as Pakistan's attempts to fight its own militants. "Each month there are more suicide terrorists trying to kill Americans and their military allies in Afghanistan, Iraq and other Muslim countries than in all the years before 2001 combined," Pape said. In addition to nations where the United States is involved in military conflicts, the United States also has stationed troops on the Arabian Peninsula, a situation that al Qaeda claims is the reason for its hostility to the U.S. The central problem is that leaders in the United States have constructed a narrative that identified the threat as coming from Islamic extremists who hate the United States. That explanation led to the invasions, occupations and eventual efforts to establish democratic regimes, something that requires a heavy military presence, the authors explained. "But we now have strong evidence that the narrative - that suicide terrorism is prompted by Islamic fundamentalism - is not true," Pape said. Despite some military success, suicide terrorism has continued, Pape said. The book's extensive research points out that after the United States occupied Afghanistan and Iraq, suicide attacks worldwide rose dramatically - from 300 between 1980 and 2003 to 1,800 from 2004 to 2009. More than 90 percent of the attacks were anti-American. Indirect occupations, in which the United States helps lead an occupation without committing troops, such as in Pakistan, have the same impact as direct occupations and explain the rise of suicide terrorism there, Pape said. The research also showed that civilian casualties during occupations increase suicide terrorism by giving terrorist leaders rallying points to turn local residents against the invading force. Pape oversees the Chicago Project on

Security and Terrorism, the world's largest academic research project on suicide terrorism, and Feldman is the project's principal advisor. The CPOST team recently completed a study of more than 2,000 suicide attacks. The team also studied tapes left by suicide bombers and collected other key information, such as their religious backgrounds, methods and number of casualties resulting from the attacks. The research found that in each of the countries where suicide terrorism flourished, it was used to combat an occupying force. While occupation may sometimes be necessary to achieve immediate foreign policy goals, it does so at the risk of stimulating a suicide terrorist campaign against the occupier's homeland. This is the dilemma an occupier faces, Feldman noted, since when the threat of occupation was removed, suicide terrorism largely stopped. After Israel withdrew from southern Lebanon in 2000, for instance, Lebanese suicide terrorist attacks against Israel ended, Pape pointed out. Since Israel withdrew militarily from Gaza and portions of the West Bank, suicide attacks have been down 90 percent. In order to end suicide terrorism, or to "cut the fuse," the United States needs to "reduce the reliance on foreign occupation as a principal strategy for ensuring national interests," they concluded. "I'm not saying that we should cut and run, but rather that we have to use our military power differently," Pape said. Offshore and in-country balancing would contain the threat to American rather than fuel it, he said. Offshore balancing would involve stationing American forces on ships in the Persian Gulf and and islands in the Indian Ocean, and establishing military bases with non-Western forces on the Arabian Peninsula to support rapid deployment of ground forces, if needed in a future crisis. In-country balancing involves working more closely with local forces, such was the case in Anbar Province in Iraq, where Americans empowered local Sunni leaders to be responsible for their own defense and accordingly curtailed insurgency. "Intelligent debate and decision making require putting all the facts before us. For over a decade our enemies have been dying to win. By ending the perception that the United States and its allies are occupiers, we can cut the fuse to the suicide terrorism threat," Pape said.

Profile: Al-Qaeda in North Africa

Source: http://news.bbc.co.uk/2/hi/africa/6545855.stm

Al-Qaeda in the Land of the Islamic Maghreb, to give its full name in English, has its roots in the bitter Algerian civil war of the early 1990s, but has since evolved to take on a more modern Islamist agenda.

Reported leader Abdel Moussab Abdelwadoud is rarely seen

It emerged in early 2007, after a feared militant group, the Salafist Group for Preaching and Combat (GSPC), aligned itself with Osama Bin Laden's international network. Back in the 1990s, against a background of Islamist political groups testing their strength across North Africa, the military-backed authorities in Algeria at first permitted the Islamists to play a full part in the nation's political life. But then, when the Islamic Salvation Front was poised to sweep the board in a 1992 general election, they annulled the whole process and took power back. The political ferment immediately moved into violence. Armed Islamists mounted attacks across Algeria; the security forces fought back; and sometimes it was hard to tell which group had carried out which atrocity.

Other states in the region - Tunisia and Morocco, Mauritania to the west and Libya to the east - also battled against Islamists.

Most feared

But the conflict in Algeria was particularly brutal, killing perhaps 150,000 people. It peaked in the 1990s, until an amnesty offer to Islamists in 1999 led to gradual improvements. Violence fell and the country's economy recovered during the early years of the 21st Century.


GSPC deputy leader Amari Saifi is serving a life sentence

However, the most feared of the militant organisations, the Armed Islamic Group or GIA, rejected the promised amnesty and continued a violent campaign to establish an Islamic state. By then it had split, with the most extreme faction calling itself the Salafist Group for Preaching and Combat (GSPC) - a name which echoed an Islamist group in Morocco. The Arabic word "Salafist" means fundamentalist, in the sense of going back to the original texts of Islam. In September 2006 the GSPC said it had joined forces with al-Qaeda, and in January 2007 it announced that it had changed its name to reflect its new allegiance. There has been much debate in intelligence circles about the significance of the move. Some officials have dismissed it as an act of desperation by a group on its last legs, seeking to attract new recruits by aligning itself with Osama bin Laden. Others consider it a far more worrying development, showing that al-Qaeda has succeeded in persuading North Africa's Islamic extremists to take a more global view. The news delighted al-Qaeda deputy leader Ayman al-Zawahiri, who described it at the time as "a source of chagrin, frustration and sadness" for Algeria's authorities.

Wave of attacks

Shortly afterwards, seven bombs exploded in the eastern Kabylia region, killing six people, and in April 2007 at least 30 people were killed in bomb attacks on official buildings in Algiers. Al-Qaeda's North African wing said it had planted the bombs.


Attacks in August 2008 in Bouira hit a barracks and a company bus

More attacks followed: on buses carrying foreign oil workers; on American diplomats; on soldiers; and in September 2007, a suicide bomb attack in Batna, aimed at the motorcade of President Abdelaziz Bouteflika. The president was not injured, but 20 people were killed. Two days later, a car bomb killed more than 30 people at a coastguard barracks in the town of Dellys. In December, twin car bombs claimed by al-Qaeda in North Africa killed at least 37 people in Algiers, including 17 UN staff. The death toll continued to mount in 2008. Back-to-back attacks on 19 and 20 August killed dozens of people. The first was a suicide car bombing at a police college in Issers, east of Algiers, killing 48 people. A day later, two more car bombings struck in quick succession in Bouira, south-east of Algiers. The second explosion in Bouira killed 12 Algerian employees of the Canadian engineering firm SNC-Lavalin. The attacks continued into 2009, when suspected al-Qaeda militants in February killed nine security guards who were working for the state-owned gas and electricity distributor Sonelgaz at a camp near Jijel, east of Algiers. Today, Algerian Islamists represent the largest national grouping in al-Qaeda, according to Jim Carroll, author of How Did Al-Qaeda Emerge in North Africa?

'Years of hardship'

Algeria's prime minister has warned that the bombers want to take Algeria back to "the years of hardship". But other incidents across the Maghreb point to the group's possible regional ambitions.

> "This group trained in Algeria and have learned their techniques from Iraq as well as in Afghanistan"
>
> Maghreb Analyst: Mohamed Ben-Madani

In January 2007, 12 people were shot dead by the security forces in Tunisia near the small town of Solimane, south of the capital, Tunis. The authorities initially described their adversaries as criminals but later admitted that the men were Islamic militants with connections to the GSPC. Meanwhile, in Morocco, security forces have clamped down on several militant cells - arresting, trying and jailing their leaders - after four incidents blamed on al-Qaeda-inspired groups in 2007. The security forces are said to be on the lookout for militants who are believed to be crossing into Morocco from Algeria. And of course the Madrid train bombs, which killed almost 200 people in 2004, were the work of a Moroccan gang. In December 2008, militants from al-Qaeda in North Africa abducted the United Nations special envoy, Robert Fowler, and his assistant, Louis Guay, near Niger's capital, Niamey. They were released in April 2009. The group also seized four European tourists who disappeared in January 2009 along the Mali-Niger border. Two were freed in April. The group threatened to kill one of the remaining pair - a Briton - unless a radical Islamic cleric convicted of terrorism in Jordan, Abu Qatada, was released from jail in the UK. And in June the British government said it believed the group's claims on an Islamist website that the death threat had been carried out against the British captive, Edwin Dyer.

'One-eyed'

The group is thought to have between 600 and 800 fighters spread throughout Algeria and Europe. Its leader is thought to be Abou Mossab Abdelwadoud, a former university science student and infamous bomb-maker. He took over in 2004, though there are unconfirmed reports that he has since been toppled by internal rivals. Another leading member is Mokhtar Belmokhtar, 36, known as the "one-eyed", a former soldier who followed the familiar route for radical young Muslims and went to fight in Afghanistan. He leads the Saharan faction of the group and has organised the importation of arms for the underground network from Niger and Mali. He is wanted in Algeria on terrorism charges. Two years ago, deputy GSPC leader Amari Saifi was sentenced to life in prison for kidnapping 32 European tourists in 2003. The former paratrooper was captured by Chadian rebels in mysterious circumstances and passed on to Libya before standing trial in Algeria.

Mokhtar Belmokhtar is known as the "one-eyed"

Islamic Extremist Targets Facebook Users

by Daniel Huff

Source: http://www.meforum.org/2772/islamic-extremist-facebook

Court documents filed last week reveal Islamic extremists have obtained personal contact information on members of the defiant Facebook group "Everybody Draw Mohammed Day." Zachary Chesser, who provided the information, pled guilty to "communicating threats" and renounced jihad, but the damage was done. Prosecutors say he "seriously endangered the lives of innocent people who will remain at risk for many years to come." This lasting effect makes it all the more frustrating that authorities did not charge him sooner. He had made very similar threats against the producers of *South Park* weeks before. The case highlights the urgent need for better legal tools to protect free speech from extremist intimidation. On April 15, Chesser, acting through the website RevolutionMuslim.com, "warned" the creators of South Park that they would "likely" be executed for producing an episode lampooning Muslim outrage over depictions of Mohammed. Chesser's post provided their photos and work address

and included audio of radical cleric Anwar Al-Awlaki calling for the assassination of anyone who has "defamed" Mohammed. As was widely reported, Comedy Central, which carries the show, succumbed to the threat and heavily censored the episode. Nevertheless, Chesser was not charged. NYPD Commissioner Kelly called Chesser's posting a threat but said authorities did not believe legally it "rises to a crime right now." Facing no legal consequences after his first success, Chesser turned the same intimidation tactics on a fresh target. Facebook users, determined to defy the intimidation tactics that vanquished Comedy Central, had started the group "Everybody Draw Mohammed Day." The theory was safety in numbers. If thousands of people all committed to draw Mohammed on a single day, there would be so many potential targets fanatics would be unable to focus their retribution efforts effectively on any single one. It failed because even though thousands of people joined the group, Chesser was content to start small. In May of 2010, he obtained personal contact information on 11 members of the group and posted it to a jihadi website saying the data was "just a place to start." As before, he provided the addresses of his targets against the backdrop of Al-Awlaki's recorded sermon and examples of artists targeted for insulting Mohammed. He even proffered his own reflections on the propriety of executing them in accordance with Islamic law. Yet again, he was not immediately prosecuted. Instead, he was finally arrested July 11th on independent charges of providing material support to a foreign terrorist organization. He was intercepted at Kennedy airport, with his infant son in tow, on his way to Somalia to join al-Shabaab and "engage in violent jihad." It was only in light of this subsequent arrest that federal prosecutors felt comfortable characterizing Chesser's earlier activities as meeting the threshold for true threats in violation of federal law. On October 18th, they amended the charges against him to include the threats relating to *South Park* and Facebook. He pled guilty on all counts. It seems prosecutors did not act earlier, because without Chesser's subsequent behavior, they did not have sufficient evidence of intent to threaten to meet the heightened burden of proof required in criminal cases. In the meantime, Chesser did deep damage to free speech rights. US Attorney Neil MacBride warns Chesser's "solicitation of extremists to murder U.S. citizens … caused people throughout the country to fear speaking out – even in jest – lest they also be labeled as enemies who deserved to be killed." This might have been avoided if Federal law provided the same protection to free speech rights that it already gives to abortion rights. In the 1990's, abortion providers faced the same sorts of extremist threats that cartoonists and authors face now. In response, Congress passed the Freedom of Access to Clinic Entrances Act (FACE) which not only prohibits threats against persons exercising abortion rights, but permits victims to sue for damages. The provision for civil suits with preset damages is key. It empowers victims of intimidation to act as private attorneys general to defend their rights in a setting with a lower burden of proof. Indeed, in a 2002 case with facts similar to the Chesser case, the Ninth Circuit found a fringe pro-life group had threatened abortion doctors by distributing their photos and contact information. The doctors had sued under the FACE Act and obtained a substantial jury award. With only minor modifications, FACE can be expanded to cover threats against free speech. The original passed by solid bipartisan margins in both houses. All 10 federal circuit courts who have heard challenges to FACE have upheld it. To forestall any concerns regarding federalism or unintended consequences, Congress can include a sunset provision. Had such a law been in place in April, Chesser's first victims could have immediately mired him in costly, time consuming civil litigation. The net effect would have been both to distract and deter him from making further threats and preparing for jihad. At least 11 Facebook users would "like" this.

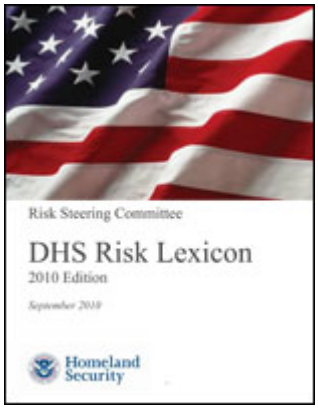
Daniel Huff is Director of the Legal Project at the Middle East Forum and a former counsel to the Senate Judiciary Committee.

DHS Risk Lexicon

Source: http://www.dhs.gov/files/publications/gc_1232717001850.shtm

Developed by the DHS Risk Steering Committee (RSC), the purpose of the DHS Risk Lexicon is to establish and make available a comprehensive list of terms and meanings relevant to the practice of homeland security risk management and analysis. Accomplishing this goal improves the capability of

the Department to assess and manage homeland security risk. To support integrated risk management for the Department, the DHS Risk Lexicon:



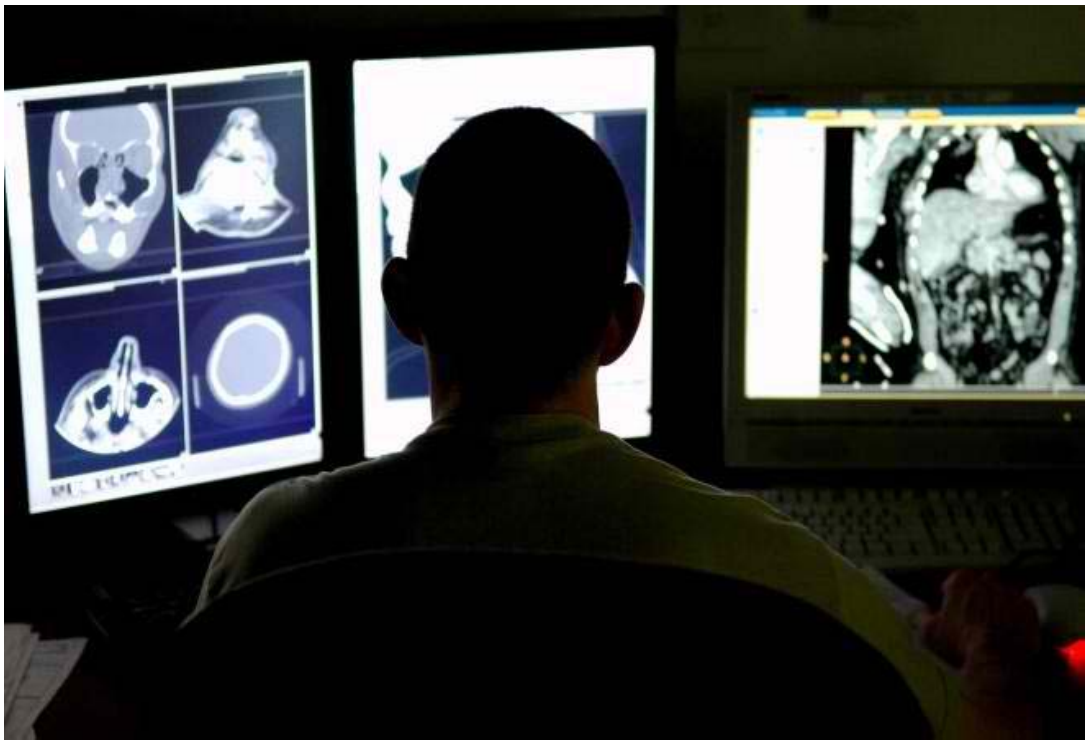
- Promulgates a common language to ease and improve communications for the Department and its partners;
- Facilitates the clear exchange of structured and unstructured data, essential to interoperability amongst risk practitioners; and
- Garners credibility and grows relationships by providing consistency and clear understanding with regard to the usage of terms by the risk community across the Department.

Developing terms, definitions, extended definitions, annotations, and examples is accomplished through a RSC working group known as the Risk Lexicon Working Group, which is open to all Department of Homeland Security Components. Definitions are validated against glossaries used by other countries and professional associations. All terms in the DHS Risk Lexicon were developed through the collective work of the Department's risk community of interest. The DHS Risk Lexicon terms and definitions will be included as part of the DHS Lexicon and future editions will be coordinated by the RSC in collaboration with the DHS Lexicon Program. This is the second edition of the DHS Risk Lexicon and includes fifty new terms and definitions and updated definitions for twenty-three original terms from the 2008 edition.

Air Force Wants Neuroweapons to Overwhelm Enemy Minds

Source: http://www.wired.com/dangerroom/author/noah_shachtman/

It sounds like something a wild-eyed basement-dweller would come up with, after he complained about the fit of his tinfoil hat. But military bureaucrats really are asking scientists to help them "degrade enemy performance" by attacking the brain's "chemical pathway[s]." Let the conspiracy theories begin. Late last



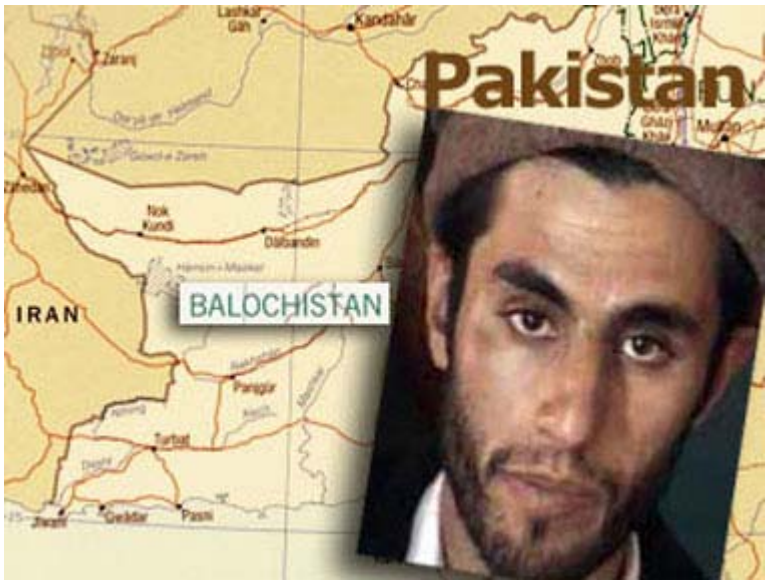
month, the Air Force Research Laboratory's 711th Human Performance Wing revamped a call for

research proposals examining "Advances in Bioscience for Airmen Performance." It's a six-year, $49 million effort to deploy extreme neuroscience and biotechnology in the service of warfare. One suggested research thrust is to use "external stimulant technology to enable the airman to maintain focus on aerospace tasks and to receive and process greater amounts of operationally relevant information." (Something other than modafinil, I guess.) Another asks scientists to look into "fus[ing] multiple human sensing modalities" to develop the "capability for Special Operations Forces to rapidly identify human-borne threats." No, this is not a page from *The Men Who Stare at Goats*. But perhaps the oddest, and most disturbing, of the program's many suggested directions is the one that notes: "Conversely, the chemical pathway area could include methods to degrade enemy performance and artificially overwhelm enemy cognitive capabilities." That's right: the Air Force wants a way to fry foes' minds — or at least make 'em a little dumber. It's the kind of official statement that's seized on by anyone who is sure that the CIA planted a microchip in his head, or thinks that the Air Force is controlling minds with an antenna array in Alaska. The same could be said about the 711th's call to "develo[p] technologies to anticipate, find, fix, track, identify, characterize human intent and physiological status anywhere and at anytime." The ideas may sound wild. They *are* wild. But the notions aren't completely out of the military-industrial mainstream. For years, armed forces and intelligence community researchers have toyed with ways of manipulating minds. During the Cold War, the CIA and the military allegedly plied the unwitting with dozens of psychoactive drugs, in a series of zany (and sometimes dangerous) mind-control experiments. More recently, the Pentagon's most revered scientific advisory board warned in 2008 that adversaries could develop enhancements to their "cognitive capabilities … and thus create a threat to national security." The National Research Council and Defense Intelligence Agency followed suit, pushing for pharma-based tactics to weaken enemy forces. In recent months, the Pentagon has funded projects to optimize troop's minds, prevent injuries, preemptively assess vulnerability to traumatic stress, and even conduct "remote control of brain activity using ultrasound." The Air Force is warning potential researchers that this project "may require top secret clearance." They'll also need a high tolerance for seemingly loony theories — sparked by the military itself.

New terrorism organization in US international terrorist list

Source: www.stratfor.com

The United States placed Jundallah, a Sunni-Balochi Islamist group active in Iran, on its list of international terrorist entities Nov. 3. In its statement, the U.S. State Department said Jundallah was engaged in a variety of terrorist activities confirmed by the group's leadership. In recent years, Jundallah has emerged as the most lethal rebel group fighting Iran via its use of suicide attacks targeting Shiite mosques and even the leadership of the country's elite military force, the Islamic Revolutionary Guard Corps. Washington's apparently sudden move to declare Jundallah a terrorist organization, which Tehran previously has accused Washington and its European and Arab allies of backing, represents a huge gesture toward Iran. Washington likely made the move in hopes of reaching an understanding on the balance of power in the Persian Gulf region after U.S. forces exit Iraq. The step follows a number of recent events. These included a preliminary understanding between Iran and the

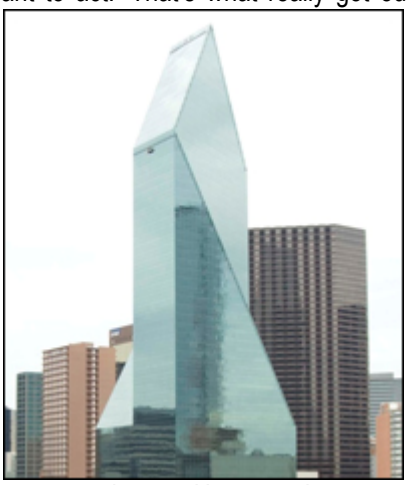


United States regarding a new power-sharing formula in Iraq in the form of a government led by incumbent Prime Minister Nouri al-Maliki, Washington seeking Iranian input in the process toward a settlement in Iraq, Iranian cooperation in Afghanistan, and Iran not creating instability in Lebanon. Declaring Jundallah a terrorist organization is also part of the Obama administration's efforts to reach an overall bilateral understanding with Tehran. This has become especially urgent given the new Republican control of the U.S. House of Representatives, which will force Obama to show progress on the foreign policy front if he wants to be re-elected. All eyes will now be on Iran for its reaction and/or a reciprocal gesture, particularly on the nuclear issue -- for which talks are scheduled for this month -- and on the Sunni share of power in the Iraqi government.

Terror Plot Foiled - Inside the Smadi Case

Source: http://www.fbi.gov/news/stories/2010/november/terror-plot-foiled/terror-plot-foiled

Hosam Smadi will be spending the next 24 years in prison for trying to blow up a Dallas skyscraper in 2009. His recent sentencing brings to a close a successful FBI operation—one that potentially saved many lives—and it also illustrates the threat posed by lone offenders. Smadi, at the time a 19-year-old Jordanian citizen living in Texas, came to our attention in January 2009 through his pro-violence writing on a radical Islamic website. "He was on a very extreme website, where people were saying a lot of unspeakable things, endorsing and celebrating acts of violence against U.S. citizens and our allies," said Special Agent Tom Petrowski, who oversaw the investigation out of our Dallas office. "What made Smadi's postings stand out from the other rhetoric was that he was saying, 'I want to act.' That's what really got our attention," Petrowski added. "Smadi wanted to imitate 9/11 and bring down a skyscraper and kill thousands of people. And he was already in the country. He said he just needed the tools—essentially he was online asking for someone to help him build a bomb." Although he espoused loyalty to Osama bin Laden and al Qaeda, Smadi was not affiliated with any group or other would-be terrorists. With the help of the Internet, he had become radicalized on his own. Smadi entered the U.S. legally but overstayed his visa. "Based on that expired visa, law enforcement could have immediately arrested and deported him," Petrowski said, "and that would have been the easiest thing to do." But it would not have been the right thing to do—because after conferring with the experts in our Behavioral Analysis Unit, it became clear that Smadi was not making empty threats. He wanted to mount an attack. During the undercover operation, Petrowski noted, Smadi said if he were to be deported, he would go to Pakistan or elsewhere overseas to seek out terrorist training. The Bureau decided to use undercover agents to set up a sting. Three FBI agents—all Arabic speakers—began to talk with Smadi, first online and later in person. "He believed he had found an al Qaeda sleeper cell in the U.S. and that he was now planning the next 9/11 attack," Petrowski said. What followed was 10 months of around-the-clock surveillance, until the moment Smadi was arrested—after dialing a cell phone number he believed would detonate a truck bomb. But the bomb—which was made to Smadi's specifications—was a fake, supplied by our undercover agents. "This case involved a lot of work by many people throughout the FBI and our partner agencies," Petrowski said. In addition to the undercover agents, surveillance teams, and behavioral analysts, contributions were made by our bomb experts, the multi-agency Joint Terrorism

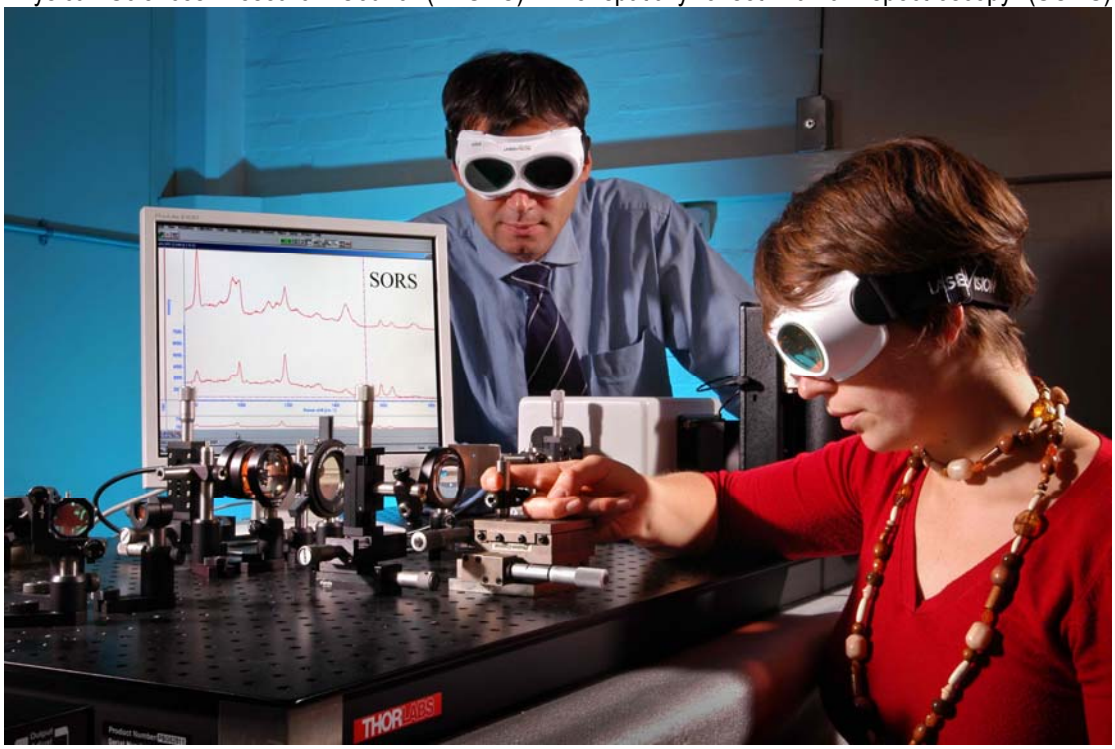


Task Force, attorneys in the U.S. Department of Justice, and other members of our Counterterrorism Division in Washington, D.C. The Smadi case ended successfully, with no injuries or loss of life. But the threat from lone offenders continues—and requires constant vigilance. "One big takeaway from this case," Petrowski said, "is the question of how many other potential violent extremists are out there, being exposed to terrorist ideologies online and contemplating an attack."

Laser has clinical, security applications

Source: http://homelandsecuritynewswire.com/laser-has-clinical-security-applications

A novel laser system that could help detect bone diseases -- and airport security; the spatially offset Raman spectroscopy (SORS) instrument uses a technique that allows it to scan deep into human tissue; the instrument is also being studied as a bottle and packaging scanner for airport security and is already used to assess the content of drugs. A novel laser system that could help detect bone diseases is to be tested at the Royal National Orthopaedic Hospital. The first commercially available laser of its kind, which also has potential uses in airport security, will be delivered to researchers at the hospital in Stanmore, where it will begin a four-year £1.7 million program funded by the U.K. Engineering and Physical Sciences Research Council (EPSRC). The spatially offset Raman spectroscopy (SORS)



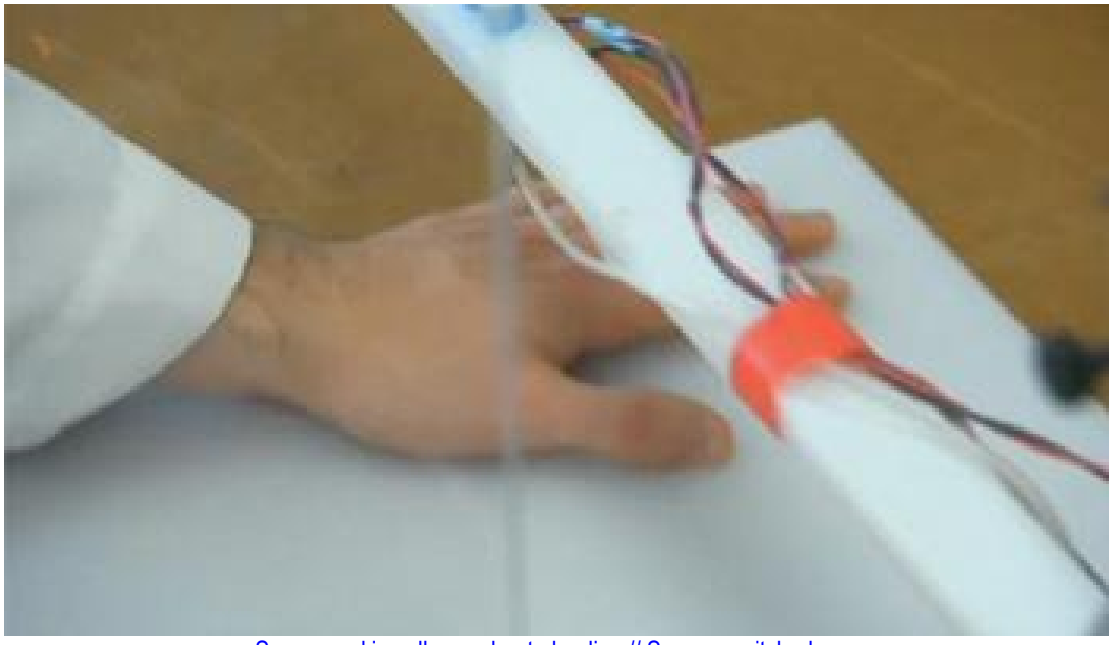
instrument uses a technique that allows it to scan deep into human tissue using simpler equipment than other spectroscopic lasers, making it more suitable for clinical use. Stephen Harris writes that this means it can assess the chemical make-up of bones to look for illnesses such as osteogenesis imperfecta (brittle bone disease). The instrument is also being studied as a bottle and packaging scanner for airport security and is already used to assess the content of drugs. The STFC Central Laser Facility developed the laser for the project in collaboration with its spin-out firm Cobalt Light Systems and UCL's Institute of Orthopaedics and Musculoskeletal Science. "SORS is really exciting because it gives us a potential screening system, where we look at not just a patient's genes but how their bones are modified," Allen Goodship, the institute's director and the project's principal investigator, told Harris. "Most imaging gives you information on the mineral density [in bone], whereas Raman spectroscopy allows us to look at the chemistry of the bonds of the collagen and its interaction with the mineral." SORS works by detecting and analyzing photons from the laser that spread out as they go deeper into a material. This removes the need to suppress the signal from photons reflected by the material surface that are stronger but do not spread out as much. "By gaining insight into the migration of photons, we realized they penetrate much deeper than we or anyone else thought possible," said Pavel Matousek,

SORS's inventor and chief scientific officer for Cobalt Light Systems. "On the basis of this effect, SORS enables you to do this with much simpler instrumentation. Rather than bulk instruments that occupy several rooms, you can do it with desktop equipment." To make the technique safe for use with human tissue, the laser has been adapted to shine a ring-shaped beam that can scan a wide surface area but has an intensity similar to that of a laser pointer. The project will also look at using the laser to detect osteoarthritis, which causes joints to degrade, and osteoporosis, where bone mineral density is reduced, increasing the risk of fractures. "We may be able to convert the laser to an endoscopic device and look at the bone under cartilage," said Goodship.

Wounded soldiers to be helped by "skin printer"

Source: http://homelandsecuritynewswire.com/wounded-soldiers-be-helped-skin-printer

Using an inkjet printer and cartridges full of living tissue, researchers demonstrate rapid healing in animals; the system, which lays down cells with the same fluid-based inkjet technology used in many printers, could print large swathes of living tissue directly onto the injuries of soldiers wounded on the battlefield.



Spray-on skin cells accelerate healing // Source: switched.com

In a recent presentation at the American College of Surgeons Clinical Congress, researchers from the Wake Forest Institute for Regenerative Medicine showed off the results of a unique experiment involving a printer that uses living cells as its "ink." Christopher Mims writes that the system, which lays down cells with the same fluid-based inkjet technology used in many printers, could print large swathes of living tissue directly onto the injuries of soldiers wounded on the battlefield. Covering burns and related wounds is of critical importance because, the scientists note, "any loss of full-thickness skin of more than 4 cm in diameter will not heal by itself." Tests on mice revealed advanced healing by both the second and third week of recovery, with complete closure and formation of scar tissue by week three in treated (but not untreated) subjects. The printer has two heads, one of which ejects skin cells mixed with fibrinogen (a blood coagulant) and type I collagen (the main component of the connective tissue in scars). The other head ejects thrombin (another coagulant). Mims notes that like the components of quick-setting resins which must be kept separate until mixing causes a chemical reaction that hardens the resin, the products of the two print heads mix to form fibrin immediately, yet a third protein involved in the clotting of blood. The whole confection is topped by a layer of keratinocytes (that is, skin cells), which are also printed. Future iterations of the research will be conducted on pigs (which have skin that more closely resembles that of humans), and it's not clear when, if ever, such a device might appear in a field hospital in Afghanistan, not to mention your local burn center.

Urban terror threats prompt new UK police training

Source: http://news.yahoo.com/s/ap/20101026/ap_on_re_eu/eu_britain_mumbai

The British bobby is about to go ballistic. Faced with growing terror threats involving urban areas, British police are receiving new weapons and specialized training from the SAS, Britain's elite military unit. The hope is that the training and equipment will help if Britain ever faces an attack similar to the 2008 Mumbai shooting spree that killed 166 people and paralyzed India's business capital for days. Tuesday's announcement comes amid an active European terror threat being tracked by U.S. and European officials. The U.K.'s terror threat rating remains at "severe" — the second highest tier — which means an attack is likely.

News of a possible Mumbai-styled small arms attack emerged last month after the CIA increased strikes in Pakistan to flush out al-Qaida operatives suspected in the plot. Some of the plot's details came from a terror suspect arrested in Afghanistan, intelligence officials have said. Terror attacks in cities pose multiple challenges — there are more people, increased difficulties in responding because of clogged routes and multiple problems in evacuating crowds. British officials have refused to comment on whether the plan will arm more of Britain's some 144,000 police officers — a fraction of whom are in armed response units. But they praised the new training. "We are in a much better place than ever before, with dedicated counterterrorism units based within our regions," a spokeswoman for the Association of Chief Police Officers said, speaking on condition of anonymity in line with departmental policy. "This new training and equipment will put us in an even better position." Part of the problem in Mumbai was that the first Indian police to respond were armed with little else than sticks and batons while the attackers had AK-47s. Britain has a deep-rooted tradition of having unassuming and unarmed police — iconic images of bobbies donning their trademark hats and batons. Although gun crimes are relatively rare in Britain because of tough gun laws, unarmed police struggled for hours last summer to stop a taxi cab driver who went on a shooting spree, killing a dozen people in rural England. Officers said they had to break off their pursuit of the suspect, Derrick Bird, when he turned his gun on unarmed officers. The new police arsenal will include automatic or semiautomatic weapons that are more powerful and accurate, but Britain's Home Office — which overseas the police — refused to give further details about the types of weapons or how many officers would receive them. Some U.S. officials have been calling for American police officers to be armed with assault rifles to better prepare for Mumbai-style urban attacks. Warren Bamford, the special agent in charge of the FBI in Boston, has backed proposals to arm some neighborhood police with the semiautomatic weapons. Boston Mayor Tom Menino had criticized a proposal to arm up to 200 officers with M-16s, saying only specialized police units should have those guns. The New York Police Department, after studying the Mumbai attack, decided to train reinforcements for its 400 Emergency

Service Unit officers who can carry fully automatic Colt M4 rifles. An additional 200 officers have regularly been put through exercises using Mini-14s, a lightweight semiautomatic weapon.

Indian police are also changing their tactics and equipment.

"Mumbai police officers showed tremendous devotion to duty, but they lacked the requisite commando training and equipment to fight the attackers," said K.P.S. Gill, a retired senior Indian police officer with experience in India's counterinsurgency operations. An inquiry this month into the 2005 suicide attacks in London that killed 52 commuters illustrated just how difficult it was for emergency workers to reach four separate blast sites and the chaos that reigned as everyone tried to determine what was happening. Militaries around the world have long struggled with urban warfare. "The Battle of Algiers" — a film about France's colonial struggle with insurgents in the Algerian capital — has been used by militants and governments alike as a training lesson in urban combat. "Most of us have specialized training of some sort, but a situation like Mumbai would be difficult to deal with in London — largely because of how densely populated it is and because of how badly it's congested," a police officer in a specialized unit told The Associated Press. "There would almost certainly be casualties." He spoke on condition of anonymity because he was not authorized to speak to the media. The Home Office declined to elaborate on the training, some of which will be taking place at military bases in Britain. The Ministry of Defense would also not comment on the training. Brian Jones, an American tourist in London, said he believed all the equipment and training in the world wouldn't likely stop an urban attack. "What happens happens and there is nothing we can really do to stop it," said the 50-year-old from Boston. But 21-year-old Payal Patel from India had a different view. "I think increasing security this way is absolutely necessary," she said. "We need to do what we can to prevent any future attacks."

Al Qaeda Brigade 313 website goes online

Source:http://www.longwarjournal.org/archives/2010/08/al_qaeda_brigade_313_website_goes_online.php#ixzz15eWKsRWu

Banner for the Al Qaeda 313 Brigade website/forum. Pictured, from left to right, are Mustafa Abu Yazid, Abu Yahya al Libi, and Ilyas Kashmiri.

A website connected to al Qaeda's military arm in Pakistan has sprung up on the Internet in the past month. The website, called Al Qaeda Brigade 313, at www.aqbrigade313.com, was registered on June 2, 2010, and became active in early July. The site has 86 registered users and five administrators, according to a report at the Open Source Center that was obtained by *The Long War Journal*. The website contains a forum and a blog, and posts links to Taliban propaganda, including a statement by failed Times Square bomber Faisal Shahzad. Several authorities, including US intelligence officials and an expert on terrorist websites, all of whom wish to remain anonymous, said that the Al Qaeda Brigade 313 website appears to be legitimate and may be directly associated with al Qaeda. The Brigade 313 website's landing page has the words "Al Qaeda Brigade 313" in the center, while text describing Harkat-ul-Jihad-al-Islami, Lashkar-e-Jhangvi, Jundallah, and the Movement of the Taliban in Pakistan occupies the four corners of the page. Once inside the Al Qaeda Brigade 313, a banner appears with images of slain al Qaeda leader Mustafa Abu Yazid and ideologue Abu Yahya al Libi on the left, and an image of Ilyas Kashmiri on the far right [see banner above]. Yazid was al Qaeda's leader in the Khorasan, which includes Pakistan and Afghanistan, before he was killed in a US Predator strike in North Waziristan in May 2010. Brigade 313 is al Qaeda's military organization in Pakistan, and is made up of Taliban and allied jihadist groups. Members of Laskhar-e-Jhangvi, Harkat-ul-Jihad-al-Islami, Lashkar-e-Taiba, Jaish-e-Mohammed, Jundallah (the Karachi-based, al Qaeda-linked group), and several other Pakistani terror groups are known to have merged with al Qaeda in Pakistan, and the group operates under the name of Brigade 313. This group is interlinked with Pakistan's Taliban and also recruits senior members of Pakistan's military and intelligence services, a senior US intelligence

official told *The Long War Journal*. Brigade 313 has been behind many of the high-profile attacks and bombings inside Pakistan, including multiple assassination attempts against former President Pervez Musharraf and Prime Minister Gilani. The unit has also been involved in the rash of attacks on

A screen shot of the Al Qaeda Brigade 313 main web page; click image to view.

Pakistan's military and intelligence services, including the assault and siege of the Army General Headquarters in Rawalpindi in December 2009. Brigade 313 is led by Ilyas Kashmiri, who is also the leader of the Lashkar al Zil or the Shadow Army, al Qaeda's military organization along the Afghan-Pakistani border. Kashmiri is suspected of planning and leading some of the terror group's most sophisticated assaults in the Afghan-Pakistan theater. He also has been implicated in the failed 2009 plot by Najibullah Zazi to carry out suicide attacks on New York City's subways. The Lashkar al Zil is also known at the Jaish al Usrah, or the Army of the Protective Shield. The Lashkar al Zil operates six brigades in the Afghan-Pakistan border region, including Brigade 055, al Qaeda's original military formation, which was created during the rule of the Taliban in the 1990s. Abu Laith al Libi was the leader of Brigade 055, another al Qaeda military formation based in Afghanistan, before he was killed in a Predator airstrike in North Waziristan in January 2008. The Lashkar al Zil is also thought to operate other formations in Somalia and Yemen. The US killed the previous commander of the Lashkar al Zil, Abdullah Said al Libi, during a Predator airstrike in North Waziristan in December 2009. Brigade 313 is named after the 313 companions who fought with Mohammed during the Battle of Badr.

Background on Ilyas Kashmiri

Ilyas Kashmiri is considered by US intelligence to be one of al Qaeda's most dangerous commanders. He served as the operational chief of the Harkat-ul-Jihad-allslami, an al Qaeda-linked terror group that operates in Pakistan, Kashmir, India, Afghanistan, and Bangladesh. Kashmiri was recently listed as the fourth most wanted terrorist by Pakistan's Interior Ministry. Kashmiri is now serving as the "acting chairman of the military committee as Saif al Adel has moved up the ranks," a senior official told *The Long War Journal* in 2009. Saif al Adel, who is thought to be based in Iran, served as al Qaeda's version of the US Chairman of the Joint Chiefs of Staff as well as a top strategist. Kashmiri is thought to have played a major role in the multi-pronged suicide attack against government and security installations in the eastern Afghan province of Khost in May 2009, the military intelligence official said. In 2008, Kashmiri reportedly drafted a plan to assassinate General Ashfaq Pervez Kayani, Pakistan's top military officer, but the plan was canceled by al Qaeda's senior leadership, according to a report in the *Asia Times*. Although he is currently listed as a most wanted terrorist by the Pakistani government, Kashmiri is also a longtime asset of Pakistan's military and intelligence services. He served as a commando in the elite Special Services Group (SSG), Pakistan's special operations unit trained by Britain's Special Air Service. In the early 1990s, Kashmiri was ordered by the military to join the Harkat-ul-Jihad-al-Islami, and later he was urged to join the Jaish-e-Mohammed, which he refused to do. Kashmiri reportedly dropped out of favor with the military after refusing the military's suggestion to join Jaish-e-Mohammed. In 2003 he was arrested after being accused of involvement in the assassination attempts against then-President Musharraf, and was later released. After the 2007 Pakistani Army assault on the radical Lal Masjid in Islamabad, he set up camp in Ramzak in North Waziristan, and was joined by several Pakistani Army military officers. Kashmiri is widely thought to have maintained his links with the radical elements in Pakistan's military and intelligence services throughout his time operating with jihadi groups. Kashmiri was behind the assassination of Major General Faisal Alvi, the retired commander of the SSG, in Rawalpindi in late 2008. Alvi was killed just months after sending a letter to General Kayani. In the letter, Alvi accused two generals of forcing his retirement. According to *The Times Online*, Alvi said he was forced to retire after threatening to expose the two generals' involvement with the Taliban. Kashmiri is on the record as swearing allegiance to Afghan Taliban leader Mullah Omar as far back as 1999. "[W]e folks have taken oath from Mullah Omar and we consider him

as Ameerul Momineen [the leader of the faithful]," Kashmiri told a Pakistani reporter a decade ago. "We have absolute permission from him to go to any place and engage ourselves in jihadi activities."

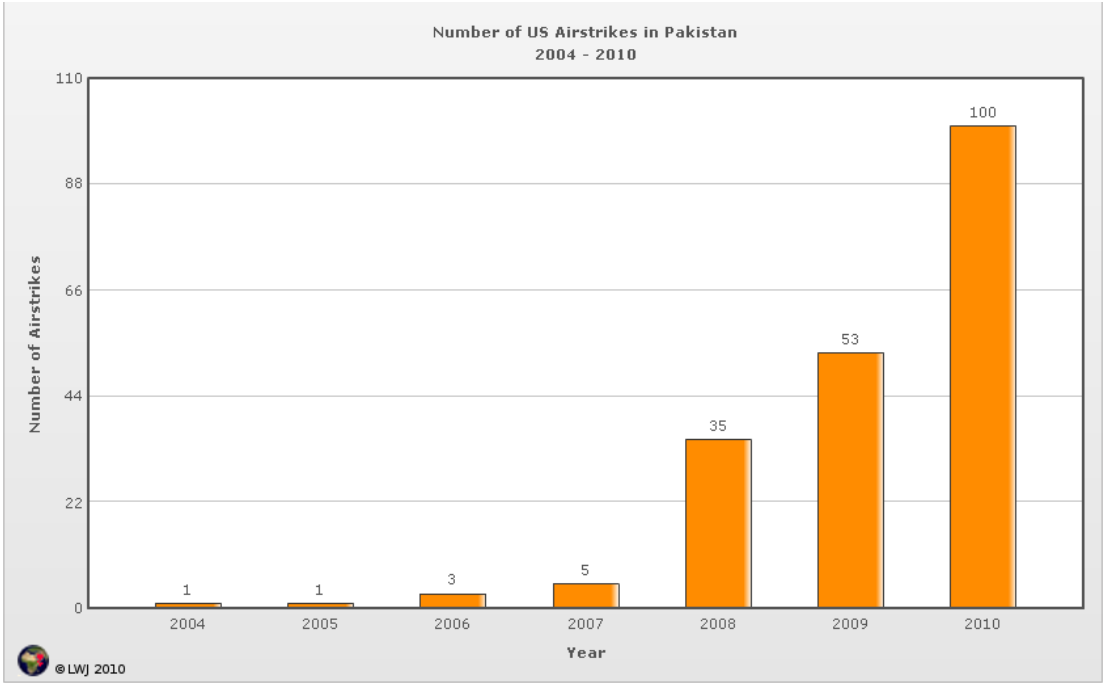
Charting the data for US airstrikes in Pakistan, 2004 - 2010

Created by Bill Roggio and Alexander Mayer

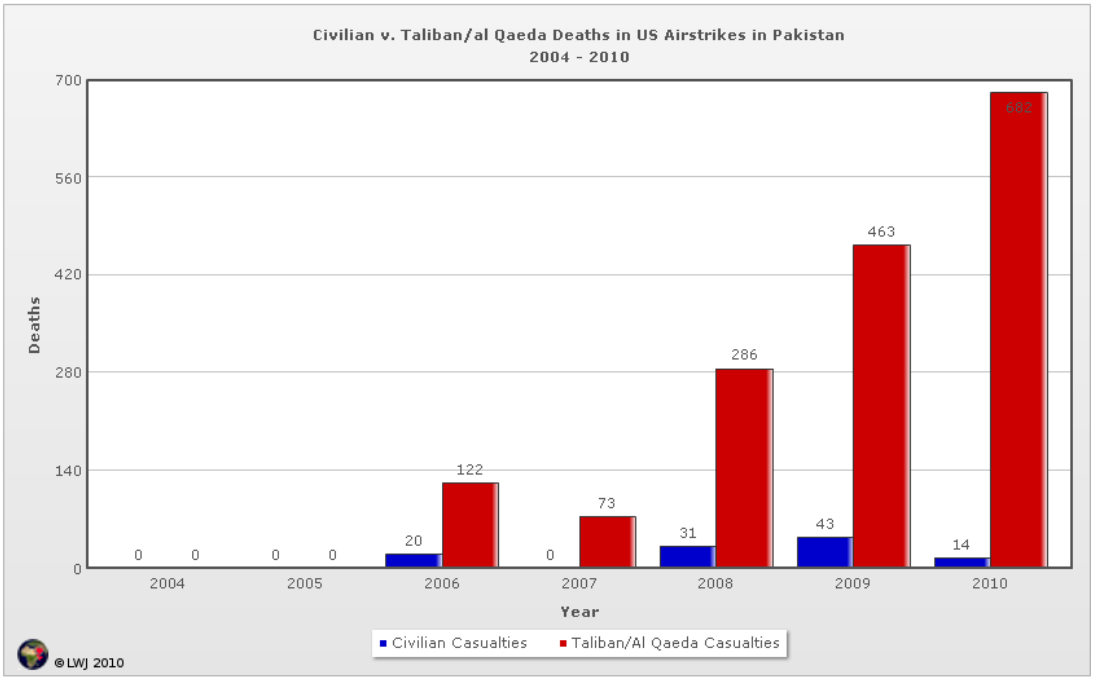
Source: http://www.longwarjournal.org/pakistan-strikes.php

Since 2004, the US has been conducting a covert program to target and kill al Qaeda and Taliban commanders based in Pakistan's lawless northwest. The program has targeted top al Qaeda leaders, al Qaeda's external operations network, and Taliban leaders and fighters who threaten both the Afghan and Pakistani states. The charts below look at the following: 1) the number of US airstrikes inside Pakistan per year; 2) civilian casualties vs. Taliban/al Qaeda casualties; 3) the distribution of strikes over time by tribal agencies; 4) the overall distribution of strikes, by tribal agencies; 5) the distribution of strikes over time by territories targeted; 6) the overall distribution of strikes, by territories targeted; and 7) the number of high value targets killed in territories managed by individual Taliban commanders. The data is obtained from press reports from the Pakistani press (*Daily Times*, *Dawn*, *Geo News*, *The News*, and other outlets), as well as wire reports (*AFP*, *Reuters*, etc.), as well as reporting from *The Long War Journal*. Given the Taliban's control of the areas where strikes occur, and a dearth of reporters in those areas, the exact numbers for casualties are difficult to know. For more details on the Predator program and its effects, see *LWJ* report, Analysis: US air campaign in Pakistan heats up. For a list of al Qaeda and Taliban leaders thought to have been killed in the attacks, see *LWJ* report, Senior al Qaeda and Taliban leaders killed in US airstrikes in Pakistan 2004 - 2010.

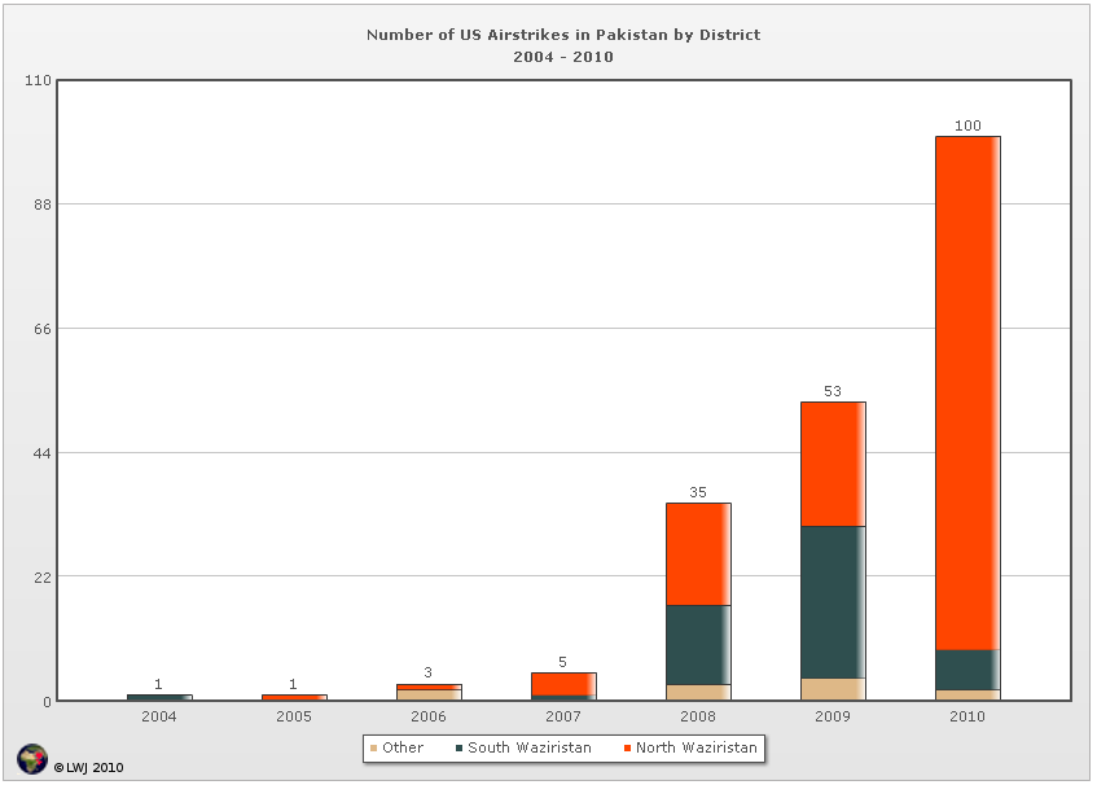
This page was last updated on Tuesday, November 16, 2010, 4:39 pm GMT. These seven charts will be updated when information about prior or new strikes comes to light.



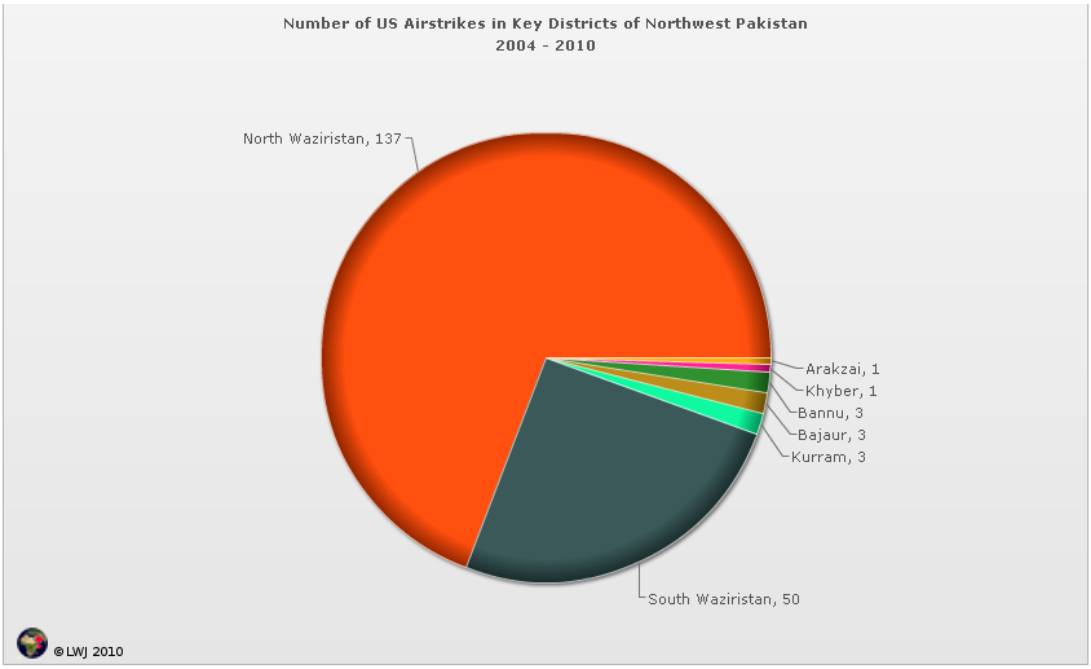
The US ramped up the number of strikes in July 2008, and has continued to regularly hit at Taliban and Al Qaeda targets inside Pakistan. There have been 198 strikes total since the program began in 2004; 188 of those strikes have taken place since January 2008.



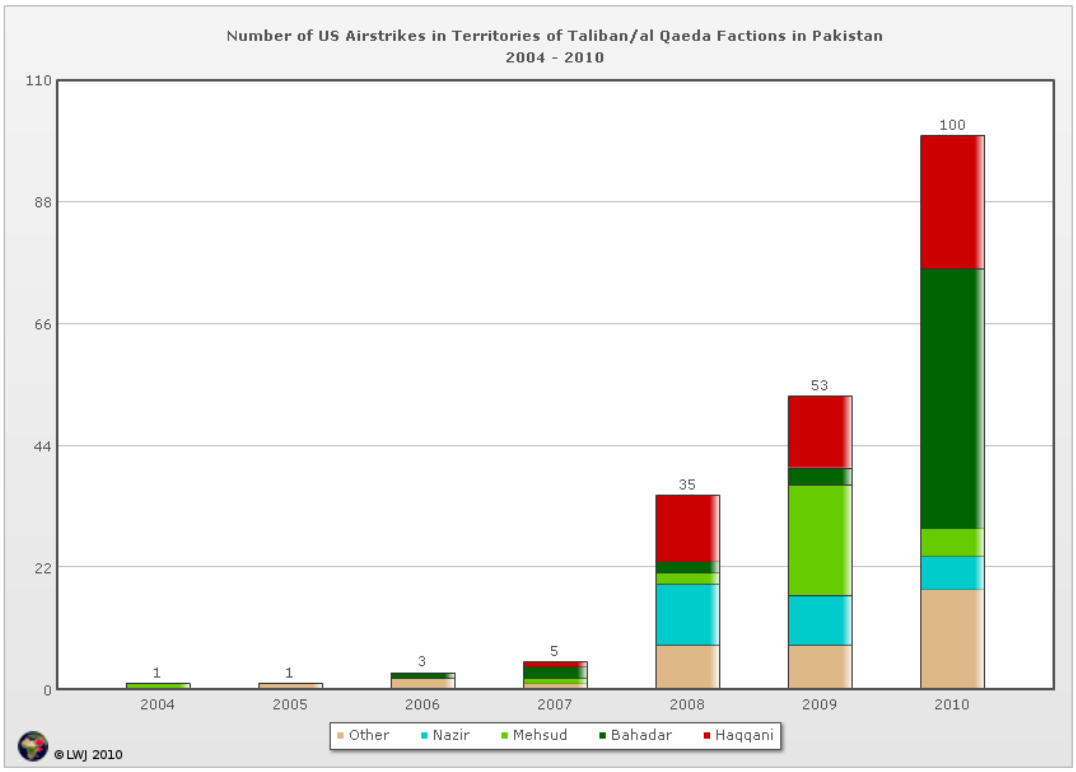
Since 2006, there have been 1,626 leaders and operatives from Taliban, Al Qaeda, and allied extremist groups killed and 108 civilians killed. Data for 2004 and 2005 are not available at this time.



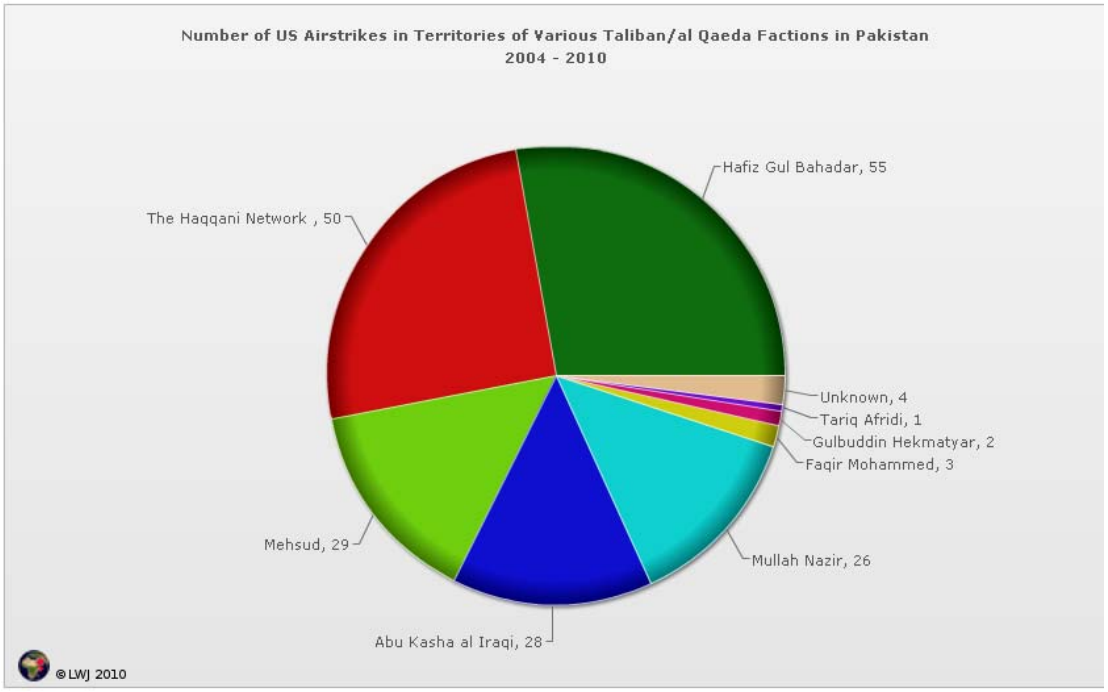
Over the past six years, the strikes have focused on two regions: North and South Waziristan. Over the past two years, there has been a dramatic shift in the location of the strikes. In 2009, 42% of the strikes took place in North Waziristan and 51% in South Waziristan. In 2010, 91% of the strikes have taken place in North Waziristan and 7% in South Waziristan.



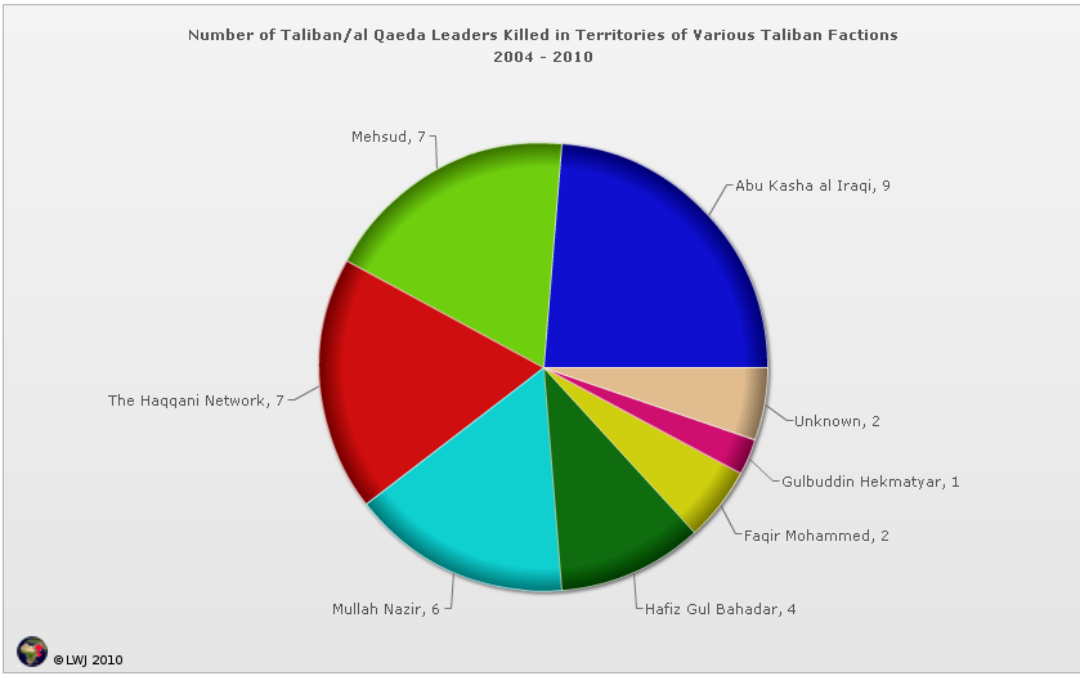
Of the 198 strikes since 2004, 70% have hit targets in North Waziristan, and 26% have hit targets in South Waziristan.



The majority of the attacks have taken place in the tribal areas administered by four powerful Taliban groups: the Mehsuds, Mullah Nazir, Hafiz Gul Bahadar, and the Haqqanis. In 2010, there was a dramatic shift in strikes to tribal areas administered by Hafiz Gul Bahadar.



Mullah Nazir and Waliur Rehman are based in South Waziristan; the Haqqanis, Hafiz Gul Bahadar, and Abu Kasha al Iraqi are based in North Waziristan; Hakeemullah Mehsud is based in Arakzai; and Faqir Mohammed is based in Bajaur. Two bases operated by Gulbuddin Hekmatyar were hit in South Waziristan. For four of the strikes, territorial control has not been reported.



The Pakistani government considers Nazir, the Haqqanis, Bahadar, and Hekmatyar to be a 'good Taliban' as they do not carry out attacks against the Pakistani state. All of these Taliban factions shelter al Qaeda and various other terror groups.

Manchester Airport conducts distance biometrics trial

Source: http://homelandsecuritynewswire.com/manchester-airport-conducts-distance-biometrics-trial

Manchester Airport begins a 2-week trial of a system which can recognize an individual's iris while they walk around; the system might allow international transfer passengers to mix with domestic passengers in a departure lounge because they can be securely identified before boarding their flight. Manchester, U.K. Airport's passengers will be invited to participate in the trial of a system that can recognize an individual's iris while they walk around. The trial of the system, which was developed by Liverpool-based Human Recognition Systems, will last for two weeks in the airport's Terminal 1. Passengers register after check-in so that their iris can be used to identify them as they enter the security search area. The technology could have a variety of future applications to speed up the identification of passengers. For example, it might allow international transfer passengers to mix with domestic passengers in a departure lounge because they can be securely identified before boarding their flight. Currently, arriving passengers from overseas who are connecting to another international flight in Manchester remain separated from domestic passengers to protect the integrity of U.K. border security. The airport already uses iris-recognition technology to manage staff access into sensitive areas of the airport. Immigration authorities also use it for pre-registered people arriving back into the United Kingdom. The current system, however, requires users to look directly into a device that uses photo-recognition software to authenticate individuals. The trial is one of several currently taking place at airports across the United Kingdom as part of a government program called Innovative Science and Technology IN Counter-Terrorism, or INSTINCT. Run by the Home Office, INSTINCT looks to identify and trial innovative counter-terrorism technologies, solutions or ideas.

Airline Wi-Fi sparks security concerns

Source: http://www.ajc.com/news/nation-world/airline-wi-fi-sparks-743309.html

Even as airline passengers struggle with whether they should have the full-body security scan or go for the "enhanced" pat-down, another potential safety issue has arisen: Does the coming of Wi-Fi service to passengers pose any sort of danger aboard the plane? A number of airline workers, security professionals and technologists say they agree Wi-Fi can create serious security risks. The question arose after Yemeni terrorists tried recently -- and failed -- to destroy two U.S.-bound cargo planes by stuffing printer cartridges full of explosives and then detonating the charges in flight. British explosives consultant Roland Alford created a stir when he told New Scientist magazine that Wi-Fi is a "Pandora's box" for terrorists and that giving passengers Internet access "gives a bomber lots of options for contacting a device on an aircraft." A number of airline workers, security professionals and technologists say they agree that Wi-Fi can create serious security risks. The Association of Flight Attendants, for example, has asked the government to ban Wi-Fi. "We recognize the potential of the threat and are looking at it closely," said Gideon Ewers, the spokesman for the International Federation of Air Line Pilots' Associations. His reaction was mirrored by the Washington. D.C.-based Air Line Pilots Association. "We need to fully explore what could the bad guys do, how could this be turned against us," said Robb Powers, a Boeing 737 pilot and chairman of the national security committee for ALPA. Security expert and blogger Bruce Schneier dismissed such concerns in a blog posting last week: "Put together a sloppy and unsuccessful

package bomb with an imagined triggering mechanism, and you have a *new and dangerous threat* that -- even though it was a threat ever since the first airplane got Wi-Fi capability -- must be immediately dealt with right now," he wrote. "Please, let's not ever tell the TSA about timers. Or altimeters." The Yemeni bomb plot demonstrates one way Wi-Fi could facilitate terrorists, said Dinkar Mokadam, an occupational safety expert with the Association of Flight Attendants. He said wifi Wi-Fi and Internet-enabled calls could enable a terrorist to maneuver around the U.S. ban on the use of cell phones on airplanes and actually trigger a bomb. “This sort of a detonation doesn’t require a voice," Mokadam said. "It requires communication to a cell phone and you can text to a device and have it go off. You don’t have to even talk to it.” Banning Wi-Fi use completely or during high security-alert periods are two of several proposals the Department of Homeland Security is considering. TSA spokesman Greg Soule said DHS was “using the latest intelligence and state of the art technology to address ever-evolving threats.” Some travellers say they fail to see the risk. “I don’t think the Wi-Fi to trigger a bomb is something to worry about,” said Jon Safran, who lives in Atlanta and travels at least once a week. “I’m just not quite sure it’s technically feasible to do all that, get it through security and trigger it. And I guess you’d have to be on the plane yourself dialling it in. “I think one or two incidents shouldn’t be a reason to fundamentally change our lives,” Safran said. He said he thought a ban of Wi-Fi would be an overreaction. Scott LaGrand, who lives in Columbus, Ohio, and recently passed through was at Hartsfield-Jackson International Airport, said he travels often for work and has been on flights with in-flight wi-fi Wi-Fi but also hasn’t used it. before. “If there’s proof that those sorts of things could happen, then I would support not having Wi-Fi available,” said LaGrand, who is also a former Atlanta Knights hockey player. “Because it’s not something that most travellers have become accustomed to, I don’t think we would be missing it.” While the Yemeni bombs contained cell phone components, they do did not appear to have been designed to detonate with a phone call but by cell phone alarm; that is, communication with the plane would not have been necessary to set off the bombs. But since the call-activated bomb is an established technique, terrorists could conceivably hide devices in checked luggage and then trigger them through an Internet-enabled call, according to Roland Alford’s father and business partner, explosives engineer Sidney Alford. The debate comes at a time when airlines are ramping up their marketing of Wi-Fi service to passengers. AirTran and Delta Air Lines, for example, have partnered with Google to offer free Wi-Fi aboard hundreds of their planes during the holidays. At Southwest Airlines, where Internet service is being installed on airplanes, spokesman Chris Mainz said their broadband doesn’t work that way. “Our Wi-Fi product will not enable cell phone-to-cell phone interaction and it blocks Voice over Internet Protocol,” Mainz said. Whether Voice over Internet Protocol (VoIP), the system that delivers voice communication over the Internet, can be completely restricted is not entirely certain. Aircell, the airline Internet company in Illinois that provides broadband to airlines including Delta, AirTran and American Airlines under the name Gogo, declined to be interviewed for this story. But earlier this year, Aircell released a statement saying it is “extremely difficult to stop every instance of VoIP.” Delta Air Lines declined to comment on its security practices. In opposing the use of cellphones on airplanes in the U.S., DHS, the FBI and the Department of Justice said in 2005 that they were concerned that terrorists or hijackers could use the phones to “facilitate a coordinated attack,” either with someone on the ground, on another airplane or even among people sitting in different sections of the same airplane.

New worry: terrorists may blow up off-shore oil rigs

Source: http://homelandsecuritynewswire.com/new-worry-terrorists-may-blow-shore-oil-rigs

The BP disaster offers new venue for terrorists: blowing up off-shore oil rigs in order to inflict vast economic and environmental damage and impose steep costs on the U.S. government and private companies; terrorists can make such attacks on the cheap because oil rigs are unprotected and

completely vulnerable; lawmakers note that the Nuclear Regulatory Commission (NRC) now requires that atomic generators withstand plane crashes; Senator Jim Webb says that similar standards should be considered for the oil and gas industries; in a letter to President Obama he says: "While Congress will continue to scrutinize BP and regulatory agencies, I write to urge you to also be vigilant against deliberate acts, such as an attack or sabotage, that could similarly devastate the region". Offshore drilling rigs present relatively easy targets for terrorist attack. Oil derricks may not be sprouting anytime soon off the Virginia coast because of the BP blowout, but the state's senior U.S. senator says those operating elsewhere must be protected from another threat: terrorism. Democrat Jim Webb, a member of the Senate Armed Services Committee, is calling on the Obama administration to develop safeguards

for shielding offshore platforms from attack. The Richmond Times-Dispatch's Jeff Schapiro writes that Webb made his case in a recent letter to Defense Secretary Robert Gates, Secretary of Homeland Security Janet Napolitano, and Interior Secretary Kenneth Salazar. "While Congress will continue to scrutinize BP and regulatory agencies, I write to urge you to also be vigilant against deliberate acts, such as an attack or sabotage, that could similarly devastate the region," says Webb, referring to the oil-rich Gulf Coast. Webb favors exploration for oil and gas in Virginia waters, but after the Deepwater Horizon disaster he backed a White House-ordered delay until safety and environmental concerns are addressed. In his letter, Webb notes that the Nuclear Regulatory Commission (NRC) now requires that atomic generators withstand plane crashes. Similar standards should be considered for the oil and gas industries, Webb says. "Security issues surrounding oil and gas drilling are of a different nature, but a lack of vigilance could leave the marine ecosystem, as well as certain areas of our national security, at great risk," Webb said. "The Deepwater Horizon incident has caused the worst environmental disaster in our nation's history. With dozens of wells operating in the Gulf of Mexico and elsewhere, we must employ policies that mitigate all types of risk. "I therefore request that you provide, as soon as practicable, your assessment of the vulnerability of offshore oil rigs to attack, the current framework for addressing such risks and your recommendations to Congress for deploying adequate resources and safeguards," Webb says. Schapiro notes that Webb's request for administration suggestions to Congress on improving security of offshore platforms comes as the Virginian readies for a possible rematch in two years with the incumbent Republican he narrowly defeated in 2006, George Allen. Allen, too, supports energy exploration off the state's coast. A former governor, Allen operates a political consultancy that is aligned with the U.S. energy industry and through which he advocates for increased domestic drilling.

Econo-Jihad: Terrorists increasingly focus doing economic damage to West

Source:http://homelandsecuritynewswire.com/econo-jihad-terrorists-increasingly-focus-doing-economic-damage-west

After the 9/11 attacks, Bin Laden boasted that he sued an operation which cost al Qaeda $500,000 to finance to inflict a $500 billion damage on the U.S. economy; it was not a mere boast: it was an indication the econo-jihad was an integral part of al Qaeda's strategy to weaken and defeat the West; "the economic turn actually influences the terrorists' targets, which have included oil-drilling infrastructures, tourism, international economic institutions and more. Indeed, Islamic terrorism's future devices will focus on targets that will yield the most economic damage," one expert says. Islamic terrorist organizations have set economic terrorism as their new target, intending to harm and paralyze Western economies, the United Sates in particular, claims Professor , a specialist on terrorism over the Internet at the University of Haifa 9Weiman is the author of *Terror on the Internet: The New Arena, the New Challenges* [2006]). According to Weimann, who has monitored Web sites hosted by terrorist and terrorism-supporting organizations, “For the Jihadists, the present economic crisis signifies an ideal opportunity and platform to leverage an economic terrorist campaign.” The *Eurasia Review* reports that in the course of a study that was carried out over a number of years, Weimann surveyed public and encoded websites run by Islamic terrorist organizations, forums, video clips, and practically all the information related to Islamic Jihad terrorism that is flowing through the network. According to Weimann, the focus on economic terrorism was set in motion with the 9/11 attack on the Twin Towers, when Osama bin Laden stated on the video tapes that he sent out that these attacks mostly damaged the U.S. economic base and that these attacks, which cost $500,000 to carry out, cost the U.S. $500 billion. Other publications by bin Laden himself and by other terrorist leaders show that they understand that Western and U.S. power lies in their economic strength and that the jihad movement should focus on damaging this power by employing various tactics, including: hitting international corporations directly; harming international corporations by means of 1.2 billion Muslims boycotting them, which would pressure the respective governments to adjust their policies; striking at resources that were “looted” from Muslim countries, such as oil-drilling companies in Iraq; assassinating key personalities in the global economy, most of whom they believe are Jews, and killing anyone who collaborates with these personalities. Monitoring the Muslim terrorist-related information on the Internet, Weimann also claims that the armed struggle against the United States in Iraq and Afghanistan is aimed at prolonging American expenditure on maintaining forces in these countries, and not necessarily at military defeat. The jihadists believe that this would help drain America’s financial resources and eventually critically damage the American economy, said Weimann, adding that therefore, they aim to make the United States open as many military fronts around the world as possible. Another result of this new focus on Econo-Jihad is an increasing jihadist interest in Web sites and online information on the American and Western economies, so as to glean an understanding of how these economies can be hit the hardest. Not only official Web sites are monitored: forums and e-mails of individual surfers are penetrated too. By tracking Jihadist forums, Weimann said he has found that these surfers are increasingly following Western finance-related media publications too, as well as expert and academic analyses of the factors influencing Western economy, such as the war in Iraq, global terrorism, natural disasters, oil prices, unemployment rates, and declines in the stock market. “One might think that an Econo-Jihad is less violent, but this is not the case. Jihadist Internet monitoring alongside terrorist activity in the field, is evidence that the economic turn actually influences the terrorists’ targets, which have included oil-drilling infrastructures, tourism, international economic institutions and more. Indeed, Islamic terrorism’s future devices will focus on targets that will yield the most economic damage,” Weimann said.

Non-lethal device deters hostile divers

Source: http://homelandsecuritynewswire.com/non-lethal-device-deters-hostile-divers

Hostile divers may be deterred from approaching U.S. Navy ships, sea ports, off-shore oil rigs, and other infrastructure facilities with an acoustic device that overwhelms them with the amplified sound of their own breath; the device generates low frequency underwater sound that interferes with breathing, induces disorientation, panic, uncontrolled ascent to surface, and decompression sickness. A researcher in the United States is developing a non-lethal weapon for protecting ports from divers with malicious intentions. Dr. Alexander Sutin, a research professor at Stevens Institute of Technology, New Jersey, believes such divers could be thwarted with an acoustic device that overwhelms them with the amplified sound of their own breath. The technique may offer DHS and the U.S. Navy an alternative to underwater explosive charges or loud underwater sirens, which may negatively impact marine life.

According to a paper by Sutin and Dr. Yegor Sinelnikov, current underwater sound systems to deter divers generate low frequency underwater sound that interferes with breathing, induces disorientation, panic, uncontrolled ascent to surface, and decompression sickness. Strong sound with acoustic pressure above 170-180dB can cause lung and liver damage. Marine life and other divers can suffer, too, because the sound is radiated in all directions. The *Engineer* reports that Sutin's idea is to detect the diver's breathing passively instead of using an active acoustic technology such as a sonar ping. The acoustic noise given off by the diver could be used to focus acoustic energy back to the diver because he or she acts as an active self-disclosing acoustic beacon. Time Reversal Acoustics (TRA) has been proposed to produce a precise, amplified beam of sound loud enough to overwhelm an intruder. The major advantage of proposed approach is that the TRA system for non-lethal neutralization focuses all radiated, refracted, reflected and scattered underwater sound back to a hostile swimmer. The next step in the development of the technology will be to create a method to isolate a narrow band of the breathing sound and radiate it back to the diver.

—Read more in Alexander Sutin and Yegor Sinelnikov, "Time Reversal Acoustic Approach for Non-Lethal Swimmer Deterrent" (paper presented at the 2nd Pan-American/Iberian Meeting on Acoustics, Cancun, Mexico, 16 November 2010)

Robot soldiers, first responders could make better decisions than humans

Source:http://homelandsecuritynewswire.com/robot-soldiers-first-responders-could-make-better-decisions-humans

Air Force Lt. Gen. David A. Deptula says that soon enough, soldiers will be "swimming in sensors and drowning in data"; to avoid that, BAE has developed ALADDIN (Autonomous Learning Agents for Decentralized Data and Information Networks), which allows a network of robot soldiers quickly to collect and exchange information and then to bargain with each other to determine the best course of action and execute it.

Modern warfare relies increasingly on robotics for intelligence gathering — but increasingly also for strike capabilities. The decision-making capacity, though, still rests solely in the hands of human commanders. British defense company BAE systems is testing a way to turn over battlefield decisions over to robot troops as well. The *Economist* reports that ALADDIN (Autonomous Learning Agents for Decentralized Data and Information Networks) is BAE's response to the overload of sensors and data now confronting battlefield commanders who now have UAV observations, soldier-based sensors, satellite data, and reams of other intelligence washing over them in such volumes that, as Air Force Lt. Gen. David A. Deptula puts it, they will be "swimming in sensors and drowning in data." The system allows a network of robot soldiers quickly to collect and exchange information and then to bargain with each other to determine the best course of action and execute it. The robots are armed with algorithms employing a range of models — game theory, probabilistic modeling, optimization techniques — that let them predict outcomes and allocate battlefield resources far more quickly and efficiently than humans trying to process the same amount of data. All that should help troops — both robotic and otherwise — avoid drowning in the data deluge. Does it work, though? *Popular Science* reports that ALADDIN has not seen any trigger time yet, but BAE and university researchers collaborating on the system have put it through simulated natural disasters (another potential application). Disasters, they theorize, are similar to warfare in their chaotic nature, and therefore the simulations are a good analog. In disasters the system operates well: Robots gather data on the various casualties in different areas, objectively assess where a limited number of ambulances can have the greatest possible impact, and execute a strategy quickly without egos or human emotions or errors clogging up the machinery. It is like an auction for resources based on need, and while it may sound insensitive to auction off life-saving help to a bunch of machines, when this resource auction was eliminated from some simulations, some of the ambulances were not used at all because the system could not figure out where to send them. BAE is building what is known as "flexible autonomy" into ALADDIN which will keep the higher decisions in the hands of humans (decisions like "go to war" and "don't go to war," for instance). The idea of being able to crunch sensor data, raw intelligence, crowd-sourced information from the Web, and other data sources to make good decisions quickly could prove invaluable.

ONE STEP AHEAD: Al-Qaeda 'planned poison plot'

Source: http://english.aljazeera.net/news/middleeast/2010/12/201012412410125305.html

Operatives plotted to kill government officials and media workers by sending them poisoned perfumes, Al-Qaeda members planned to kill Saudi Arabian government and security officials, as well as media workers, by sending poisoned gifts to their offices, a Saudi interior ministry official was quoted as telling the Reuters news agency. Last month, Saudi Arabia said it had captured 149 al-Qaeda-linked fighters over the past few months. They were accused of raising money and recruiting members to carry out attacks inside the kingdom. The group "planned to rob banks and companies to finance their operations", the official, who declined to

be named, said on Saturday. "Using poisoned perfume ... is one of the ways the arrested people planned to carry out their assassinations," he said. The operatives, who have apparently revealed this information to Saudi security forces since their arrest, belonged to 19 al-Qaeda cells and included 124 Saudis and 25 foreigners.

Change in tactics

"Changes from explosives to chemicals is significant because it demonstrates resolve and the ability to try to trick the security services," Theodore Karasik, a security analyst at the Dubai-based group INEGMA, said. "This is a change in tactics. It means they are trying every possible way to spread

chaos... The security services are very lucky that they discovered this," he said. The arrests announced last month were part of one of the largest crackdowns on al-Qaeda by Saudi Arabia in years. The groups detained have links to fighters in Somalia and Yemen, the interior ministry said. Saudi Arabia has been fighting al-Qaeda for years but in 2009 the Saudi wing of the group merged the Yemeni group to form Al-Qaeda in the Arabian Peninsula (AQAP), based in Yemen. In August 2009, a suicide bomber posing as a repentant al-Qaeda fighter tried to assassinate Saudi Arabia's senior anti-terrorism official, Prince Mohammed bin Nayef, but inflicted only minor injuries. In October, a plot to send two parcel bombs from Yemen to the US was foiled after a tip off from Saudi Arabia. In March, the kingdom arrested 113 al-Qaeda figures, including alleged suicide bombers who it said had been planning attacks on energy facilities in the world's top oil-exporting country.

E/T Lights™
Solutions For First Responders

4-in-one lights
IR

Southwest Synergistic Solutions

E/T Lights™
Solutions For First Responders
IR

Attachment Locations (Loops)

Notched Tip
Designed to aid the user in locating the switch even under blind conditions.

Recessed Switch
The switch is located inside the body of the **E/T Lights™**. This helps prevent the selected condition from being changed inadvertantly. The user needs to press into the body of the light.

Silicon Housing
Used because of its wide temperature usability. The light has been used at –20°F for an extended period and did not freeze or get brittle.

Interference Fit Seal
Water resistant, pressure tested to 66 ft.

End cap Options
Choose from the flat bottomed end cap, loop and cap or custom end cap for electronics, storage, flotation, etc....

Lithium Battery
Provide longer light function. Our tests show that the red LED will remain on for a minimum of 72 hrs... Blue LED will stay on a minimum of 144 hrs... Green LED will stay on a minimum of 192 hrs. (From 144 hours up to 240 hours when set to blinking) Battery shelf life is 4+ years.

Easy Battery Removal
Designed to be re-usable/ disposable and economical.

Software Features/Board Features
The sequence for Version 1 is Press once - Infra-red, press twice blinking Infra-red (60/minute), press a third time- Red, press a fourth time - Green, press a fifth time - Blue, and press a sixth time - light turns Off and sequence restarts.
Emergency Off Feature - If at any time the user presses the switch for over 2 seconds the light will turn off and the sequence will restart.
Selection Memory - The **E/T Lights™** has a selection memory. It is very important that the selected condition not change or if the lights were tossed or banged around that the selection remained on. All electronics when thrown around may lose power for milliseconds and subsequently turn off because of interruption of power due to shock. We have solved this issue by building the **E/T Lights™** with a memory. So even if the lights are thrown and battery contact is lost. The lights will turn back on to the last selection selected.
Reprogrammable chip - The new boards have programming pads. This was done to customize the color sequence and pulse rates to any sequence or rate desired. You can have the same light wavelength flashing at different rates within each different selection. This also facilitates accommodating special requests for customized operations and inclusion of specific operating sensors.

Lock Feature
Versions 3 and 4 of the **E/T Lights™** have the lock feature activated. This feature locks in a color selection after it has been left on for over 3 seconds, preventing the patients from re-prioritizing themselves.

LED's
Used because of their low power consumption and long life. LED's have 100,000 to 200,000 hours of use.

Infra-red LED may be replaced with other colored LED.

Colored LED's may be replaced with different wavelength infrared LED's or different intensity infrared LED's.

All comments provided by Special Operations Personnel

"Patient Triage Light (Now combat proven by SOF Forces)."

"Just got package in. Played with the light and I am happy. It is reliable, and the battery is easily removed."

"Have now been used in a mass casualty mission in combat and performed admirably."

"Combat proven."

"I took the triage light into -20°F the other day and it worked well. The outer shell did not get brittle as I suspected, and the lights worked whenever I tried them for over a one hour time-frame."

"I was able to toggle the light while wearing blue glove liners and OR wind stopper outer gloves."

Juan Cienfuegos
Owner / Inventor

www.TriageLights.com

Southwest Synergistic Solutions
215 N. Center Road, #701
San Antonio, TX 78202
(956) 645-5265
info@triagelights.com

(956) 645-5265

Patents & Patents Pending
7326179, D576323, 7510527, 7674227

www.TriageLights.com

E/T Lights™
Solutions For First Responders
4-in-one lights IR
Southwest Synergistic Solutions

E/T Lights™ are a newly patented technology available for the first time to nonmilitary personnel. Developed in conjunction with United States Special Operating Forces the **E/T Lights™** are a new triage device and method for use that offers a faster, easier, and more effective way of marking and prioritizing individuals for medical care at the scenes of various emergency situations such as natural disasters, plane crashes, train and automobile accidents and other mass-casualty incidents. **E/T Lights™** are easy to place and provide accurate information relating to a victims degree of injury.

This improved triage tagging system is easy to see in the dark, underwater and in buried situations,where traditional tags have been proven as inadequate. Complete darkness and underwater settings prevent the cards from being read and from being clearly seen from a distance.

Further, triage tagging is often performed under the most harried of conditions as well as increasing and heightened when smoke, dust and poor weather conditions obscure the ability to determine the triage status and to manually corresponding fill out a comment card too. The **E/T Lights™** provide illuminated signals that visually provide the triage status of an injured person/animal at a distance and in low visibility settings such as in the rain, fog, snow, in areas of dense undergrowth and multiple other scenarios.

E/T Lights™ are "Combat proven' and have been used in actual mass casualty situations by U.S. Air Force medics.

In addition to being used as triage tags, **E/T Lights™** can take the place of traditional emergency light sources such as chemical light sticks while offering numerous benefits over and above what the chemical light sticks offer.

	E/T Light Life	Chemical Light (CL) Stick Life	Qty utilized
Red	72+ Hours	2 Hours**	36 CL's to 1 E/T Light
Green	192+ Hours	5 Hours**	38 CL's to 1 E/T Light
Blue	144+ Hours	2 Hours**	72 CL's to 1 E/T Light
Blinking Red	168+ Hours	Not Available	N/A
Blinking Green	200+ Hours	Not Available	N/A
Blinking Blue	240+ Hours	Not Available	N/A

** Note- Packaging of the chemical light sticks stated that the products had up to 6 hours of use. My personal test results were that the red and blue chemical light sticks were usable for up to 2 hours. The green chemical light sticks were usable for 5 hours.

- Potential cost savings of over 90%
- Reduction in storage space
- Reduction in logistic and storage costs
- Reduction in weight and volume carried by First Responders
- Reduction in landfill usage
- E/T Light's are reusable and have replaceable silicon nose cones and end caps
- Improves response times of support personnel.

First responders can also use the **E/T Lights™** for distinguishing between contaminated patients (Blinking color) and non-contaminated patients (Solid color), route marking, traffic control, perimeter marking, low light illumination and more.

These lights could be dispersed to a population that did not evacuate a disaster area prior to the occurrence. Using Hurricane Katrina as an example those who chose not to evacuate could be given **E/T Lights™** and instructed to wear them during the disaster on a constant on color selection (red-children, green-woman, blue-men). Once the disaster has passed the user would only need to press the **E/T Lights™** switch once in order to change the color to blinking, indicating their survival. This would turn the night into a friend for first responders. The night would turn into clusters of lights visible from the air that would tell first responders the numbers, general condition, makeup and location of anyone who remained in the disaster area. Specific programming could be set which would let the rescuers know if the victim is alive, injured, etc... In addition, disaster survivors could use the **E/T Lights™** for night illumination and general safety and survival.

The method, design and devices themselves are patent protected. To date patents 7326179, D576323, 7510527, & 7674227 have been issued. Many additional patents are still pending.

Southwest Synergistic Solutions is a minority owned small business (MBE) and is looking forward to serving our military and first responder community. Please email us today at **info@triagelights.com.**

CBRNE-TERRORISM Newsletter

Δελτίο ΧΒΡΠΕ-ΤΡΟΜΟΚΡΑΤΙΑΣ

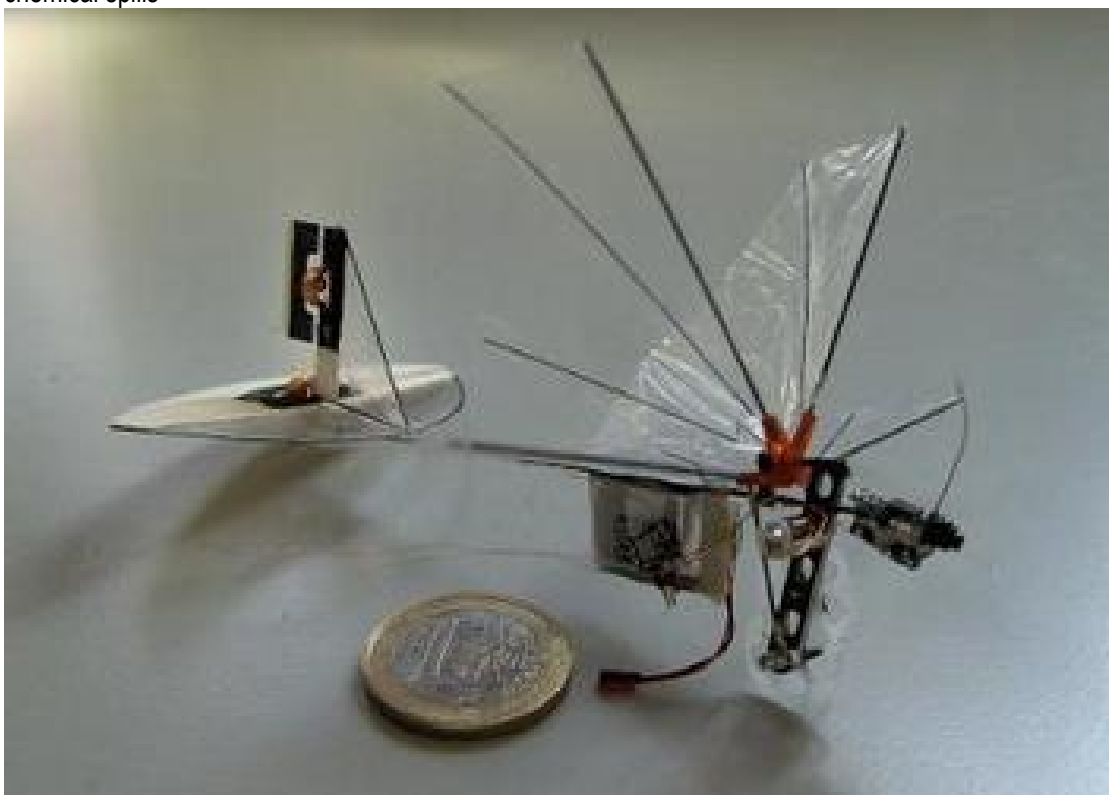
Volume 5 - 2010

CHEM –News

Insect-size air vehicles to explore, monitor hazardous environments

Source:http://homelandsecuritynewswire.com/insect-size-air-vehicles-explore-monitor-hazardous-environments

High-performance micro air vehicles (MAVs) are on track to evolve into robotic, insect-scale devices for monitoring and exploration of hazardous environments, such as collapsed structures, caves and chemical spills



This MAV weighs 3 grams and measures 10 centimeters // Source: sciencedaily.com

\A U.S. Air Force Office of Scientific Research-sponsored researcher, Dr. Robert Wood of Harvard University, is leading the way in what could become the next phase of high-performance micro air vehicles (MAVs) for the Air Force. His basic research is on track to evolve into robotic, insect-scale devices for monitoring and exploration of hazardous environments, such as collapsed structures, caves, and chemical spills. "We are developing a suite of capabilities which we hope will lead to MAVs that exceed the capabilities of existing small aircraft. The level of autonomy and mobility we seek has not been achieved before using robotic devices on the scale of insects," said Wood. Wood and his research team are trying to understand how wing design can impact performance for an insect-size, flapping-wing vehicle. Their insights will also influence how such agile devices are built, powered and controlled. "A big emphasis of our AFOSR program is the experimental side of the work," said Wood. "We have unique capabilities to create, flap and visualize wings at the scales and frequencies of actual insects." Maria Callier reports that the researchers are constructing wings and moving them at high frequencies recreating trajectories similar to those of an insect. They are also able to measure multiple force components, and they can observe fluid flow around the wings flapping at more than 100 times per second. Performing experiments at such a small scale presents significant engineering challenges beyond the study of the structure-function relationships for the wings. "Our answer to the engineering challenges for these experiments and vehicles is a unique fabrication technique we have developed for creating wings, actuators, thorax and airframe at the scale of actual insects and evaluating them in fluid conditions appropriate for their scale," he said. They are also performing high-speed stereoscopic motion tracking, force measurements and flow visualization; the combination of which allows for a unique perspective on what is going on with these complex systems.

WE REDUCED THE SIZE. NOT THE PROTECTION.

AVON PROTECTION

1 888 AVON 440

www.avon-protection.com

NEW

CHEMPRO 100i

Handheld Chemical Detector

ChemPro100i is a handheld vapor detector for classification of Chemical Warfare Agents (CWAs) and Toxic Industrial Chemicals (TICs). The ChemPro100i adds 6 more sensors to increase the number of chemicals that it can detect and to decrease the potential for false alarms.

No maintenance costs for 5 years!

- Industry leading sensitivity
- Stores well - no regular exercise needed
- Non-threatening design
- Easy-to-use

* Contact Us for details on our standard 5-years Guaranteed Cost of Ownership (GCO) program

Environics

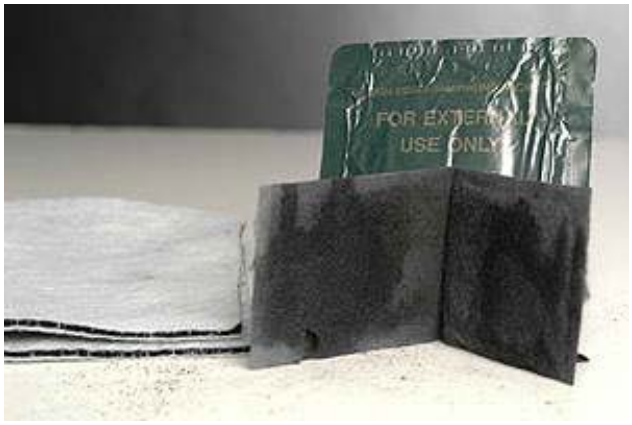
Environics Oy
Graanintie 5
P.O. Box 349
FI-50101 Mikkeli, Finland
tel. +358 201 430 430
fax. +358 201 430 440
www.environics.fi
sales@environics.fi

Environics USA Inc.
1308 Continental Drive, Suite J
Abingdon, MD 21009
USA
tel. +1 (410) 612-1250
fax. +1 (410) 612-1251
www.EnvironicsUSA.com
sales@EnvironicsUSA.com

New chemical contamination wipe developed

Source: http://homelandsecuritynewswire.com/new-chemical-contamination-wipe-developed

A newly developed decontamination wipe (Fibertect™) designed by researchers at the Institute of Environmental and Human Health (TIEHH) at Texas Tech University has proven itself in cleaning up chemical warfare agents and toxic chemicals. The evaluation of the nonwoven dry wipe product, called Fibertect, was performed as part of a study by the Lawrence Livermore National Laboratory using mustard gas and other toxic chemicals. Researchers found that the Texas Tech-created product out-performed thirty different decontamination materials, including materials currently used in military decontamination kits. The results are published 3 December in the American Chemical Society's Industrial & Engineering Chemistry Research (title: "Next Generation Non-particulate Dry Nonwoven Pad for Chemical Warfare Agent Decontamination"). TIEHH says it has developed the product to meet the needs of today's military as expressed in a 2004 report to Congress published by the U.S. Department of Defense. In this and the March 2005 annual report, the department called for products to decontaminate people and military equipment as part of the Pentagon's Decontamination Science and Technology Modernization Strategy. "These test results are another affirmation that Texas Tech researchers, particularly those working at The Institute of Environmental and Human Health, are some of the best in the world," said Kent Hance, chancellor of Texas Tech University System. "The new products developed from their research will help safeguard our troops against chemical hazards and assist emergency crews in cleanups from toxic accidents and environmental disasters." Seshadri Ramkumar supervises the Nonwovens and Advanced Materials Laboratory at Texas Tech. He and other scientists with the Admiral Elmo R. Zumwalt Jr. National Program for Countermeasures to Biological and Chemical Threats have worked to create a product that will be an asset to military and homeland security efforts in the post-9/11 environment. The program is funded by the U.S. Department of Defense. "Needlepunch nonwoven technology has been used to develop this flexible, absorbent and adsorbent material that can be used not only as a decontamination wipe, but also as the liner of protective suits, filters and masks," said Ramkumar, who served as the lead author for the study. "The material is flexible, doesn't contain loose particles and is capable of cleaning intricate parts of everything from the human body to the control panel of a fighter jet." The product features an activated carbon core sandwiched between an absorbent layer on the top and the bottom, he said. "Dr. Ramkumar and others have worked hard to make us a leading research institution by developing this innovative and necessary product," said Ron Kendall, director of TIEHH and a co-author for the report. "This new fabric will help protect our troops on the battlefield as well as Americans here at home against biological and chemical warfare and terrorism threats." The technology has been licensed by Texas Tech's Office of Technology Commercialization to Waco-based Hobbs Bonded Fibers. The company is organizing a global marketing team to expedite the commercialization of Fibertect. The initial member of the team is

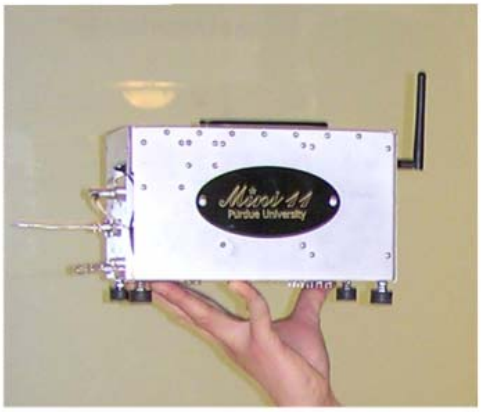


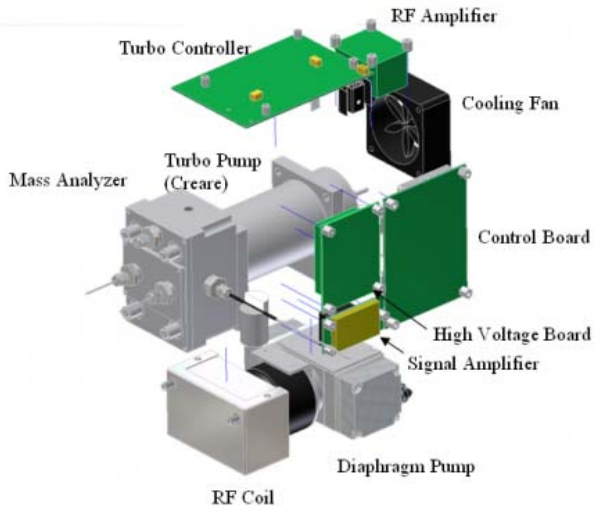
The Bellator Group, which has a successful history of commercializing products into the military sector. “The exciting news here is that the federal government saw a need for this product, and Texas Tech came up with a product to meet that need,” said Carey Hobbs, president of Hobbs Bonded Fibers. “Now, the federal government is going to see an actual return on its money. You can buy this product today, and we’re already manufacturing and exhibiting it to people in the marketplace.”

Small hand-held detector for security, health threats

Source: http://homelandsecuritynewswire.com/small-hand-held-detector-security-health-threats

Researchers develop the world's smallest detection system: The size of a shoe box, the complete mass spectrometer identifies tiny amounts of chemicals in the environment. Researchers in Indiana are describing development of the world’s smallest complete mass spectrometer (MS), a miniature version of a standard lab device — some of which would fill a living room — to identify tiny amounts of





chemicals in the environment. The researchers say that the hand-held MS, about the size of a shoe box, could speed the detection of bioterrorism agents, hidden explosives, and other threats. Their study is scheduled for the current issue of ACS’ Analytical Chemistry. R. Graham Cooks, Zheng Ouyang, and colleagues note that scientists have developed several different versions of portable mass spectrometers over the past few decades. The problem was that the instruments’ large size, weight, and inability to analyze a wide variety of different target molecules have limited their practical use. The scientists responded to the need for a small but sensitive MS by developing the Mini 11. About the size of a small shoe box, it weighs only 9 pounds (half the weight of other portable MSs), and can be operated by remote control. Laboratory tests showed that the Mini 11 could accurately identify the chemical composition of three commonly used commercial drugs within just one minute using tandem mass spectrometry. Unlike previous portable mass specs, this new instrument is capable of analyzing a wider variety of molecules, including large proteins, the scientists say.

Low-Dose Exposure To Chemical Warfare Agent May Result In Long-Term Heart Damage

Source: http://www.medicalnewstoday.com/articles/204600.php

New research found that the pattern of heart dysfunction with sarin exposure in mice resembles that seen in humans. Sarin is a chemical warfare agent belonging to class of compounds called organophosphates - the basis for insecticides, herbicides and nerve agents. As an inhibitor of the nervous system enzyme acetylcholinesterase, sarin can cause convulsions, stoppage of breathing and death. Aiming to determine the delayed cardiac effects of sarin, researchers studied mice injected with sarin - at doses too low to produce visible symptoms - 10 weeks after the exposure. "The two-month period was used to simulate the late onset effect of sarin/nerve agents in gulf war veterans," said

Mariana Morris, director of the research program. "There are suggestions that gulf war illness; in which symptoms are long-lasting, may be related to exposure to low-dose chemical warfare agents."

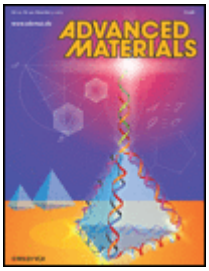
- Cardiac damage detected in sarin-exposed mice at 10 weeks, but not earlier, included:
- Left ventricular dilation, meaning the heart's left ventricle is larger.
- Prolonged ventricular repolarization, an electrical conduction anomaly that could lead to heart rhythm abnormalities.
- Reduction in contractility, the extent of ventricular contraction and hence the amount of blood pumped from the ventricle when it contracts.

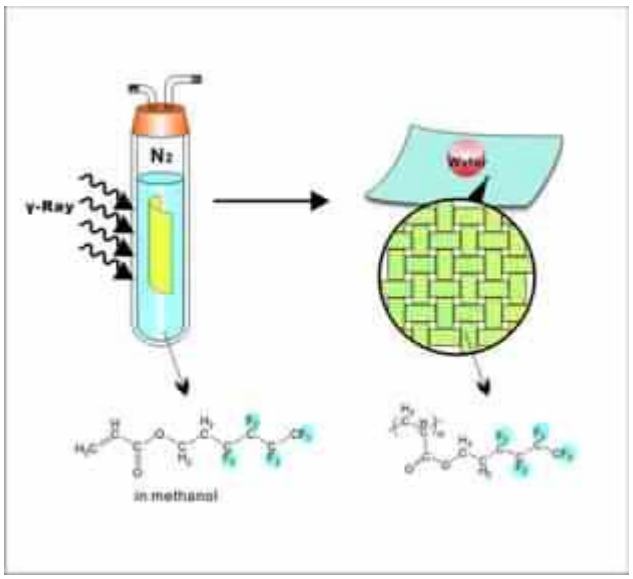
"These results have implications for the military in times of conflict and for civilian populations in cases of environmental or occupational exposure," Morris said.

New cotton fabric stays waterproof through 250 washes

Source: http://homelandsecuritynewswire.com/new-cotton-fabric-stays-waterproof-through-250-washes

Most waterproofed fabrics lose their super-hydrophobic properties after only one or two washes, and they become uncomfortable to wear because they do not allow air flow through the material. In contrast, the new fabric, which according to the researchers looks almost identical to ordinary cotton fabric, is completely impermeable and breathable, and retains its properties even after being laundered many times. Scientists in Shanghai in China, have developed a waterproof cotton fabric that remains waterproof after going through a domestic wash at least 250 times. Most waterproofed fabrics lose their super-hydrophobic properties after only one or two washes, and they become uncomfortable to wear because they do not allow air flow through the material. In contrast, the new fabric, which according to the researchers looks almost identical to ordinary cotton fabric, is completely impermeable and breathable, and retains its properties even after being laundered many times. RSC reports that the new fabric was made by grafting a commercially available fluorinated acrylate monomer (1H,1H,2H,2H-nonafluorohexyl-1-acrylate) onto bundles of cotton fibers which were irradiated with gamma rays to induce polymerization. In this process the cotton forms covalent bonds with the polymer, and it is not simply coated. The polymer prevents water adhering to the cotton surface and the water instead forms droplets that roll off the fabric, taking any dust or surface dirt with them. Researcher Jingye Li, from the Shanghai Institute of Applied Physics at the Chinese Academy of Sciences, said grafting the polymer onto the bundles of fibers meant the small holes between the cotton bundles are retained in the fabric. This enables the material to remain breathable and comfortable to wear even after multiple washings. He also said its super-hydrophobic nature made the fabric feel smoother than normal cotton. Li and colleagues tested the fabric by subjecting it to fifty accelerated launderings in a domestic washing machine with different detergents, and with fifty stainless steel balls to simulate the repeated washing. The tests showed the fabric retained its super-hydrophobic properties even after the equivalent of 250 domestic or commercial washes at 40ºC.





CRISTANINI CBRN

DECONTAMINATION SYSTEMS

LIGHT EXPEDITIONARY
CBRN RAPID DECON/DETOX TRAILER
for SPECIAL OPERATIONS

L.E.D.T.

FD 400

AS009
CONFORM TO THE QUALITY
SYSTEM STANDARD AQAP 2110
and ISO 9001:2008

RAPID DEPLOYABILITY

MISSION:
DECON & DETOX OF
- Personnel
- Vehicles
- Equipment

ADDITIONAL CAPABILITIES:
- Sensitive Equipment
- Terrain
- Sanitization and degassing

We have been doing for years things others have yet to do

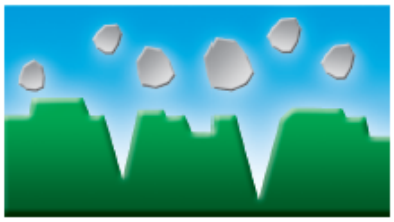
MOVE FORWARD WITH US!

1972 since

CRISTANINI
37010 RIVOLI - VERONA - ITALY - Tel. +39-045-6269400 - Fax +39-045-6269411
cristanini@cristanini.it - **www.cristanini.com**

FAMILY OF DECONTAMINANTS

Contaminating agent on surface



Particles decomposed and neutralized by detoxificant BX 24

BX 24 (powder) Code 240243 - **NATO Standard Number 6810-15-149-4789**

Decontamination/detoxification product for vehicles and different types of materials from CBRN agents.

BX 24 is absolutely the most efficient and the most interesting non-aggressive detoxifying agent available today. It is also tested for preventive Decon/Detox (Sanitization) of materials and vehicles in redeployment from mil operations.

CBRN

BX 29 (liquid)

Code 240240 - **NATO Standard Number 6850-15-157-8945**
Decontaminant product for persons.

PERSONNEL DECONTAMINATION

BX 30 (powder)

Code 240256
Training version of BX 24

CBRN TRAINING

BX 40 (liquid)

Code 240257 - **NATO Standard Number 6850-15-157-8946**
Decontaminant product for CBRN decontamination of aircraft, helicopters, etc.

CBRN

SX 34 (aerosol)

Code 240230 - **NATO Standard Number 6850-15-203-0546**
CBRN decontaminant product for **sensitive equipment.**

SENSITIVE EQUIPMENT

BX 60 (liquid)

Code 240350

Biological decontamination product for apparatus:

1) CFH (electric applicator for chemical products - aerosol),

2) PRT (autonomous portable fogger system) and SANIJET.

ALL CRISTANINI PRODUCTS HAVE A LOW ENVIRONMENTAL IMPACT.
THE COMPLETE TESTS BOOK IS AVAILABLE ON REQUEST TO CRISTANINI SPA

CBRNE-TERRORISM Newsletter

Δελτίο ΧΒΡΠΕ-ΤΡΟΜΟΚΡΑΤΙΑΣ

Volume 5 - 2010

BIO –News

France: Anthrax (human, livestock: 1999-2009)

Source: http://www.promedmail.org

Between 1999 and 2009, 74 outbreaks of animal anthrax, primarily in cattle, were confirmed by isolation of _Bacillus anthracis_ in 14 French districts (annual mean: 7 outbreaks). All cases occurred in areas where outbreaks had been reported previously. While the annual number of outbreaks remained low and stable from 1999 to 2007 (0-6 outbreaks/year), 19 utbreaks were recorded in 2008 (of which 17 clustered outbreaks in Doubs) and 22 in 2009 (of which 17 clustered outbreaks in Savoie). All cases occurred in cattle, except for one horse case in 2001, while goat and horse cases occurred in 2009. The relatively high number of outbreaks observed in Savoie and in Doubs is not fully explained, but certainly related in part to the local anthrax history and to weather conditions during summer.

Outbreaks by year

1999 (5), 2000 (5), 2001 (3), 2002 (0), 2003 (6), 2004 (3), 2005 (2), 2006 (3), 2007 (6), 2008 (19), 2009 (22).

Farms in 2009

In 2009, a total of 24 farms were suspected (of anthrax) in 8 departments. These suspicions were confirmed in 5 departments. (A department is similar to a state in the USA) The outbreaks occurred in areas already affected by anthrax (fievre carboneuse) in the past. The 1st 2 outbreaks in June-July 2009 involved 2 cattle herds, respectively, in the Puy de Dome (one dead animal) and Cote-d'Or (3 dead). The 3rd outbreak, which occurred in July 2009 in Aveyron, was in a holding of mixed cattle and goats and began with the death of a heifer in a field with a water point. The calf was necropsied in the pasture without special protection as it was thought to have been killed by lightning. The body was

moved using a tractor. A week later, 4 more corpses were discovered over 3 days in this field, and 2 had been consumed by scavengers.

A 2nd necropsy was done, this time with some caution, and anthrax diagnosed. A total of 19 goats and 5 heifers died in this breeding establishment. The tractor used to move the corpses had been used in transporting feed to the goat barn and specifically their common feed trough. This undoubtedly contributed to the extension of infection in the goat population. During this outbreak, preventive

chemotherapy was put in place for the employees of the establishment and the family (of the) the breeder and veterinarians who performed the autopsies. The operation to vaccinate the cattle was also rapidly implemented.

The following farms, where a significant episode occurred, are in Savoie in the township of La Rochette (Valee des Huiles). In less than a month (26 Jul to 15 Aug 2009), 17 outbreaks were confirmed. 15 cattle herds and 2 horses were infected, which led to the deaths of 32 head of cattle and 2 horses located in 11 nearby municipalities. Seven other herds experienced deaths of cattle over the period but were not confirmed as anthrax. A 3rd horse which showed clinical signs of anthrax was treated. The 3 horses had been in contact with each other and were epidemiologically linked to at least one cattle farm. Cases of anthrax in horses are usually rare in France. A single outbreak was recorded in Mayenne in 2001, where a horse had died of anthrax. Previous episodes of confirmed anthrax in Savoy had been reported in Bauges in 2000 and in the same area of Valee des Huiles in 1997.

Two outbreaks were also confirmed in Isere in August 2009. They involved 2 herds with the same common boundary with 2 already infected communes in Savoy. Vaccination of livestock in Savoie and Isere was very quickly established in 16 Communes. No human cases have been reported, but preventative treatment was administered to exposed people. Control for public health and milk safety was put in place on the infected farms following an assessment by the competent authorities (Direction General of Health, Direction General of Food, National Reference Center, French Food Safety Agency). Suspicious strains were solated by departmental veterinary laboratories (LVD) and/or the NRL mainly from cattle (23), but also goats (1) and horses (2), and were confirmed as _B. anthracis_ by specific PCR and were susceptible to penicillin, facilitating a preventive antibiotic for people exposed. Molecular typing by MLVA [multi-locus VNTR analysis] analysis using 10 VNTR (variable number tandem repeat) loci was performed on all strains. The profiles of recent strains and those isolated since 1982, in the same departments, were compared. The same VNTR genotype was found in each department, regardless of place and date of isolation. For all households of Savoy, the strains showed the same genotype (10 identical loci) suggesting a common origin (for example epidemiologically linked to outbreaks, contaminated land, same genotype). The ongoing review of other VNTR loci is likely to test this hypothesis.

The question that remains unanswered, after successive episodes in Doubs (French Department on Swiss border) in 2008 and Savoy in 2009, concerns the mechanisms that led to he emergence of a significant number of affected farms in a given location over a short period in some regions, while in others -- fortunately in most instances -- only isolated sporadic cases were seen. In historically contaminated areas and in favourable hydro-geological conditions, along with delayed diagnosis, the movements of animals, people or materials, and weather conditions all certainly contribute each in their own way to the occurrence of multiple episodes of disease over a short period.

Anthrax in man: review of cases and persons exposed and treated during recent animal outbreaks in France, 2002-2008

Anthrax has been subject to compulsory notification since 2002. Since that time, 4 cases of human anthrax have been identified. In 2003, a case of cutaneous anthrax was diagnosed in a patient exposed while butchering an infected sheep in an enzootic area. In December 2008, 3 cases of cutaneous anthrax were identified in men who had taken part in the evisceration and butchering of a cow with anthrax. The investigation identified 11 people in contact with that cow who were possibly infected and consequently received antimicrobial prophylaxis. A risk assessment was carried out concerning the consumption of meat from cows gutted with the same knives previously used to gut the infected cow and concerning the consumption of meals handed by one of the cases. [1] They were diagnosed by PCR of skin biopsies from the lesions. All responded favourably to treatment and without complications. [2]

References:
1. Mailles A, Alauzet C, Mock M, Garin-Bastuji B, Veran Y. Cas groupes de charbon cutane humain en Moselle - Decembre 2008. Saint-Maurice: Institut de veille sanitaire, fevrier 2010 ;4 p.
2. Cinquetti G, Banal F, Dupuy AL, Girault PY, Couderc A, Guyot P, et al. Three related cases of cutaneous anthrax in France: clinical and laboratory aspects. Medicine (Baltimore). 2009;88(6):371-5.

Question: How Quickly Could a Single Supervirus Spread to Every Single Person on Earth?

Source:http://www.popsci.com/science/article/2010-09/how-quickly-could-single-supervirus-spread-every-single-person-earth

Germs on a Plane Air travel can rapidly spread viruses across continents. Treating patients before landing is critical. Getty Images

If it's a particularly contagious virus, it would spread across the planet in a year. "If it starts in New York, it's going to be in London certainly within a week," says Ira Longini, a biostatistician at the University of Washington and the Fred Hutchinson Cancer Center in Seattle who uses computer models to analyze how viruses globe-trot. "And from there, it will quickly travel to the rest of North America and Europe." For Longini's computer forecasts to become reality, though, certain conditions would need to be met. First, it should be a strain of influenza. As anyone who has suffered through a bout of flu knows, it affects the respiratory tract, so sneezing and coughing make it easy to infect anyone within a three-foot radius. The virus must originate in a major city with plenty of airport traffic, to ensure that it jumps continents. Arising during the winter would speed its spread too, because the "normal" colds or flus people typically catch at that time of year could throw health officials off the trail of the real megabug, says Andrew Pekosz, a virologist and immunologist at Johns Hopkins University. The idea seems to freak him out. "With everybody expressing similar symptoms, we'd end up chasing, chasing, chasing, but always being a few steps behind, never really able to interrupt the spread."

A superbug could spread to every single person on Earth in one year

Source:http://homelandsecuritynewswire.com/superbug-could-spread-every-single-person-earth-one-year

If certain conditions obtain, a particularly contagious virus would spread across the planet and infect every single person on Earth in one year; the conditions: it must be a strain of influenza, originate in a major city, and arise during the winter.

How quickly could a single supervirus spread to every single person on Earth? If it is a particularly contagious virus, it would spread across the planet in a year. "If it starts in New York, it's going to be in London certainly within a week," says Ira Longini, a biostatistician at the University of Washington and the Fred Hutchinson Cancer Center in Seattle who uses computer models to analyze how viruses globe-trot. "And from there, it will quickly travel to the rest of North America and Europe." Rosa Pastore writesthat for Longini's computer forecasts to become reality, though, certain conditions would need to be met. First, it should be a strain of influenza. As anyone who has suffered through a bout of flu knows, it affects the respiratory tract, so sneezing and coughing make it easy to infect anyone within a 3-foot radius. The virus must originate in a major city with plenty of airport traffic, to ensure that it jumps continents. Arising during the winter would speed its spread too, because the "normal" colds or flues people typically catch at that time of year could throw health officials off the trail of the real megabug, says Andrew Pekosz, a virologist and immunologist at Johns Hopkins University. The idea worries him out. "With everybody expressing similar symptoms, we'd end up chasing, chasing, chasing, but always being a few steps behind, never really able to interrupt the spread."

Scientists closer to a safer anthrax vaccine

Source: http://homelandsecuritynewswire.com/scientists-closer-safer-anthrax-vaccine

The currently available, 40-year-old anthrax vaccine, can prevent disease, but it has significant drawbacks: Immunity is temporary, and five injections over the course of eighteen months are needed to sustain it; one in five vaccine recipients develop redness, swelling, or pain at the injection site, and a small number develop severe allergic reactions; researchers offer a better vaccine

Researchers at Albert Einstein College of Medicine of Yeshiva University have identified two small protein fragments that could be developed into an anthrax vaccine that may cause fewer side effects than the current vaccine. The research is significant because anthrax is considered a major bioterrorism threat. The current anthrax vaccine is intended mainly for members of the armed forces serving in areas considered high risk and for individuals involved in homeland biosecurity. "Our research was motivated by the fact that the current anthrax vaccine has significant limitations and there is great need for a better one," says lead author Nareen Abboud, Ph.D., an Einstein postdoctoral fellow and lead author of the study, which appears in the current issue of the Journal of Biological Chemistry. The study's senior author is Arturo Casadevall, M.D., Ph.D., Leo and Julia Forchheimer Professor and chairman of microbiology & immunology. Anthrax, a disease caused by the bacterial species Bacillus anthracis, occurs when anthrax spores (the microbe's dormant stage) are inhaled, ingested, or enter the body through an open wound. Anthrax is a common disease among grazing animals such as cows, goats,

and sheep but can also result from bioterrorism. Eighty to 90 percent of people infected through inhalation will die if not treated, according to the U.S. Department of Health and Human Services. In 2001, five people died after inhaling anthrax spores contained in envelopes mailed to U.S. lawmakers and media personnel. Typical treatment post-exposure includes the antibiotics ciprofloxacin, doxycycline and penicillin. Anthrax results in part from toxic proteins, or toxins, that the multiplying bacteria secrete. The current anthrax vaccine employs one of these proteins, which elicits protective antibodies when injected into people. While this 40-year-old vaccine can prevent disease, it has significant drawbacks. Immunity is temporary, and five injections over the course of eighteen months are needed to sustain it. One in five vaccine recipients develop redness, swelling or pain at the injection site, and a small number develop severe allergic reactions. A recent article in the journal Clinical Infectious Diseases states that nearly seven million doses of the anthrax vaccine were administered to more than 1.8 million Americans between 1998 and 2008. In their study, the Einstein scientists focused on the protein toxin used in the current vaccine, looking for the smallest protein sections (known as peptides) that could trigger the production of protective antibodies when injected into animals.

The researchers injected the current vaccine into mice and recovered six different "pure" strains of antibodies known as monoclonal antibodies. They then mixed each type of antibody with the 145 peptides formed by chopping up the vaccine protein. The researchers looked for peptides that were "recognized by" (became bound to) an antibody - an indication that those particular peptides might themselves be able to stimulate the production of protective antibodies on their own. Ultimately, the researchers found that two of the 145 peptides fit the bill: Each peptide elicited antibodies when injected into mice, and these antibodies protected macrophages from death that would normally have occurred when the macrophages were exposed to anthrax toxin (macrophages are protective white blood cells involved in the body's immune response to foreign invaders). The next step in the Einstein research will be to inject the peptides into an animal model to see if the peptides can protect against anthrax infection. "An ideal anthrax vaccine contains only the proteins needed to provide protection against disease, and none of the extraneous protein material that triggers the adverse reactions caused by the current vaccine," says Dr. Abboud. "We're hopeful that the two peptides that we have identified in this study can offer these benefits." The simple structure of these peptides — one is only five amino acids in length, the other six — means it should be easy to synthesize the peptides and inexpensive to produce a vaccine containing them, Dr. Abboud notes. Einstein will be applying for a patent for the use of the two peptides in an anthrax vaccine.

A new dual vaccine protects against both smallpox and anthrax

Source:http://homelandsecuritynewswire.com/new-dual-vaccine-protects-against-both-smallpox-and-anthrax

A new protective vaccine against both smallpox and anthrax, two agents of bioterrorism, shows promise in animal models; the new vaccine more quickly elicited immunity and was more effective than the licensed anthrax vaccine, BioThrax, in protecting mice and rabbits against anthrax

Scientists have developed and tested a new protective vaccine against smallpox and anthrax, two agents of bioterrorism, in animal models. Liyanage P. Perera, Ph.D., NCI, and colleagues made the enhanced dual vaccine by inserting the genes for protective parts of anthrax and the immune-boosting chemical, interleukin-15, into the backbone of the licensed smallpox vaccine, ACAM2000. They found their new vaccine more quickly elicited immunity and was more effective than the licensed anthrax vaccine, BioThrax, in protecting mice and rabbits against anthrax — it was also safer in immune deficient mice and more effective than the licensed smallpox vaccine in protecting mice and monkeys. The study appeared online in PNAS on 4 October 2010. Current licensed vaccines for smallpox and anthrax have certain negative side effects, require multiple doses, or have certain storage and delivery problems. For example, ACAM2000 may cause encephalitis, cardiac inflammation, and is also contraindicated for people with weakened immune systems or those with eczema; BioThrax has a short

shelf-life and requires multiple boosters to confer adequate protection. Added to the benefit of having one vaccine that effectively protects against two deadly pathogens this new vaccine can be freeze-dried, stockpiled, and rapidly delivered in the event of a bioterror attack involving smallpox or anthrax. Plans are underway for further safety and efficacy testing of this new vaccine in non-human primates with the view of advancing this vaccine for testing in humans.

Virus related to smallpox rising sharply in Africa

Source: http://homelandsecuritynewswire.com/virus-related-smallpox-rising-sharply-africa

Thirty years after the eradication of smallpox, and the end of the mass smallpox vaccination campaign, rates of a related virus known as human monkeypox have increased dramatically in the rural Democratic Republic of Congo, with sporadic outbreaks in other African nations and even the United States

Human monkeypox cases rise in Africa // Source: healthspablog.org

In the winter of 1979, the world celebrated the end of smallpox, a highly contagious and often fatal viral infection estimated to have caused between 300 and 500 million deaths during the twentieth century. The virus was eradicated through an aggressive worldwide vaccination campaign, which itself ended in 1980. With no virus, there was no longer a need for a vaccine. Now, researchers at UCLA say the elimination of the smallpox vaccine has allowed a related virus to thrive. In the current online edition of Proceedings of the National Academy of Science, Anne Rimoin, an assistant professor of epidemiology at the UCLA School of Public Health, and colleagues report that thirty years after the mass smallpox vaccination campaign ceased, rates of a related virus known as human monkeypox have increased dramatically in the rural Democratic Republic of Congo, with sporadic outbreaks in other African nations and even the United States. Until 1980, Rimoin said, the smallpox vaccine provided cross-protective immunity against monkeypox, a "zoonotic orthopoxvirus," meaning it can be passed from animals to humans. Symptoms of monkeypox in humans include severe eruptions on the skin, fever, headaches, swollen lymph nodes, possible blindness and even death. There is no treatment. "All you can do is provide supportive care," Rimoin said. "There are no antibiotics. If you survive, the illness eventually runs its course." Once the smallpox vaccination program ended, new generations of people who were "vaccine naive" were exposed to the monkeypox virus the Democratic Republic of Congo over time, and the number of people who became infected gradually increased. But the increase went unnoticed because the nation has little or no health infrastructure and thus no way to monitor the spread of such diseases. This is why, until her recent report, Rimoin said, monkeypox was thought to be very rare. Her research shows, however, that it has become very common. Rimoin travels frequently to the

Democratic Republic of Congo, where she has established a research site to study and track cross-species transmission of the disease. For this work, Rimoin and her colleagues conducted a population-based surveillance in nine health zones in the central region of the country between 2006 and 2007, gathering epidemiologic data and biological samples obtained from suspected cases. They then compared the current, cumulative incidences of infection with data gathered in similar regions from 1981 to 1986. The results were startling, showing "a 20-fold increase in human monkeypox in the DRC since smallpox vaccinations were ended in 1980," Rimoin said. Rimoin noted that a monkeypox outbreak in the United States in 2003 had more to do with rodents than primates. That year, ninety-three people were infected throughout the Midwest, and the origin of the disease was later tracked to prairie dogs that had become infected and sold at a single pet store. "The name 'monkeypox' is really a misnomer," Rimoin said. "The disease was first identified in laboratory monkeys, thus providing it with its name. But in its natural state, it seems to infect squirrels and other rodents much more than primates." This is one of Rimoin's chief concerns — that the virus will spread into the animal population more broadly. "The point is, it doesn't take much for it to spread," she said. Because it is unlikely that smallpox vaccinations would be resumed, Rimoin is calling for improved health care education in the Democratic Republic of Congo and better disease surveillance. There is an urgent need to develop a strategy for reducing the risk of a wider spread of infections, she said.

U.S. faces growing biological threat

Source: http://homelandsecuritynewswire.com/us-faces-growing-biological-threat

An international treaty banned biological warfare in 1975, but it had no inspection and verification plan; hundreds of tons of anthrax bacteria and other pathogens were produced by the Soviet Union in violation of the treaty and only ordered destroyed in 1988 as the cold war ended; when U.S. scientists visited the anthrax burial sites, they found live spores had survived

The United States faces a growing biological threat from rogue nations and terrorists, a leading biologist told Huntsville's first biodefense symposium last week. Under the right circumstances, tens of thousands, even hundreds of thousands could die in a biological attack, said Dr. Jerry Jaax of Kansas State University. "There's a reason for all of this," Jaax said of the symposium. "There is a serious problem for us out there that is not going to go away," Jaax said in an interview with the Huntsville Times before delivering the symposium's keynote address. "We're not going to be able to say in 15 years, 'We've got it licked.'" The Huntsville Times reports that the two-day symposium hosted by the HudsonAlpha Institute for Biotechnology brought together local biotech and defense companies interested in joining the nation's biohazard response. Jaax is an associate vice president and researcher at Kansas State University, where the government plans to spend $700 million to relocate biohazard laboratories now housed on Plum Island off the coast of Long Island, New York. An international treaty banned biological warfare in 1975, Jaax said, but it had no inspection and verification plan. Hundreds of tons of anthrax bacteria and other pathogens were produced by the Soviet Union in violation of the treaty and only ordered destroyed in 1988 as the cold war ended. When U.S. scientists visited the anthrax burial sites, they found live spores had survived. "They had huge programs we were unable to detect," Jaax said. "And we certainly have indications that the bad guys, the non-state actors, are saying they would do this if they could figure out a way to do it, and some of these agents don't require very sophisticated biotechnology." A major threat today, Jaax said, is the spread of technology and knowledge from rogue national programs to terrorist groups. Biological threats are not limited to anthrax and other airborne pathogens, biodefense researchers say. Threats also exist to animals (foot and mouth disease), plants and water. "I think the government is taking it seriously," Jaax said. "There has been a proliferation of biocontainment facilities that have been sponsored by the federal government … There certainly is a sense that people seeing the valid threat information recognize what a problem it is," he said. "The question is, is it sustainable," Jaax said of the research. "Is it going to continue… in this (economic) environment?" Should Huntsville companies try to join the fight? "I think so," Jaax said. He acknowledged, though, that not everyone supports such research. "The alternative is to cross your fingers and do nothing," Jaax said, "and I think that's a big mistake."

Synthetic DNA makers alerted to bioterrorism threats

Source: http://homelandsecuritynewswire.com/synthetic-dna-makers-alerted-bioterrorism-threats

Scientists have been engineering genetic sequences for decades and commercial gene sequencing has been around for years -- but this year, researchers for the first time were able to design and produce cells that do not exist in nature without using pre-existing biological matter -- marking the latest evolution in the rapidly advancing field of synthetic biology; the developments could pave the way for advancements in medicine, energy, and agriculture, but also could put sensitive materials in the wrong hands; it will soon be possible to recreate bacterial pathogens like smallpox -- and even enhance these pathogens, making them more potent

To make it harder for bioterrorists to build dangerous viruses from scratch, guidelines for firms who supply “custom DNA” are being introduced in the United States. The United States and other countries restrict who can work with certain germs, but it might be possible to build some viruses from their genes. A number of firms supply DNA sequences to order. New Scientist reports that its 2005 investigation raised alarms when it found that only five out of twelve of these firms in North America and Europe always screened orders for sequences that might be used in bioweapons. The United States now wants firms to verify a customer’s identity and make sure they are not on a list of banned buyers. It also wants them to screen orders for sequences that are unique to Select Agents, a list of microbes the United States deems dangerous. Scientists, however, commenting on the draft rules earlier this year, fear that sequences from microbes other than Select Agents might also be dangerous. The U.S. Department of Health and Human Services says not enough is known about them to say which ones should arouse a firm’s suspicions. Other potential weaknesses include the fact that the rules are voluntary, and that much custom DNA is made outside the United States.

U.S. Seeks to Aid Africa in Securing Deadly Bioagents

Source: http://gsn.nti.org/gsn/nw_20101104_6903.php

A group of U.S. Defense Department arms control specialists is scheduled to travel to Africa next week to supporting regional efforts to secure deadly pathogens that could be turned into biological weapons, U.S. Senator Richard Lugar (R-Ind.) announced. "Deadly diseases like Ebola, Marburg, and anthrax are prevalent in Africa," Lugar said in released remarks. "These pathogens can be made into horrible weapons aimed at our troops, our friends and allies, and even the American public. This is a threat we cannot ignore." Lugar is set to accompany the Pentagon experts in their examinations of scientific facilities in Uganda and Kenya. The laboratories are involved in infectious disease diagnosis and research and in supporting pandemic-curbing treatments. "We’ve discovered through [the U.S. Cooperative Threat Reduction program] that Soviet scientists used pathogens from Africa to make biological weapons during the Cold War," the senator said in the release. "Those weapons are being destroyed. Now we have to secure their sources" . "Al-Qaeda and other terrorist groups are active in Africa, and it is imperative that deadly pathogens stored in labs there are secure," Lugar said. "Building cooperative programs with African countries are in our mutual security interests, and will also have the humanitarian effect of identifying and controlling new diseases that could quickly spread around the world." Defense Department specialists have identified vulnerabilities in safeguards at the Ugandan and Kenyan laboratories that should be addressed in light of their potential exploitation by terrorist organizations, the release said. Given Lugar's standing as a well-known arms control advocate, his involvement is anticipated to assist in convincing the Ugandan and Kenyan governments to cooperate with U.S. agencies such as the Centers for Disease Control in addressing security issues at the laboratories, according to the release (U.S. Senator Richard Lugar release, Nov. 4). Meanwhile, a science organization called on Nigerian politicians to this year approve legislation that would allow for domestic implementation of the Biological Weapons Convention, the African Press Agency reported. Nigeria signed the accord, which prohibits the development, production, stockpiling and use of weaponized disease agents such as anthrax, smallpox and plague, in 1972. The nation followed up with convention ratification the next year. International Council for Science regional panel for Africa Chairman Gabriel Ogunmola said yesterday the chief obstacle confronting the convention in

Nigeria is the absence of a law that would allow for its implementation. Legislation that would put into force the convention's strictures is before both houses of the Nigerian parliament, he said. "I hope the National Assembly will take it as a matter of great importance and pass this bill before the end of the year," Ogunmola said. "If we signed the convention in 1972 and in the year 2010 we still have not put in place an enabling law to back it up we need to wonder." "Without this law, we cannot prevent bioviolence; we cannot safeguard the security of the state; we cannot put the protocol for controlling what goes on in the laboratory and how we can deter bioterrorism," he stated. A BWC enabling law is more necessary than ever, he said, due to advancements in biotechnology and molecular technology that could make it simpler to develop biological warfare agents (African Press Agency/AfriqueAvenir.org, Nov. 4).

Bandages changes color to indicate state of a wound

Source: http://homelandsecuritynewswire.com/bandages-changes-color-indicate-state-wound

Medical dressings are effective at protecting the site of an injury, but to examine a wound they must be removed; this can not only be painful for a patient, but it can also allow germs to enter the wound and cause infection; researchers developed dressing materials and plasters that do not need to be removed to check the state of a wound -- they indicate pathological changes in the skin by changing from yellow to purple

Bandage color change in the presence of infection // Source: designlaunches.com

While medical dressings are effective at protecting the site of an injury, to examine a wound they must be removed. This can not only be painful for a patient, but it can also allow germs to enter the wound and cause infection. SifyNews reports that now, scientists at the Fraunhofer Research Institution for Modular Solid State Technologies EMFT in Munich have developed dressing materials and plasters that do not need to be removed to check the state of a wound — they indicate pathological changes in the skin by changing from yellow to purple. Dr. Sabine Trupp, a scientist at the EMFT, said: “We have developed an indicator dye which reacts to different pH values, and we have integrated it into a dressing and a plaster. Healthy skin and healed wounds usually show a pH value of below five. If this value increases, it indicates complications in the healing of the wound. If the pH value is between 6.5 and 8.5 an infection is frequently present and the indicator color strip turns purple.” Production of the color-control strip posed a number of challenges for the research scientists as it had to meet several different requirements. “The dye had to remain chemically stable when bonded to the fibers of the dressing material or the plaster to ensure that it does not get into the wound. At the same time, the

indicator had to show a clear change in color and also react sensitively in the right pH range," said Trupp. A prototype of the dressing has already been produced and initial tests have proved successful. The next step will be to use the dressing in a hospital environment at the University of Regensburg's dermatology clinic. At present Trupp and her team are looking for an industrial partner to produce the dressing commercially.

MS drug to lead fight against bioterrorism

Source: http://homelandsecuritynewswire.com/ms-drug-lead-fight-against-bioterrorism

A drug already approved for treating multiple sclerosis show promise as a long sought treatment for victims of bioterrorist attack with botulinum neurotoxin -- which is 10,000 times deadlier than cyanide and the most poisonous substance known to man

Scientists are reporting that variants of a drug already approved for treating multiple sclerosis show promise as a long sought treatment for victims of bioterrorist attack with botulinum neurotoxin — which is 10,000 times deadlier than cyanide and the most poisonous substance known to man. The potential drugs also could be useful in treating other forms of botulism poisoning as well as Alzheimer's disease, multiple sclerosis, and myasthenia gravis, they say in an article in ACS Chemical Biology, a monthly journal. Drug Discovery & Development reports that Kim D. Janda and colleagues explain that the lack of any approved drug treatment for botulism poisoning leaves a major gap in defenses against bioterrorism and biological warfare. People exposed to botulism toxin develop paralysis, cannot breathe, and may require months of treatment on respirators. "The numbers of medical care units capable of providing supportive care for recovery in the event of a bioterrorism incident would be limited," they note. The scientists knew that the multiple sclerosis drug diaminopyridine showed promise for working inside nerve cells to counteract the effects of diaminopyridine botulism toxin. Diaminopyridine itself, however, had disadvantages, including its ability to pass into the brain and have toxic effects on brain tissue. They modified the molecular structure of diaminopyridine to produce two new substances that did not enter the brain and showed good potential as botulism treatments in mice that had been paralyzed by the toxin.

Letter Carriers Add Bioterror Response to the Postal Service

Source: http://www.emergencymgmt.com/health/Letter-Carriers-Add-Bioterror-Response-to-the-Postal-Service.html

An attack on the United States using weaponized anthrax — although considered a low-probability event — would have a high impact on the affected communities. If left untreated, the death rate for those who inhale anthrax is more than 99 percent, according to the Military Vaccine Agency

Anthrax, an acute infectious disease caused by spore-forming bacteria, can be used for biological warfare because the spores can be spread using missiles, artillery, aerial bombs and other methods, making it easily airborne. The good news is that oral medications can be used to treat people who have been exposed; however, the medication must be administered within 48 hours of infection. A bioterrorist attack would likely take place in a large, metropolitan area, and depending on wind speed and direction, the spores could travel hundreds of miles. In response, state and local health departments are prepared to set up mass dispensing sites to distribute medication from the Centers for Disease Control and Prevention's (CDC) Strategic National Stockpile to people who may have been infected. But the federal government sought additional methods to dispense the medical countermeasures, and in its planning found a partner in a program that visits nearly all U.S. residences Monday through Saturday — the U.S. Postal Service (USPS). The plan was put on the federal front burner in December 2009 when President Barack Obama signed an executive order stating: "The U.S. Postal Service has the capacity for rapid residential delivery of medical countermeasures for self-administration across all communities in the United States." The order gave the USPS and U.S. Department of Health and Human Services (HHS) 180 days to create a national dispensing model for U.S. cities to respond to a large-scale anthrax

attack. The result was a program — the postal plan — that uses the nation's letter carriers to deliver medical countermeasures. "The postal plan puts letter carriers on the street to deliver medications in the event of such an attack," said Peter Nowacki, a USPS spokesman in Minneapolis. "Mail delivery would be curtailed, and they would just be going house to house delivering the medication along with information sheets telling people how to take the medication or whether they could take the medication." The postal plan was identified as a viable delivery method following an anthrax attack, because postal workers would be doing their everyday job, but with a different material. "It's something that enhances the existing capabilities to do the distribution and goes further to helping protect our American people in the event of this kind of crisis," said John Koerner, chief of the Chemical, Biological, Radiological, Nuclear and Explosives Branch within the HHS' Division of Preparedness Planning. The "postal plan," as people working on the initiative call it, is being tested in the Minneapolis/St. Paul area for locations within the ZIP codes beginning with 551 and 554. The plan is part of the CDC's Cities Readiness Initiative (CRI), which enhances preparedness in the nation's largest metropolitan areas and has developed a set of strategies for the rapid delivery of preventive medication to people living in major metropolitan areas following a biological attack. Although the executive order was issued in late 2009, the CRI began in 2004. Cities are selected based on criteria, including population and potential vulnerability to a bioterrorism threat.

Preparing the Nation

The question that comes to many minds is why focus on anthrax when there's a broad spectrum of potential biological weapons. "The CDC has identified a criteria list of certain agents that we could anticipate being used for such purposes," Koerner said, "and some of the intelligence and other information we have suggest that if one is going to be used, anthrax is, for a number of reasons, probably the likeliest agent." Before the president called for the creation of a national dispensing model in 2009, proof-of-concept exercises had been conducted in Boston, Philadelphia and Seattle. During the exercises, letter carriers delivered mock antimicrobial agents to 20,000, 40,000 and 50,000 separate housing units in each jurisdiction, Koerner said. "The process went well, and it took only about six to nine hours for them to cover their route and make sure all those folks — the 20, 40 and 50 thousand — received their mock antibiotics in a timely fashion," he said. "The proof of concept showed that it can work." The planning regiment that was used in the drills was applied to the Minneapolis/St. Paul area's postal plan. USPS representatives visited some post offices within the 551 and 554 ZIP codes and spoke with managers, letter carriers and delegates from the letter carriers' union to outline the program and its expectations, as well as enlist volunteers to participate in the pilot, Nowacki said. Before the volunteer postal workers began training, they completed a medical screening to ensure that they could ingest the antibiotics and were fitted for safety equipment. Volunteers were trained on what types of safety equipment to wear; where they'd report if called upon to distribute the medication; what their specific assignments would be; and the procedures for obtaining the medication, loading it into their vehicles and how to deliver it. About 400 people — including letter carriers, USPS supervisors and public health representatives — in the Minneapolis/St. Paul area are participating in the pilot program, Nowacki said.

Collaboration Is Key

Jude Plessas, executive manager of counter- measures delivery and distribution at USPS Headquarters, stressed that this project requires collaboration and participation from all the parties involved. "If one party decides that they're not interested in pursuing this, we basically have to pick up our tents and go home," he said. "But what we saw in Minneapolis/St. Paul was really an extraordinary collaboration between the Postal Service, Health and Human Services, the public health departments — principally the Minnesota Department of Health, which is the regional planning lead — and also law enforcement agencies, because we require security for our volunteer carriers as they're performing this mission." The cities approached the USPS about participating in the postal plan when the concept was floating around, Plessas said, adding that the Minnesota Department of Health looked at its dispensing network and determined it needed methods to supplement its primary distribution model: mass dispensing sites. In an anthrax attack in the area, most residents would receive antibiotics by visiting a mass dispensing site, which will be located throughout the metropolitan area, according to Buddy Ferguson, a risk communication specialist with the Minnesota Department of Health. "However,

initially we also may activate the postal plan and have postal personnel deliver antibiotics to addresses in selected high-density, highly populated ZIP codes," he said, "basically so we can take some of the pressure off the mass dispensing sites." Although some people will receive the pills through the mail service, affected individuals will need to visit a dispensing site at some point. Each household will initially receive 20 pills, Ferguson said, but individuals exposed to anthrax must take the medication for 60 days. Also, people who cannot take doxycycline — "the first-choice antibiotic" according to Ferguson — will have to visit a mass dispensing site to obtain alternative medication. "If we can get everyone started within 48 hours, that's the goal," he said. "That's what we would need to do to prevent the very serious outcome that we would see if there was a mass attack using airborne anthrax." As of press time, the Minneapolis/St. Paul area had yet to complete an on-the-ground test of putting letter carriers on the street delivering mock antibiotics, but the plan is in place and ready for execution. "Right now in Minneapolis/St. Paul, the plan — at least for the first sector in 20 ZIP codes — is operational," Plessas said. "If we received the call from the Minnesota Department of Health and the governor made the request, we would follow through on bringing carriers in and we would perform the mission."

A Bridge to the Future

Before the postal program is expanded to other cities, another pilot will take place in Louisville, Ky. Plessas said the city, like the Minneapolis/St. Paul area, completed a strategic security plan, and the USPS is working with Louisville officials on the initiative. "We would like to take some lessons learned from what we went through in Minneapolis/St. Paul and tweak a few things when it comes to the solicitation process, screening process and overall planning process," he said. "So Louisville will probably be our bridge between the pilot and full program implementation." However, as with all initiatives during this economic climate, the program's future depends on funding. There's very little funding available for the postal program, Plessas said, and it costs money to screen and train volunteers, equip delivery units with supplies, and exercise the plan. It should also be noted that none of the funding for this initiative comes from stamp sales — it's funded through HHS appropriations in the annual budget. "If they continue to show up and we can continue to put together that selection process," Plessas said, "we should be able to expand it to other cities." Many major municipalities already have contacted the HHS about the postal program, Koerner said, and he urged interested localities that want to participate to do the same. "The idea is that over the next couple of years we'll expand this particular program to help supplement, augment and enhance whatever is existing in a locality," Koerner said.

Modeling Preparedness

Jurisdictions that aren't included in the Centers for Disease Control and Prevention's Cities Readiness Initiative, which develops preparedness programs in large cities and metropolitan areas, can still actively equip their agencies for a bioterrorist event like an anthrax attack. John Koerner, chief of the U.S. Health and Human Service's Chemical, Biological, Radiological, Nuclear and Explosives Branch, said the first piece in preparing for such an emergency is to ensure that jurisdictions' planning is evidence-based by using existing experience and expertise to inform plans and processes. He recommends the department's Public Health Emergency website, www.phe.gov, as a reference for planning and preparedness. An anthrax playbook on the website offers a high-level description of what the federal response to an anthrax attack looks like and planning factors that must be identified.

From Future Microbiology

Third-generation Smallpox Vaccines: Challenges in the Absence of Clinical Smallpox

Clement A Meseda; Jerry P Weir

Abstract

Smallpox, a disease caused by variola virus, is estimated to have killed hundreds of millions to billions of people before it was certified as eradicated in 1980. However, there has been renewed interest in smallpox vaccine development due in part to zoonotic poxvirus infections and the possibility of a re-emergence of smallpox, as well as the fact that first-generation smallpox vaccines are associated with

relatively rare, but severe, adverse reactions in some vaccinees. An understanding of the immune mechanisms of vaccine protection and the use of suitable animal models for vaccine efficacy assessment are paramount to the development of safer and effective smallpox vaccines. This article focuses on studies aimed at understanding the immune responses elicited by vaccinia virus and the various animal models that can be used to evaluate smallpox vaccine efficacy. Harnessing this information is necessary to assess the effectiveness and potential usefulness of new-generation smallpox vaccines.

Smallpox: A Disease Conquered in the 20th Century

Smallpox is caused by variola virus (VARV), an orthopoxvirus of the Poxviridae family. Smallpox was notoriously reputed to have caused the deaths of hundreds of millions to billions of people from the times of ancient Egyptian civilization until it was eradicated in the fourth quarter of the 20th Century through prophylactic vaccination. The practice of variolation, the inoculation of matter from smallpox lesions on scarified skin surface, has recently been reviewed. Variolation was practiced in Asia, Africa and Europe until the English physician, Sir Edward Jenner, published an interesting observation showing that dairymaids who contracted cowpox were protected from smallpox. This seminal observation led to the use of cowpox virus, and later vaccinia virus grown on the skin of different animal species (e.g., sheep, calf), as vaccines for immunization against smallpox. First-generation smallpox vaccines did not undergo clinical trials before they were used to immunize against smallpox. Nevertheless, as different strains of vaccinia virus, including the New York City Board of Health (NYCBH), Lister-Elstree, Tian-Tan and EM63 were employed for vaccination in different parts of the world, cases of smallpox began to wane in the industrialized world as early as the 1950s, underscoring the effectiveness of vaccinia virus-based smallpox vaccines. A global campaign to eradicate smallpox was initiated in 1959 by the WHO. The smallpox eradication campaign was invigorated in the 1960s and 1970s, such that in most industrialized nations, smallpox was no longer endemic by the late 1960s/early 1970s. In the USA, for instance, vaccination of the general population was stopped in 1971. With Somalia as the final frontier, the last known natural case of smallpox was reported in October 1977, and 3 years later, smallpox was declared eradicated at the World Health Assembly meeting in 1980, ushering in a new era of a smallpox-free world.

Global mass vaccination against smallpox was discontinued thereafter, but vaccination has continued to be recommended for people with occupational risk of acquiring vaccinia virus (or other orthopoxvirus) infection (e.g., laboratory workers who handle vaccinia virus). Among the growing list of historical and emerging infectious diseases of clinical significance, smallpox is the only infectious disease of man to have been successfully eradicated to date. The successful eradication of smallpox has been attributed to a number of factors, amongst which are:

* The causative agent, VARV, has only one known reservoir; humans. Therefore, unlike a zoonotic infection, combating smallpox was essentially a war with one front;
* The discovery that orthopoxvirus species that caused mild infections in humans elicited cross-protective immune responses against VARV. Thus, following initial practices of prophylactic variolation in ancient times, vaccinia virus-based vaccines were developed and used for prophylactic immunization against VARV infections;
* The successful implementation of vaccination campaigns across the globe, facilitated by, arguably, an unprecedented positive political will on the part of governments of the various countries.

Although smallpox has been eradicated, VARV is known to be officially retained at two WHO collaborative centers: the Centers for Diseases Control and Prevention (Atlanta, GA, USA) and The State Research Center of Virology and Biotechnology (Novosibirsk, Russia). It is not known, however, whether there is/are clandestine/unregistered sources of the virus. Thus, despite the eradication of smallpox, the possibility of a re-emergence of the disease either from inadvertent or malicious release of existing stocks of VARV, or reconstruction of VARV in the laboratory, remains a concern. Also, a number of orthopoxviruses that infect different animal species are known to be potential sources of zoonotic infections in humans. Zoonotic poxvirus infection in humans is epitomized by the recurring human monkeypox virus (MPXV) outbreaks in Central Africa; the persistent recurrence of vaccinia-like

virus infections in Brazil; buffalopox virus infections in India; and cowpox virus infections in Europe. An outbreak of MPXV infections (from animals imported from West Africa) was also recorded in the midwestern states of the USA in 2003. Given the historical antecedent of smallpox as a disease of high mortality, and coupled with a persisting threat of zoonotic infections by other orthopoxvirus species, and the dwindled state of herd immunity against poxviruses consequent upon the cessation of vaccination, the availability of effective smallpox vaccines remains a necessity. This review focuses on the immune responses to smallpox vaccines, with a view to providing insights on recent advances in understanding the nature of the protective immune response elicited by smallpox vaccines and how such understanding will be useful in advancing the development of a new generation of safe, immunogenic and effective smallpox vaccines.

Smallpox Vaccines: From Live Vaccinia Virus to Subunits

For most of the 20th Century, replicating vaccinia virus strains were propagated in live animals (e.g., calf, sheep, water buffalo) and used as smallpox vaccines. The effectiveness of smallpox vaccines was demonstrated by the steady decline in the number of cases of smallpox. Despite their efficacy as prophylactic vaccines against smallpox, replicating vaccinia virus strains, including first-generation (traditional) smallpox vaccines, were associated with some rare, but serious, adverse reactions in some vaccinees, including immunocompromized people, individuals with certain skin conditions (eczema and atopic dermatitis), and people with heart disease, although a direct causal association with heart diseases has not been established.

The common adverse reactions seen in people for whom replicating smallpox vaccine is contraindicated include generalized vaccinia, eczema vaccinatum and post-vaccinial encephalitis. In relatively recent smallpox vaccinations in the USA, high rates of myopericarditis were reported among military and civilian healthcare workers inoculated with Dryvax® between 2002 and 2003. Because of these adverse reactions, efforts were made as early as the 1930s and continuing through to today to develop safer, less reactogenic smallpox vaccines.

Progress in the development of new smallpox vaccines for immunization against smallpox has recently been reviewed. First-generation smallpox vaccines, including Dryvax, Aventis-Pasteur smallpox vaccine, Lister/Elstree, EM-63, Temple of Heaven and Lancy-vaxina were derived from replicating vaccinia virus strains, and were successfully used as prophylactic vaccines for the eradication of smallpox. Concerns in the early 2000s about the possibility of terrorism-related use of VARV or MPXV led to efforts to increase the number of available vaccine doses. Second-generation smallpox vaccines were derived directly from the first-generation vaccines by propagation in cell culture, under controlled good manufacturing practices, without any intended genetic manipulations or extensive passage in cell culture, and are thus similar in characteristics to their predecessor strains. For example, ACAM2000®, currently licensed in the USA, is prepared in Vero cells, and was derived as a plaque-purified clonal isolate from Dryvax (an NYCBH strain), the vaccine that was used in the USA during the smallpox eradication program. Similarly, the Elstree-BN vaccine was derived from the Lister/Elstree vaccine (widely used in Europe and other parts of the world) by propagation of the Lister/Elstree virus in chick embryo fibroblast cells.[38] Although the second-generation smallpox vaccines have not been directly shown to be effective against smallpox, they are expected to retain the efficacy of the first-generation smallpox vaccines because of their close relatedness. In Phase 1 clinical trials, ACAM2000 elicited vaccinia-neutralizing antibodies and cell-mediated immune responses, with both clinical and immunological outcomes similar to Dryvax. Second-generation smallpox vaccines also induce reactogenicity similar to first-generation vaccines.

Development of candidate smallpox vaccines currently categorized as third-generation smallpox vaccines actually began much earlier (in the 1970s) than the second-generation vaccines. Their development was in response to the known adverse reactions caused by inoculation with first-generation smallpox vaccines. Unlike first- and second-generation smallpox vaccines, third-generation smallpox vaccines were derived by more extensive passage of vaccinia virus in cell culture, leading to attenuation. Efforts to develop third-generation smallpox vaccines followed an initial attempt in the 1930s to developed 'cultured vaccine' by attenuating the NYCBH strain through systematic passage in

minced chick embryo tissue.] Two candidate third-generation smallpox vaccines that are relatively far along in development, modified vaccinia Ankara (MVA) and LC16m8, were derived by passaging of parent vaccinia virus strains in cell culture: MVA by extensive (> 570) passages of the chorioallantois vaccinia virus Ankara strain in chick embryo fibroblast cells;[36] and LC16m8 by more than 45 passages of the Lister strain in primary rabbit kidney cells. MVA and LC16m8 were used as vaccines in children in Germany and Japan, respectively, in the 1970s, and appear to have better safety profiles than the first- and second-generation vaccines. Other potential third-generation vaccines, including NYVAC,[48] defective vaccinia virus Lister and VACVDE3L, have also been described.

These third-generation vaccine candidates have undergone preclinical testing, with varying amounts of data with regard to the dosage required to elicit a protective response. For example, MVA must be inoculated at a dose in the order of 107–108 pfu (or TCID50), sometimes with booster inoculations, in order to elicit a robust immune response that is similar to that of a replicating vaccinia virus when administered into animals. In terms of immunogenicity, NYVAC was found to provoke lower antibody titers than Dryvax and Lister vaccines, and did not induce antibodies to the vaccinia virus A27 protein, a protein that induces neutralizing antibodies after vaccination with first-generation smallpox vaccines or when used as a subunit vaccine in animals. Both MVA and LC16m8 have been evaluated in clinical trials and have been shown to be immunogenic, but their efficacy in preventing smallpox is unknown. NYVAC and MVA have also been used extensively as recombinant viral vectors for the expression of bacterial, parasitic and viral genes in immunization studies for clinical and veterinary vaccines. Attempts to develop subunit smallpox vaccines (sometimes referred to as fourth-generation smallpox vaccines) using combinations of viral proteins, DNA or vaccinia genes expressed in other virus vectors are ongoing, but these approaches are in relatively early stages of development.

Thus, despite the availability of vaccines that are currently licensed for immunization for the prevention of smallpox, efforts are ongoing to develop new smallpox vaccines. The new-generation vaccines under development are generally expected to be less reactogenic and safer for most of the human population than their predecessors. But in the absence of clinical smallpox, the evaluation of efficacy of new-generation smallpox vaccines poses a challenge, and will rely heavily on efficacy data obtained from appropriate animal models. Bridging of preclinical immunogenicity and efficacy data to immunogenicity data from clinical studies is also important. Over the past decade, several studies have been published comparing new smallpox vaccines under development with first-generation smallpox vaccines in various animal models of vaccine efficacy. For example, compared with Dryvax, LC16m8 elicited similar humoral responses and protection in mice and rabbits when vaccinated animals were challenged with vaccinia virus, ectromelia virus or rabbitpox virus. Similarly, a two-dose regimen of MVA induced protective responses against MPXV, equivalent to immunization with Dryvax, in cynomolgous macaques. Immunogenicity data from studies such as these have yielded additional information on the type of immune responses to smallpox vaccines, and are a critical component of the efficacy evaluation of new-generation smallpox vaccines.

Immune Responses to Smallpox Vaccines

During the smallpox eradication campaign, much effort was devoted to accomplishing the objective of eradicating the disease. Thus, relevant scientific questions regarding the mechanisms of vaccine immunogenicity and protection, as well as vaccine manufacturing practices, were not extensively addressed at the time. For instance, smallpox vaccines were routinely prepared from vaccinia virus that had been propagated in live animals, which in the stringent regulatory environment of the 21st Century would be problematic for a variety of reasons. Interestingly, despite the obvious success of smallpox vaccination, one scientific question that has not been successfully answered is: what made the smallpox vaccines so effective? In other words, what was the nature of the immune responses elicited by smallpox vaccines, and what was the relevance of such responses to the protection against smallpox? It was known that smallpox vaccines activated both the humoral and cellular response arms of the immune system, but the key immunological responses that must be elicited in order to attain to the threshold of immune protection are not known. Arguably, the contemporary technologies of the 1930s to the 1970s would not have been adequate for such investigations. An interesting observation during the smallpox scourge was that people who survived natural smallpox developed life-long immunity against

the disease, but immunity following vaccination begins to wane in vaccine recipients 3–5 years after vaccination, even though the majority of vaccine recipients retain some level of antibody up to 75 years after vaccination. The mechanism of vaccine-induced protection is not clear, leaving a major gap in knowledge of the correlates of immune protection against smallpox that becomes relevant for efficacy evaluation of new-generation vaccines.

Nevertheless, substantial progress has been made in identifying virus-encoded proteins that are targets for immunological responses. Published sequence data of many vaccinia virus strains demonstrate that the vaccinia virus genome contains more than 200 open-reading frames, encoding different viral proteins, many of which have been investigated and characterized. Several of the viral proteins that are targets for immunological responses have been identified. An important lead was the understanding of the vaccinia virus replication process that results in the production of two distinctly different major forms of infectious virions: the mature virion (MV) and enveloped virion (EV), also known as intracellular MV and extracellular EV, respectively. The EV form has an extra lipid membrane compared with MV. The formation of MV, EV and two other intermediate forms, intracellular EV and cell-associated EV, has been thoroughly reviewed elsewhere. The MV, is the stable, predominant form of the virus, and believed to be responsible for host-to-host dissemination of the virus, while the EV is labile. With the exception of a few relatively high EV-producing vaccinia virus strain, such as IHD-J, EV constitutes only about 1% of virions, and is thought to be responsible for long-range spread of virions in an infected host. With the MV form expressing approximately 20 membrane proteins and the EV form expressing six other membrane proteins,[80] the distinct surface antigen composition of the two forms has relevance to the immune responses elicited by smallpox vaccines and the control of virus pathogenesis. For example, it was observed that inactivated vaccinia virus elicited high neutralizing antibody response in rabbits, but unlike vaccination with live vaccinia virus, failed to protect rabbits from intradermal challenge with rabbitpox virus. Since inactivation results in the loss of labile EV and inactivated vaccinia virus cannot replicate to produce EV, the data suggest that components of the EV are important for protection.

Altogether, several studies have described molecular approaches to mapping specific vaccinia virus epitopes that are recognized and targeted for antibody- or cell-mediated immune responses after vaccination. These studies have been reviewed. Data from these studies suggest that both humoral and cell-mediated immune responses are elicited, and that the majority of vaccinia virus epitopes recognized by the immune response are conserved in VARV, and thus are relevant to the immunological defense against smallpox.

Antibody Responses

Data from numerous animal studies and smallpox vaccine clinical trials have demonstrated that vaccination results in a robust antibody response including the production of vaccinia-neutralizing antibody. Although the relative contribution of specific antibody to protection is not fully understood, several observations in the 20th Century underscored the relevance of humoral immune response to smallpox vaccines efficacy. It was recognized that the detection of neutralizing antibodies correlated with protection from smallpox. For instance, it was observed that vaccine recipients with low vaccinia-neutralizing antibody titer (<10), were more prone to develop a lesion (a 'take') following re-vaccination, thus suggesting a possible correlation between the level of neutralizing antibodies and protection. Similarly, it had been observed in a study in Pakistan that people with a neutralizing antibody titer of at least 32 were protected from smallpox following contact with patients. Passive antibody transfer experiments in animal models have also suggested that vaccinia-neutralizing antibodies may ameliorate the course of infection or confer partial protection. Fenner reported that passive serum transfer protected mice from mousepox. Notably, vaccinia immunoglobulins, a human immunoglobulin preparation from individuals who have been repeatedly vaccinated, is used as a treatment regimen in some vaccinees who reacted adversely to smallpox vaccines. In investigating the relevance of vaccinia immunoglobulin in mice, it was observed that immunocompetent mice that were treated with vaccinia immunoglobulin up to 2 days after inoculation of a lethal dose of vaccinia virus survived the challenge. On the other hand, immunodeficient mice that received the same treatment succumbed to vaccinia virus infection and did not survive, suggesting that a full complement of the adaptive immune response may be needed for full protection. In another study using the MPXV challenge model, it was reported that the

antibody depletion of B cells, but not the depletion of CD4+ and CD8+ cells, prior to vaccination, precluded the development of protective immunity after vaccination of macaques. One study provided more insight as to the relevance of antibody response to immune protection. In this work, Chaudhri et al. used the mouse/ectromelia virus infection model to show that B6.μMT mice deficient in B cells or B6.Aa−/− mice lacking CD4+ T-cell function due to deficiency in major histocompatibility complex (MHC) class II, had persistent infection following ectromelia virus infection, despite having functional CD8+ T cells. Interestingly, these mice were able to survive ectromelia virus infection if they received immune sera or naive B cells. These authors recently showed that post-immunization antibody response correlated with protection from a subsequent challenge with ectromelia virus. In other studies, these authors showed that, while cell-mediated immunity is essential for clearing acute poxvirus infection, antibody response was required for recovery from persistent infection or a secondary infection.Taken together, data from these studies suggest that antibody responses following vaccination are a major contributor to the protection from orthopoxvirus infection.

With the recognition of distinct membrane antigens on the MV and EV forms of vaccinia virus,[80] it has been variously suggested and demonstrated that the vaccinia EV is a target for vaccinia-neutralizing antibodies. Other investigators have used subunit components of vaccinia virus or analyzed antibody responses to specific vaccinia virus proteins in immune sera to study their contribution to immune responses.[These efforts have led to the identification of specific viral proteins of the MV and EV form of the virus that, when used singly or in combination, provoke the elicitation of protective immune responses in various animal models, including neutralizing antibodies. Vaccinia MV proteins, notably A27 and L1, are known to provoke high titers of neutralizing antibodies when inoculated into animals. The A28 protein, a component of the MV entry/fusion complex, was also recently shown to elicit a protective immune response that includes neutralizing antibodies. Immune responses to the EV proteins A33 and B5 also elicit full or partial protection in various animal models. It appears however, that models in which a combination of both MV and EV antigens are used in immunization elicit a more robust protection. In some instances, protective epitopes in viral proteins have been identified. Similarly, the poxvirus B5R gene of the EV form, when used as DNA- or virus-vectored vaccines, or in combinations with the B5 protein in prime/boost immunization schedules, has been shown to provoke a specific antibody response that neutralized vaccinia virus EV in vitro and conferred protection from lethal challenge with poxviruses. Although the specific mechanisms of antibody-mediated protection conferred by smallpox vaccines are not fully understood and the role of the antibody response to specific viral proteins is not completely elucidated, data from such studies provide strong supporting evidence for the relevance of antibodies in vaccine-induced protection.

Cell-mediated Immune Responses

Early evidence that cell-mediated immunity (CMI) plays an important role in the immune protection elicited by vaccinia virus came from the observation that severe adverse reactions to smallpox vaccines occurred in individuals with impaired T-cell functions, whether congenital or acquired, but not in individuals with congenital agammaglobulinemia. Subsequently, several lines of evidence have been described validating the relevance of cell-mediated responses in the protection against orthopoxviruses in animal models. Mice, including the A/J and ANcr strains, with weak Th1 cytokine response (suggestive of a weak cell-mediated immune response) are more susceptible to infection with ectromelia virus than mouse strains with a strong Th1 cytokine response. Ennis et al. reported the detection, following vaccination of naive individuals, of strong vaccinia-specific cytotoxic CD8+ cells and IFN-γ-producing T cells in peripheral blood mononuclear cells (in seven of eight subjects) obtained from vaccinees 27 days after vaccination. Similarly, high levels of IFN-γ-producing cells have been detected in both vaccinia-naive and re-vaccinated individuals, but there appears to be a lack of booster effect on the level of CD8+ T-cell response following booster smallpox vaccination.

Several laboratories have studied CMI responses to vaccinia virus, including identifying the type of cell-mediated responses and the type of immune cells involved, and specific vaccinia epitopes eliciting these responses. Terajima et al. described two CD8+ T-cell epitopes of vaccinia virus that are restricted by the human MHC I allele, HLA-A*0201. These epitopes mapped to the C16L (B15R or B22R) gene and the C7L gene in the Copenhagen strain of vaccinia virus, and were identified using T cells that were

obtained from individuals who had been vaccinated with Dryvax. This study showed that between 6 and 35% of the total vaccinia-specific T cells producing IFN-γ targeted the two epitopes. While the function of C16L is unknown, C7L has been characterized as a host-range gene and nonessential for virus replication. An interesting finding in this work was that the two epitopes are conserved in both vaccinia and VARV strains. From a vaccine perspective, the latter observation suggests that the two epitopes could be important in the protection elicited by smallpox vaccines. The product of C16L and C7L (C16 and C7, respectively) are not among the list of vaccinia virus proteins that have been extensively investigated and known to elicit a protective immune response in animal models, but the high percentage of IFN-γ cells targeted at these epitopes suggests there could be several other yet-to-be-identified epitopes spread across many of the more than 200 proteins encoded by vaccinia virus. Using an expression library of all predicted open-reading frames of vaccinia virus, Tscharke et al. identified five virus epitopes that could trigger poxvirus-specific CD8+ T-cell response in C57BL/6 mice.[114] The work further showed that the immunodominance of the peptides in eliciting a CD8+ T-cell response is in part determined by the route of immunization and the vaccinia virus strain used. The diversity of the immune response to smallpox vaccines was further highlighted in the work described in, where it was observed that some vaccinia virus peptides had equivalent immunogenicity (in terms of CD8+ T-cell response) in inbred mice and their F1 (MHC–congenic hybrid) progenies. Other peptides that were immunogenic in the inbred mice had reduced immunogenicity (as much as >90% reduction) in their F1 progeny. While significant research progress has been made over several years, the totality of the CMI response to vaccinia virus is by no means fully understood, especially given the broad genotype diversity among human populations and the difficulty in extrapolating protective T-cell epitope data from mice to humans. Therefore, further research efforts in the coming years would be critical in providing a more comprehensive understanding of the nature and significance of cell-mediated immune responses triggered by orthopoxviruses, and especially the relevance of such responses to vaccine efficacy.

Determining Immune Correlates of Protection against Orthopoxviruses

Knowledge of the correlates of immune protection against orthopoxviruses is important for the design and development of new-generation smallpox vaccines. Because little is known about the correlates of immune protection against smallpox (i.e., against VARV), coupled with the absence of clinical smallpox, various attempt at defining the correlates of protection elicited by smallpox vaccines have had to rely on data from immunogenicity and efficacy studies in animals. In the past decade, many research laboratories have devised a number of methods to study the nature and diversity of the immune responses elicited following vaccination with vaccinia virus strains in various animal models. Human sera and peripheral blood mononuclear cells obtained from vaccine recipients have also provided valuable data regarding the immune response to vaccination. In addition, various molecular approaches have been employed in dissecting the immune response to smallpox vaccines and identifying the immune correlates of protection, especially as a means toward understanding the involvement of antibody and T-cell responses to a virus with numerous virally encoded proteins that could be potential targets of the immune mechanism.

In investigating whether or not a gene product is essential for virus replication, the gene-knockout approach is commonly used. For instance, deletion of the gene encoding the uracil DNA glycosylase gene or the serpin SPI-1 gene from the vaccinia virus genome essentially results in the inability to produce virion progenies in normally permissive cells. Similarly, the deletion of EV A33R gene from vaccinia virus, although it did not obliterate virus replication, resulted in the formation of tiny plaque phenotypes in vitro, relative to the parent virus. We recently observed that the use of a similar gene knockout strategy in identifying viral gene products that could be essential for protection has limitations because of an apparent redundancy in the protective response. In our laboratory, we observed that a severely impaired NYCBH-based mutant that carries a deletion of both the A33R and B5R genes and produces minimal or no cytopathic effect in common laboratory cell lines protected BALB/c mice from intranasal challenge with either the Western reserve (WR) strain or the IHD-J strain of vaccinia virus.

The use of individual or combinations of vaccinia virus genes or proteins as subunit vaccines is another approach that helps to indirectly identify vaccinia virus genes that could be relevant in protection. For example, the vaccinia A33 and B5 (proteins of the EV form) and several of the matured virion proteins

(A27, A28, L1, D8 and H3) have been identified as eliciting protective immune responses in animal models when used as subunit DNA, protein vaccines, DNA/protein prime/boost or expressed as recombinant proteins in virus vectors in various animal models. Testing of immune sera (vaccinia immunoglobulin) from smallpox vaccine recipients also shows that neutralizing antibodies recognize both EV and MV proteins. In other studies, we observed that the vaccinia virus A56R (encoding viral hemagglutinin) is highly immunogenic, eliciting high IgG titers when inoculated into mice as a recombinant expressed in Semliki forest fever virus, but protection is not conferred as for immunization with the A33 protein. This is consistent with an earlier observation that subjects lacking detectable hemagglutination-inhibition antibody were protected from smallpox.[85] Although the information from the use of subunit vaccines will not necessarily definitively confirm a viral protein as essential for protection, it does provide useful information as to what a subunit smallpox vaccine formulation should contain. In work described in, for instance, it was observed that protection against lethal orthopoxvirus challenge was more robust when the subunit formulation contains subunits of both the EV and MV form of vaccinia virus. These EV and MV subunits seem to elicit neutralizing antibodies as the major predominant mechanism of protection.

Other modern molecular approaches have been employed in attempting to dissect the immune responses to smallpox vaccines. For instance, in determining the level of vaccinia-specific CD8+ T-cell response following vaccination with the Lister vaccine, Trojan et al. used quantitative real-time PCR to measure IFN-γ mRNA levels after re-stimulating (with peptide) peripheral blood mononuclear cells obtained (pre- and post-vaccination) from study subjects. They found that the measured CD8+ T-cell response was similar to data obtained using the IFN-γ enzyme-linked immunospot (ELISpot assay). Similarly, proteome microarrays were used to show that the antibody response elicited following vaccination with MVA was similar to the antibody response to Dryvax. In this work, microarrays of the WR strain proteome were developed and probed with immune sera obtained from macaques and humans that had been vaccinated with MVA or Dryvax, for vaccinia proteins that are targets of antibody response after vaccination. Although the focus of this work was to compare the target protein profiles for the antibody response to MVA versus Dryvax, it also yielded vital information regarding the spectrum of vaccinia proteins eliciting an antibody response. The limitation of microarray analysis as may be applicable to identifying the correlates of protection is that it does not provide information as to the functionality of the measured antibody responses.

A major difficulty in defining the correlates of protection needed against orthopoxviruses is the redundancy of the immune response to such complex virus targets. In the work described in,[75] neutralizing antibodies directed at the vaccinia H3 protein were shown to be the most immunodominant in human antibody response to vaccinia virus. While anti-H3 IgG was sufficient to neutralize vaccinia virus, depletion of anti-H3 IgG (both from human and mice sera) had no effect on the level of virus neutralization, suggesting that other neutralizing antibody against other viral targets are sufficient (in the absence of the most immunodominant MV target) to elicit vaccinia-neutralizing antibodies. Similar redundancy has been observed in the CMI to orthopoxviruses.

Animal Models for Testing Smallpox Vaccines

In addition to the difficulty in defining the most relevant vaccine antigens needed for protective immunity, the identification and development of suitable animal models to evaluate efficacy of candidate vaccines is a major challenge in the path to new-generation vaccine development. Since vaccine efficacy cannot be demonstrated directly against smallpox, animal models must play an essential role in vaccine evaluation. Insight into the pathogenesis of smallpox was obtained from various animal models of poxvirus infections, using virulent strains of vaccinia virus (WR and IHD-J) and other orthopoxviruses (MPXV and cowpox, ectromelia and rabbitpox viruses) as challenge agents in various animal models. The commonly used animal models include mouse/vaccinia virus, rabbit/rabbitpox, mouse/mousepox and monkey/monkeypox models. Over the past decade, the testing of smallpox vaccines for efficacy has also been performed in animals.

The safety and tolerability of new-generation smallpox vaccines can be determined in clinical trials. However, since clinical cases of smallpox no longer exist, data to support vaccine efficacy for licensure

will have to be determined using surrogate methods. One method that was used to test for immune responses to smallpox vaccines in the past was to revaccinate vaccinees and look for evidence of development of lesion at the inoculation site (a 'take'). Absence of a take upon revaccination was assumed to be indicative of a protective immune response to the vaccine virus. In theory, this approach could be adopted for testing new-generation smallpox vaccines, whereby candidate vaccine recipients are challenged with first- or second-generation smallpox vaccines. However, this method is somewhat problematic in practice because the end point is more qualitative than quantitative, and because of the association of the first- and second-generation challenge vaccines with myopericarditis and coronary ischemic events.

To facilitate the review of prophylactics and therapeutics in development when circumstances, including ethical considerations, do not permit clinical efficacy evaluation, the US FDA issued the 'Animal Rule', which states that efficacy data can be obtained from appropriate animal models and bridged to humans. The Final Rule for the Animal Rule was published in the Federal Register in May 2002, with 21 Code of Federal Regulation (CFR) 314.600 and 21 CFR 601.90 applicable to drugs and biologics, respectively. Since smallpox vaccines in development cannot be tested for clinical efficacy, the Animal Rule will most likely be used to evaluate the efficacy of new-generation smallpox vaccines, per 21 CFR 601.90. However, the requirements for the application of the Animal Rule stipulates the satisfaction of four key criteria, which are summarized as follows:

* The pathophysiological mechanism of toxicity of the substance and its prevention or substantial reduction by the product is reasonably well-understood;
* The effect is demonstrated in more than one animal species that is expected to react with a response predictive for humans, a single sufficiently well-characterized animal model may also be used;
* The study end point in animals is clearly related to the intended benefit in humans;
* Data on the pharmacokinetics and pharmacodynamics and other relevant data in humans and animals should allow selection of a dose that will be effective in humans.

How the Animal Rule will be used for smallpox vaccine evaluation is under discussion. It has not been possible to successfully establish an animal model of smallpox, and there is no single animal model that would perfectly model smallpox in humans. The evaluation of new smallpox vaccines will likely require the demonstration of efficacy in a combination of animal models. Bridging preclinical immunogenicity and protection data from these animal models to clinical immunogenicity data will be useful in assessing the efficacy of new-generation smallpox vaccines. The mouse/VV-WR, mouse/ectromelia, monkey/monkeypox and rabbit/rabbitpox models have been the most widely investigated. Small-animal models, especially the various mouse models, have the distinct advantage of allowing for statistical power. In addition, ectromelia virus is known to be a natural mouse pathogen,[133] as VARV is a natural pathogen of humans, and thus, the mouse/ectromelia model may be a useful model in this regard. However, differences in genetic composition, including the MHC system between mice and humans, may mean differences in epitope recognition, calling for caution in extrapolating preclinical efficacy data to vaccine effectiveness in humans.

Ongoing Challenges

Although products of several vaccinia virus genes have been identified as targets of both arms of the immune response, and indeed most of these target genes are conserved among orthopoxviruses, including VARV, whether the immune response they elicit is protective against smallpox remains unknown. In addition, a number of studies have shown that minor differences in amino acid residues can sometime have a profound effect on the functionality of some proteins. For instance, the vaccinia complement control protein (VCP) and its VARV homolog, the smallpox inhibitor of complement enzymes (SPICE), are approximately 95% identical at the amino acid level, differing in only 12 amino acids over the entire length of the polypeptide (vaccinia virus strain Copenhagen vs VARV strain Bangladesh 1974). However, Liszewski et al. demonstrated that the substitution of two amino acids (glutamine-77 and glutamate-120) in VCP with the corresponding VARV residues (histidine and lysine, respectively) in the repeat region increased the potency of VCP as a complement regulator by approximately 2.3 log. Similarly, the B5 protein of vaccinia virus, which is believed to be the main target

for antibody neutralization of the EV form of vaccinia virus, differs from its VARV homolog, B6, in 23 amino acids. However, ten of 26 monoclonal antibodies (including EV-neutralizing antibodies) that were raised against B5 failed to crossreact with the VARV homolog (B6). These data suggest continuing challenges in interpreting immunogenicity and efficacy data for subunit smallpox vaccines.

While subtle differences in epitopes may be compensated for by the availability of other antigen targets provoking neutralizing antibodies or CMI in live virus vaccines, the limited number of antigens in subunit vaccine formulations will reduce the availability of redundant epitopes as targets for protective immune responses. For instance, an antivaccinia A33 monoclonal antibody, MAb-1G10, that protected mice from poxvirus challenge failed to bind the A33 homolog (A35) of MPXV, unless two amino acid residues, serine-118 and glutamate-120, were substituted for leucine and serine, respectively, as present in vaccinial A33. By inference, a highly immunogenic subunit vaccine that elicits immune protection in animal models may not necessarily be as effective as such in the prevention of clinical orthopoxvirus disease in humans. Therefore, while subunit vaccines have a potentially better safety profile than live vaccinia virus vaccines, subunit vaccines might be relatively less efficacious compared with existing live virus vaccines, and rigorous comparisons in multiple animal models would seem prudent. One potential way of addressing this concern is to include as many antigens as possible in subunit vaccine formulations. In this regard, the identification of various vaccinia virus neutralizing-antibody epitopes and T-cell epitopes would be useful for the design and formulation of subunit vaccines.

As already noted, it has not yet been possible to successfully establish an animal model of smallpox, but animal models will be critical for vaccine efficacy evaluation. Of note is the fact that the majority of studies in animal models use routes of vaccine inoculation other than the intranasal route for vaccination; especially because the intranasal administration of vaccinia virus is generally not recommended in clinical applications. However, since it is believed that VARV infection was acquired through the respiratory route or buccal cavity in the majority of victims, a pertinent question is whether the interaction of VARV with mucosal surfaces during natural infection facilitates better downstream adaptive immune responses for life-long protection as opposed to the immune response from percutaneous inoculation (scarification) of vaccines. C57BL/6 mice that were vaccinated by intranasal inoculation of MVA were found to express a CCL2 chemokine, monocyte chemotactic protein (MCP)-1, in their lungs, which was detectable 24–48 h post-inoculation. This work further demonstrated that MCP-1 triggered the movement of leukocytes to the inoculation site, thus activating the immune responses at the inoculation site. Similarly, recent studies using recombinant MVA for the delivery of HIV genes as vaccines suggest a robust immune response against the HIV genes when vaccine was administered intranasally than by the intramuscular route. Although Lehmann et al. did not find a similar effect when replication-competent vaccinia virus strains (Lister, NYCBH and WR) were inoculated intranasally in the C57BL/6 model, it is possible that VARV infection of the respiratory mucosa activates certain factors that effectuate life-long immunity.

Finally, significant challenges must be addressed in bridging and extrapolating preclinical animal immunogenicity and efficacy data to clinical efficacy for humans. This is particularly problematic with regard to new-generation smallpox vaccines that are further removed from the first-generation vaccines, especially as the correlates of immune protection against smallpox are unknown. Therefore, it is difficult to extrapolate preclinical data to humans since even the best surrogate animal model is not likely to exactly replicate the virus–host (human) interaction with VARV. Nevertheless, an increasing amount of data on the various animal models will increase the level of confidence in the use of these models for smallpox vaccine evaluation, and possibly lead to a reliable method of bridging preclinical immunogenicity/efficacy data to humans.

Future Perspective

In the absence of active smallpox disease, the likelihood of a full understanding of the mechanisms of the immune protection elicited by first-generation smallpox vaccines is limited. By implication, the probability of having a complete understanding of the efficacy of new smallpox vaccines is also unlikely, because most efficacy studies will be conducted in animal models with their inherent limitations. However, with the significant improvement in genome sequencing in recent years, there is a vast

amount of information on the complete genome sequences of several orthopoxviruses, including several strains of VARV isolates from different geographical parts of the world, and also several vaccinia virus strains, including some third-generation vaccine candidates, such as MVA and LC16m8. Although it is possible that subtle differences in the polypeptide sequences between orthopoxvirus proteins, or yet-to-be-identified epitope targets in VARV, account for the life-long immunity in smallpox survivors, the available genome sequence data suggest that most of the immunodominant vaccinia virus proteins identified to date are conserved in VARV isolates. Similarly, it is now known that live-attenuated smallpox vaccines, such as MVA and LC16m8, retain several of the genes found in VARV, many of which have been identified as potential targets of immune responses in various animal models. Thus, advances in molecular techniques and the evolution of new biotechnologies in the coming years will further refine the enormous amount of bioinformatic data currently available, thus furthering the insight into the relevance of the various proteins encoded in the vaccinia virus genome. Harnessing these pieces of information will facilitate a more comprehensive understanding of the nature and relevance of the immune responses to smallpox vaccines. Such information would be indispensable for the assessment of the immunogenicity and efficacy of new-generation smallpox vaccines and to provide more insight on the immunology of poxvirus infections.

In summary, data are accumulating on the nature of immune responses to smallpox vaccines, and possible molecular mechanisms of immune protection following vaccination are being elucidated. This accumulating information should be useful in defining relevant molecular markers of protection, and valuable in assessing the utility of new-generation smallpox vaccines for prophylactic immunization. The efficacy of some candidate smallpox vaccines, including MVA and LC16m8, has been demonstrated in some animal models, but their effectiveness against smallpox cannot be ascertained. Nevertheless, accumulating data from preclinical efficacy studies coupled with immunogenicity data from clinical trials suggest that new-generation smallpox vaccines should be useful in ameliorating disease morbidity and reduce case fatalities among immunocompetent populations in the event of a smallpox outbreak. The most desirable situation, however, is that the current status quo prevails, and the need for smallpox vaccines for mass vaccination never arises, with smallpox remaining forever a disease confined to the archives of history.

CBRNE-TERRORISM Newsletter

Δελτίο ΧΒΡΠΕ-ΤΡΟΜΟΚΡΑΤΙΑΣ

Volume 5 - 2010

RAD-NUKE –News

US Unprepared for Dirty-bomb Attack

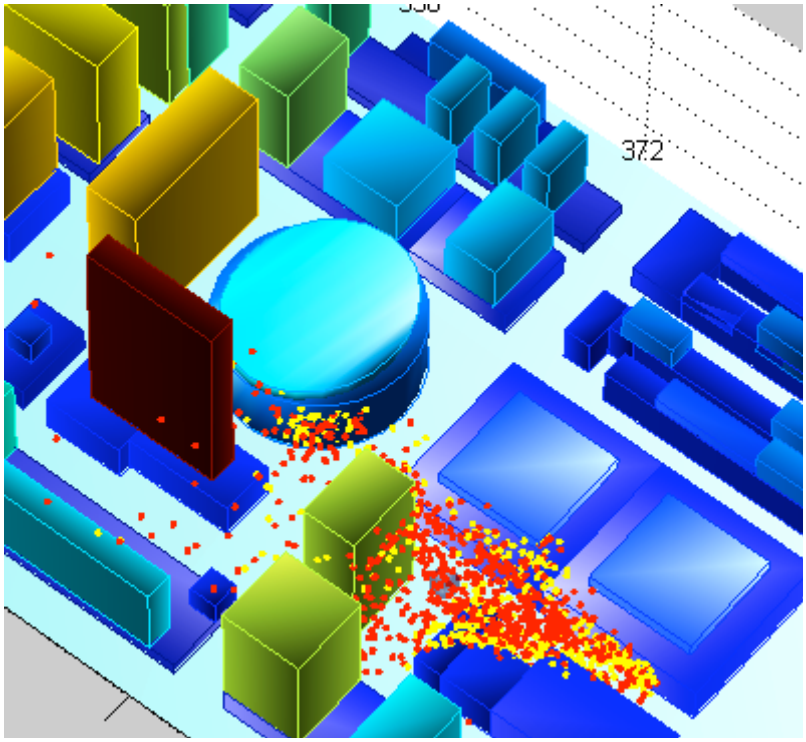
Source:http://thehill.com/homenews/house/123229-top-house-dem-us-unprepared-for-dirty-bomb-attack

The U.S. is "unprepared" to deal with a radiological or small arms attack, even though both are likely to occur, according to a top-ranking House lawmaker on intelligence issues. Rep. Jane Harman (D-Calif.), the chairwoman of the Homeland Security Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, said the possibility of a Mumbai-style attack, in which gunmen storm a specific area, is much more likely to occur than a dirty-bomb attack, but that both scenarios are serious and real threats to U.S. national security. "I'm surprised there hasn't been a successful conventional attack in the United States," said Harman at a New America Foundation event on Wednesday. Harman's comments come in the wake of a State Department warning issued last Sunday to Americans traveling in Europe. The warning asked travelers to be extra vigilant when watching for suspicious activity, but it did not specify what kinds of threats to look for or what countries in Europe were the most vulnerable to attack. Harman, who receives regular classified intelligence briefings, said the White House hasn't done a good job explaining the European scare to Americans, which she described as "a real threat." "[The government] ought to offer people more specific guidance," she said. "This warning has led to more confusion than was necessary … I wish our own government right now were giving more sensible advice to people to know what to look for and what to do." Harman is most concerned that westerners will fly into the U.S. undetected — via the visa waiver program — after they've received terrorist training in the Middle East. The program allows citizens of certain countries to travel to the U.S. for tourism or business for up to 90 days without having to get a visa. Several years ago, Harman traveled to New York City and toured three of the city's major hospitals to inspect the levels of security they use to keep radiological materials safe from theft by terrorists. "They are not adequately secured," said Harman of the materials. "It's not that hard to storm into one of these hospitals, take the source out of the machine and put together a crude bomb and explode it almost immediately, before law enforcement can arrive in adequate numbers." Harman asked administrators at the hospitals about what kinds of background checks they did on employees who handle radiological materials. She said the answers she received led her to believe the detonation of a dirty bomb from a hospital could easily be "an inside job." "I think many of the folks who have emerged as some of our homegrown terrorists would pass any of those checks," she said. "They have very clean backgrounds." Harman said it would cost $250,000 per building to secure the 500 major metropolitan hospitals in the U.S. — totaling $125 million. "I hope that once this election is over … that the House and Senate can get back to work on this subject and find $125 million," Harman said.

Predicting the effect of a nuclear weapon dropped on an urban area

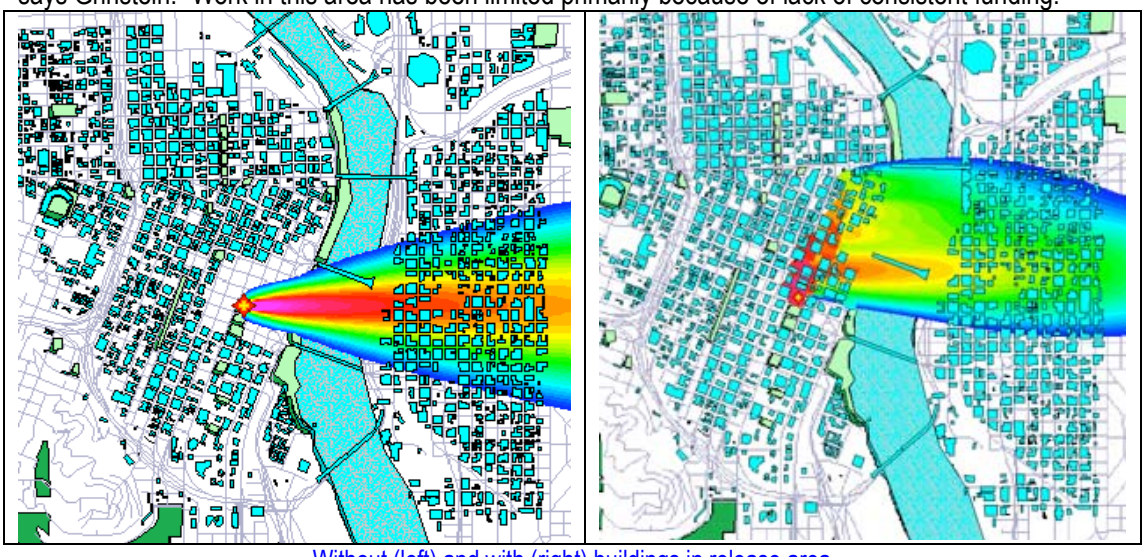
Source:http://www.homelandsecuritynewswire.com/predicting-effect-nuclear-weapon-dropped-urban-area

Red dots represent contaminant in the air, while yellow dots represent deposition on street and building surfaces. Current models of nuclear effects use wind direction and wind speed to draw a predicted



cone-shape area of fall-out; new research results show that these models are too simple in some ways -- for instance, they do not include the complex dynamics of wind movements around buildings, which can concentrate fall-out preferentially in certain areas

If a nuclear weapon were detonated in a metropolitan area, how large would the affected area be? Where should first responders first go? According to physicist Fernando Grinstein, we have some initial understanding to address these questions, but fundamental issues remain unresolved. “The predictive capabilities of today’s state-of-the-art models in urban areas need to be improved, validated and tested,” says Grinstein. “Work in this area has been limited primarily because of lack of consistent funding.”



Without (left) and with (right) buildings in release area

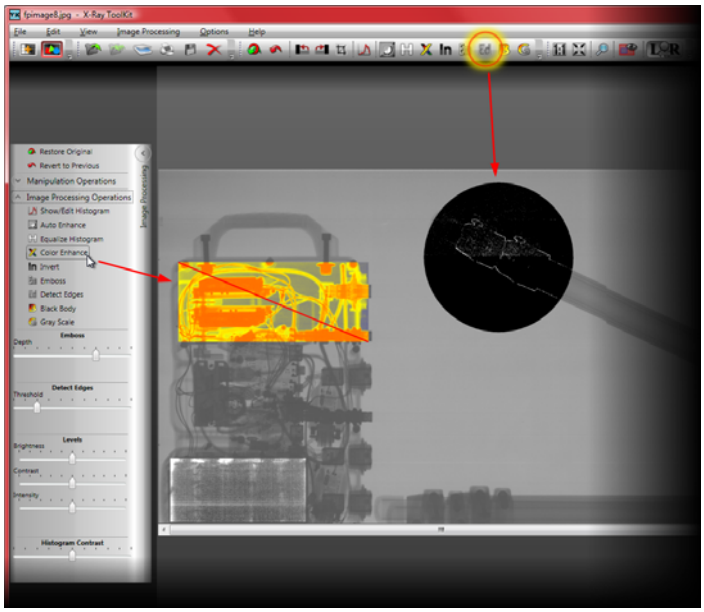
At the upcoming 62nd Annual Meeting of the American Physical Society’s (APS) Division of Fluid Dynamics, which is being held in Minneapolis this week, Adam Wachtor — a student who worked with Grinstein at the Los Alamos National Laboratory in New Mexico — presented his efforts to improve the way that models track the movement of radioactive fall-out carried by the wind. His wind models track

the aftermath of a plume of hot gas released by a small, one-ton device in a typical urban setting at a three-meter resolution. Current models use wind direction and wind speed to draw a predicted cone-shape area of fall-out. Wachtor's results show that these models are too simple in some ways. For instance, they do not include the complex dynamics of wind movements around buildings, which can concentrate fall-out preferentially in certain areas. They also indicate that small changes in the location of the blast and the temperature of the plume released can have a large effect on the contamination patterns. The simulation is part of a larger coordinated effort between DHS (FEMA), the National Laboratories, DTRA, NRL, and private contractors, each of which has concentrated on a different piece of the project. Other studies have shown that, depending on the situation, buildings can provide some degree of shielding from the radiation. The hope of the researchers collaborating in this effort is to eventually provide practical information to guide first responders.

New X-ray imaging to aid nuclear detection

Source: http://www.gsnmagazine.com/node/21656?c=cbrne_detection

The U.S. government's nuclear security agency has come up with a new software tool that will provide better image analysis and detection for nuclear counterterrorism operations. The National Nuclear Security Administration (NNSA) said Oct. 18 that its Office of Emergency Operations has "developed and delivered a new X-ray image processing capability to the nation's emergency response community." Originally developed for medical diagnostic imaging applications, but converted by the agency's Explosive Ordnance Disposal (EOD) experts, the X-Ray Toolkit (XTK) software application can be used by field responders and NNSA Laboratory experts to acquire, process and analyze X-ray images obtained during a potential nuclear terrorism incident, said the agency. The software was developed by NNSA's Emergency Operations technology integration program and implemented by its stabilization program, it said. The NNSA is a semi-autonomous agency operating within the Department of Energy charged with responding to nuclear disasters and emergencies in the U.S. and abroad, among other duties. "We have received overwhelmingly positive feedback about the XTK software from our operational partners across the nation," said Joseph Krol, NNSA associate administrator for emergency operations in a statement. "The application of state-of-the-art technical products to the nuclear counterterrorism mission is a central part of NNSA's mission and an important aspect of our vision for this program. It also showcases our ability to leverage six decades of nuclear security expertise into a product that can be used by first responders from coast to coast." XTK, explained the NNSA statement, was designed for joint use by EOD and NNSA Laboratory personnel during nuclear "render safe" operations, where specialized procedures, methods and tools can prevent the detonation of a nuclear device. Render Safe aims to safely recover and secure radiological devices, or lost or stolen U.S. nuclear weapons in support of federal, state, and local authorities using a team of NNSA special response units. It also provides for Radiological Triage--24-hour support to analyze data and confirm the identities of the radioisotopes in question. XTK provides for the intuitive and efficient transfer of data from the site of a potential incident to NNSA Laboratories, allowing



seamless transfer of critical information from field responders to NNSA nuclear security experts during a crisis situation, said the agency. Sandia National Laboratories worked closely with NNSA Emergency Operations personnel during the development, testing, and training phases of this project. Additional information for XTK development was obtained from NNSA response team members, FBI Special Agent Bomb Technicians, Department of Defense EOD experts and numerous state and local responders, it said.

Can PAKISTAN destroy INDIA?

Posted in the India Forum
Source: http://www.topix.com/forum/world/india/TJOTSAA217FIIKL9R

I know it is not an answer that would be welcomed by many Indians and in rage and frustration they would lash out at the person who has issued this thread but really, try and reason it our yourselves if such a threat exists and you are deliberately not looking in that corner or doing the right introspection?

This morning I read in The Times of India the following QUOTE:

The terrorist was supposed to be in Delhi to carry out an attack on the National Defence College (NDC) at Tees January Marg -- a target recommended by US-born Lashkar terrorist David Coleman Headley to his bosses on the basis that a strike on the institution would have killed more Indian Army officers than those who died in all Indo-Pak wars put together.

UNQUOTE
Read more: Visa denial saved Delhi from major LeT strike - The Times of India http://timesofindia.indiatimes.com/india/I-fi...

We never imagined that Pakistan will orchestrate Kargil snatch from us? We never imagine that Pakistan will organize the deadliest attack as we saw in Bombay Massacre? We never imagined that with one blow they will wipe out the elected leaders of India by bombing the parliament?

So, it is clear that a weak Pakistan is capable of bringing us to our knees. Yet, with impunity we are not doing anything about it. What has been bothersome to me for quite some time is the nuclear terrorism that can be unleashed upon India with no visible hand of any state. Some Jihadi organisations or lone loony toon decides to hit us with what we call "dirty Bomb" Often called a weapon of mass disruption, not destruction and can be assembled by a determined mind/s easily. Conventional explosives are used to spread radioactive material -- causes far fewer casualties than a nuclear explosion. But because such devices are easier to assemble and the ingredients are readily available, government officials and terrorism experts worldwide consider a dirty-bomb attack more likely than a terrorist nuclear strike. There have been several alleged attempts to carry out a dirty-bomb attack.

- In June 2002, U.S. authorities arrested Jose Padilla, a former gang member from Brooklyn, on charges of plotting a dirty-bomb strike in the United States on behalf of al Qaeda.
- December 2003, the US Department of Energy dispatched scores of nuclear scientists with sophisticated detection equipment to scour several major cities for radiological bombs.
- In September 2004, British police arrested four men suspected of plotting to set off a dirty bomb in London.

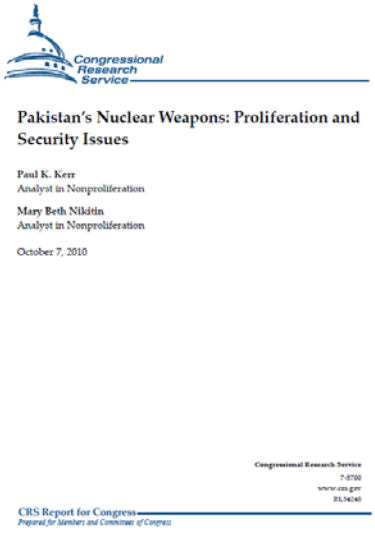
Americium, which is found in smoke detectors, is one of eight types of radioactive sources suitable for bombs. Four sources cause external injuries to skin and eyes, and three others, plus americium, can cause extensive internal damage, as well. Terrorists would need less than a gram of any one of the sources to build a dirty bomb, but the trace amounts found in everyday products are so minuscule that plotters would need more than 1 million smoke detectors to get enough americium for a weapon. US Officials and experts agree the damage would be more psychological than lethal. "The real effects

would be economic shutdown due to contamination, as well as the social and psychological fear created,"! I am not an expert on nuclear terrorism and have assembled this information from an article published in The Washington Post many years ago but the threat prevails right until today and its a miracle that it has not happened so far. Simply look at the pattern of the Pakistani strikes ! They are thinking BIG ! Big to hit India hard so that it stays HIT ! Imagine they wanted to wipe out (LeT) our National Defence College in New Delhi ? Wiping out more officers than killed in our wars so far???

Pakistan's Nuclear Weapons: Proliferation and Security Issues

Source: www.fas.org/sgp/crs/nuke/RL34248.pdf

Pakistan's nuclear arsenal consists of approximately 60 nuclear warheads, although it could be larger.


Congressional Research Service

Pakistan's Nuclear Weapons: Proliferation and Security Issues

Paul K. Kerr
Analyst in Nonproliferation

Mary Beth Nikitin
Analyst in Nonproliferation

October 7, 2010

Congressional Research Service
7-5700
www.crs.gov
RL34248

CRS Report for Congress
Prepared for Members and Committees of Congress

Islamabad is producing fissile material, adding to related production facilities, and deploying additional delivery vehicles. These steps will enable Pakistan to undertake both quantitative and qualitative improvements to its nuclear arsenal. Whether and to what extent Pakistan's current expansion of its nuclear weapons-related facilities is a response to the 2008 U.S.-India nuclear cooperation agreement is unclear. Islamabad does not have a public, detailed nuclear doctrine, but its "minimum credible deterrent" is widely regarded as primarily a deterrent to Indian military action.

Pakistan has in recent years taken a number of steps to increase international confidence in the security of its nuclear arsenal. In addition to dramatically overhauling nuclear command and control structures since September 11, 2001, Islamabad has implemented new personnel security programs. Moreover, Pakistani and some U.S. officials argue that, since the 2004 revelations about a procurement network run by former Pakistani nuclear official A.Q. Khan, Islamabad has taken a number of steps to improve its nuclear security and to prevent further proliferation of nuclear-related technologies and materials. A number of important initiatives, such as strengthened export control laws, improved personnel security, and international nuclear security cooperation programs have improved Pakistan's security situation in recent years. Instability in Pakistan has called the extent and durability of these reforms into question. Some observers fear radical takeover of a government that possesses a nuclear bomb, or proliferation by radical sympathizers within Pakistan's nuclear complex in case of a breakdown of controls. While U.S. and Pakistani officials continue to express confidence in controls over Pakistan's nuclear weapons, continued instability in the country could impact these safeguards.

Electromagnetic pulse impact far and wide

Source: http://www.usatoday.com/tech/science/2010-10-26-emp_N.htm

The sky erupts. Cities darken, food spoils and homes fall silent. Civilization collapses. End-of-the-world novel? A video game? Or could such a scenario loom in America's future?

There is talk of catastrophe ahead, depending on whom you believe, because of the threat of an electromagnetic pulse triggered by either a supersized solar storm or terrorist A-bomb, both capable of disabling the electric grid that powers modern life. Electromagnetic pulses (EMP) are oversized outbursts of atmospheric electricity. Whether powered by geomagnetic storms or by nuclear blasts, their resultant intense magnetic fields can induce ground currents strong enough to burn out power lines and electrical equipment across state lines. The threat has even become political fodder, drawing warnings from former House speaker Newt Gingrich, a likely presidential contender. "We are not today hardened against this," he told a Heritage Foundation audience last year. "It is an enormous catastrophic threat." Meanwhile, in Congress, a "Grid Act" bill aimed at the threat awaits Senate action, having passed in the House of Representatives.

Fear is evident. With the sun's 11-year solar cycle ramping up for its stormy maximum in 2012, and nuclear concerns swirling about Iran and North Korea, a drumbeat of reports and blue-ribbon panels center on electromagnetic pulse scenarios. "We're taking this seriously," says Ed Legge of the Edison Electric Institute in Washington, which represents utilities. He points to a North American Electric Reliability Corp. (NERC) report in June, conducted with the Energy Department, that found pulse threats to the grid "may be much greater than anticipated." There are "some important reasons for concern," says physicist Yousaf Butt of the Harvard-Smithsonian Center for Astrophysics in Cambridge, Mass. "But there is also a lot of fluff." At risk are the more than 200,000 miles of high-voltage transmission lines that cross North America, supplying 1,800 utilities the power for TVs, lights, refrigerators and air conditioners in homes, and for the businesses, hospitals and police stations that take care of us all. "The electric grid's vulnerability to cyber and to other attacks is one of the single greatest threats to our national security," Rep. Ed Markey, D-Mass., said in June as he introduced the bill to the House of Representatives. Markey and others point to the August 2003 blackout that struck states from Michigan to Massachusetts, and southeastern Canada, as a sign of the grid's vulnerability. Triggered by high-voltage lines stretched by heat until they sagged onto overgrown tree branches, the two-day blackout shut down 100 power plants, cut juice to about 55 million people and cost $6 billion, says the 2004 U.S.-Canada Power System Outage Task Force. Despite the costs, most of them from lost work, a National Center for Environmental Health report in 2005 found "minimal" death or injuries tied directly to the 2003 blackout — a few people died in carbon monoxide poisonings as a result of generators running in their homes or from fires started from candles. But the effects were pervasive: Television and radio stations went off the air in Detroit, traffic lights and train lines stopped running in New York, turning Manhattan into the world's largest pedestrian mall, and water had to be boiled after water mains lost pressure in Cleveland. Simple physics, big worry! The electromagnetic pulse threat is a function of simple physics: Electromagnetic pulses and geomagnetic storms can alter Earth's magnetic field. Changing magnetic fields in the atmosphere, in turn, can trigger surging currents in power lines. "It is a well-understood phenomenon," says Butt, who this year reviewed geomagnetic and nuke blast worries in The Space Review. Two historic incidents often figure in the discussion:

• On July 9, 1962, the Atomic Energy Commission and the Defense Atomic Support Agency detonated the Starfish Prime, a 1.4-megaton H-bomb test at an altitude of 250 miles, some 900 miles southwest of Hawaii over the Pacific Ocean. The pulse shorted out streetlights in Oahu.
• On March 9, 1989, the sun spat a million-mile-wide blast of high-temperature charged solar gas straight at the Earth. The "coronal mass ejection" struck the planet three days later, triggering a geomagnetic storm that made the northern lights visible in Texas. The storm also induced currents in Quebec's power grid that knocked out power for 6 million people in Canada and the USA for at least nine hours.

"A lot of the questions are what steps does it make sense to take," Legge says. "We could effectively gold-plate every component in the system, but the cost would mean that people can't afford the rates that would result to pay for it." "The high-altitude nuclear-weapon-generated electromagnetic pulse is one of a small number of threats that has the potential to hold our society seriously at risk," concluded a 2008 EMP Commission report headed by William Graham, a former science adviser to President Reagan.

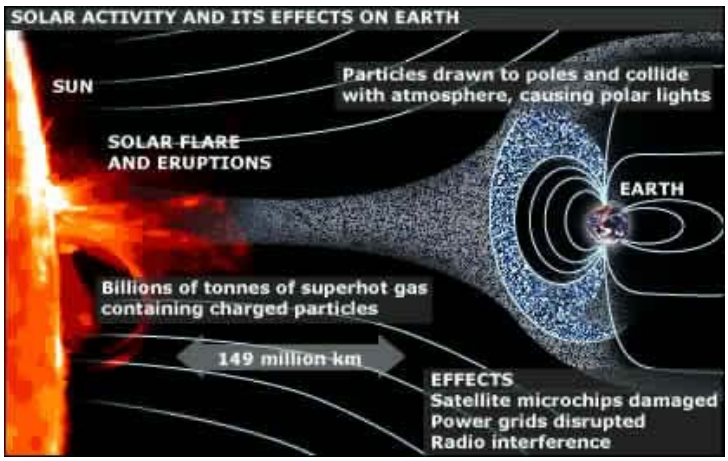
The terror effect

In the nuclear scenario, the detonation of an atomic bomb anywhere from 25 to 500 miles high electrifies, or ionizes, the atmosphere about 25 miles up, triggering a series of electromagnetic pulses. The pulse's reach varies with the size of the bomb, the height of its blast and design. Gingrich last year cited the EMP Commission report in warning, "One weapon of this kind that went off over Omaha would eliminate most of the electrical production in the United States." But some take issue with that. "You

would really need something the size of a Soviet H-bomb to have effects that cross many states," Butt says. The massive Starfish Prime blast, he notes, was at least 70 times more powerful than the atomic bomb detonated over Hiroshima in 1945, and it may have blown out streetlights but it left the grid in Hawaii intact. One complication for rogue nations or terrorists contemplating a high-altitude nuclear blast is that such an attack requires a missile to take the weapon at least 25 miles high to trigger the electromagnetic pulse. For nations, such a launch would invite massive nuclear retaliation from the USA's current stockpile of 5,000 warheads, many of them riding in submarines far from any pulse effects. Any nation giving a terror group an atomic weapon and missile would face retaliation, Butt and others note, as nuclear forensics capabilities at the U.S. national labs would quickly trace the origins of the bomb, Butt says. "It would be suicide."

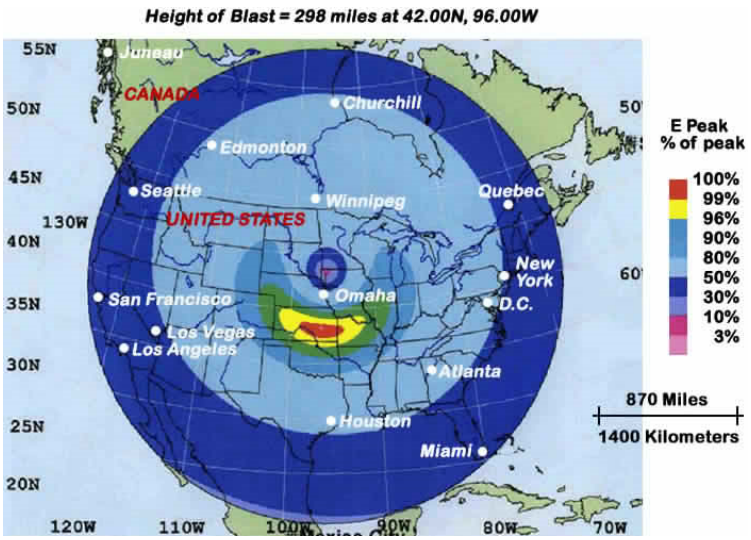
Super solar storm

On the solar front, the big fear is a solar super storm, a large, fast, coronal mass ejection with a magnetic field that lines up with an orientation perfectly opposite the Earth's own magnetic field, says solar physicist Bruce Tsurutani of NASA's Jet Propulsion Laboratory in Pasadena, Calif. Tsuritani and other solar physicists view such an event as inevitable in the next 10 to 100 years. "It has to be the perfect storm," Tsuratani says. "We are almost guaranteed a very large solar storm at some point, but we are talking about a risk over decades," Butt says. Three power grids gird the continental U.S. — one crossing 39 Eastern states, one for 11 Western states and one for Texas.



Solutions?

In June, national security analyst Steven Aftergood of the Federation of American Scientists described congressional debate over power-grid security as "a somewhat jarring mix of prudent anticipation and extravagant doomsday warnings." Although the physics underlying the geomagnetic and nuclear pulses are fundamentally the same, they have different solutions. A geomagnetic storm essentially produces a long-building surge dangerous to power lines and large transformers. A nuclear blast produces three waves of pulses. Limiting the risk from the geomagnetic-storm-type threat involves stockpiling large transformers and installing dampers, essentially lightning rods, to dump surges into the ground from the grid. Even if such steps cost billions, the numbers come out looking reasonable compared with the $119 billion that a 2005 Electric Power Research Institute report estimated was the total nationwide cost of normal blackouts e very year. "EMP is one of a small number of threats that can hold our society at risk of catastrophic consequences," Graham testified to a congressional committee last year, endorsing



such mitigation steps. Stephen Younger, former head of the Defense Threat Reduction Agency, last year argued against the catastrophic scenarios in his book, The Bomb, suggesting the effects of a pulse would be more random, temporary and limited than Graham and others suggest. The June NERC report essentially calls for more study of the problem, warning of excessive costs to harden too much equipment against the nuclear risk. "If there are nuclear bombs exploding, we have lots of really, really big problems besides the power grid," Legge says.

Researchers Propose Method to Sniff Out Dirty Bombs Via The Electromagnetic Breakdown Of Air

Source: http://www.medicalnewstoday.com/articles/207198.php

Researchers at the University of Maryland have proposed a scheme for detecting a concealed source of radioactive material without searching containers one by one. Detection of radioactive material concealed in shipping containers is important in the early prevention of "dirty" bomb construction. The concept, described in the Journal of Applied Physics, is based on the gamma-ray emission from the radioactive material that would pass through the shipping container walls and ionize the surrounding air. The facilitated breakdown of the air in a focused beam of high-power, coherent, terahertz or infrared radiation would then be an indicator of the presence of the radioactive material. The gamma rays coming through the container walls could be detected by a pulsed electromagnetic source of duration between 10 ns to microseconds. The team evaluated several candidate sources for this detection, including a 670-GHz gyrotron oscillator with 200-kW, 10-μs output pulses and a TEA CO2 laser with 30-MW, 100-ns output pulses. A system based on the 670-GHz gyrotron would have enhanced sensitivity and a range exceeding 10 m. "It is not yet clear whether this approach to detection of nuclear material is practical," says first author professor Victor Granatstein, "but it is worth pursuing since it might impact an important need related to National Security."

Is An Apocalyptic Vision Driving Al-Qaeda's Quest for the Bomb?

Source: http://www.globalsecurity.org/security/library/news/2010/12/sec-101203-rferl01.htm

Do we "get" Al-Qaeda and its goals? Nearly a decade after the 9/11 attacks, a succession of less spectacular but nonetheless traumatic subsequent outrages, and a bloody and expensive "war on terror" that has extracted a fearful price in life and treasure in Iraq and Afghanistan, it seems hard to accept that there could be any misunderstanding or underestimation of the threat posed. Yet Rolf

Mowatt-Larssen, who headed the Central Intelligence Agency's counterterrorism weapons of mass destruction (WMD) department during President George W. Bush's administration, thinks that may be happening. Now a senior fellow at Harvard University's Belfer Center for Science and International Affairs, Mowatt-Larssen has become increasingly pre-occupied by a recurring nightmare — of a nuclear-armed Al-Qaeda. A year of close study of the pronouncements of Al-Qaeda's leader, Osama bin Laden, and particularly those of his deputy, Ayman Al-Zawahiri, has convinced him that acquiring an atomic bomb, or a device of comparable destructiveness, is definitely the group's mission. The purpose, he says, is not that of deterrence, defense, or even straightforward military attack. The Islamist group seeks nothing less than the apocalyptic goal of transforming the planet to usher in a new dawn of Islamic-ruled social justice in place of the "American-Zionist conspiracy," which, according to Al-Qaeda, currently prevails. "Bin Laden and Zawahiri, if they were just worrying about achieving things through military effects, fighting a war or battles, they probably wouldn't bother with these kinds of weapons that are extremely difficult to get and are then unpredictable in their use," Mowatt-Larssen says. "But they're trying to change the world and I think

some people forget that they have these very, very serious ambitions that are very deeply religiously based for which using these weapons is almost essential."

Explicit Evidence

Mowatt-Larssen says he embarked on his study with an open mind — but even after years in the intelligence community, was deeply sobered by what he found. "I didn't take for granted what I read in the intelligence cables about Al-Qaeda's intent as far as it goes. I really wanted to understand what they're doing," he explains. "I went into my research quite receptive to coming out with all kinds of different conclusions. The essence of what I feel I've learned is that it's more frightening than I thought because I think the intent is much deeper. It's a very strong recognition of what they (WMD) could do for them in achieving these goals I've referred to. The essentiality of changing the world, not just fighting an endless battle for the sake of proving to their god that they are in fact carrying out his will as they see it. No, it's much more than that. They believe they can win." At the core of Mowatt-Larssen's conviction — set out in a recent article in "Foreign Policy" magazine and a longer piece for the Belfer Center — are arguments advanced by Zawahiri in a 2008 book, "Exoneration - A Treatise Exonerating the Community of the Pen and the Sword from the Debilitating Accusation of Fatigue and Weakness." In it, Zawahiri repeated approvingly the words of a fatwa pronounced in 2003 by a radical Muslim cleric, Nasir al-Fahd, which is widely seen as a trail-blazing religious treatise endorsing the use of WMD.

> He's [Zawahiri] talking about raising jihad to a qualitatively completely new level which requires, as he says himself, a completely different kind of justification than even 9/11.

Fahd's fatwa, which Mowatt-Larssen says was originally commissioned by Zawahiri, makes three leading arguments for using the weapons, including the particularly callous one that women and children "may be killed as collateral" if "one cannot distinguish them [from the main fighters]." Even more chillingly, Zawahiri quotes Fahd in writing: "If a bomb were dropped on them, destroying 10 million of them and burning as much of their land as they have burned of Muslim land, that would be permissible without any need to mention any other proof." There could be no more explicit evidence, in Mowatt-Larssen's view, of Zawahiri and Al-Qaeda's determination to get their hands on a nuclear bomb. "Everywhere I discussed that, everyone saw that for what it was," he says, "which was an explicit expression of intent to use weapons of mass destruction, probably nuclear. What's interesting about 'Exoneration' is that he [Zawahiri] essentially plagiarizes everything from the 2003 fatwa to make a case. I don't think that's an extrapolation. And if you read the substance of his assertions, he can't kill 10 million people by flying airplanes into buildings. He's talking about raising jihad to a qualitatively completely new level which requires, as he says himself, a completely different kind of justification than even 9/11." Mowatt-Larssen's is not exactly a voice in the wilderness. In April 2010, addressing a 47-nation summit on nuclear terrorism in Washington, President Barack Obama, identified the possibility of a terrorist group obtaining atomic weapons as the single biggest threat to U.S. security. "We know that organizations like Al-Qaeda are in the process of trying to secure a nuclear weapon — a weapon of mass destruction that they would have no compunction in using," Obama said. "This is something that could change the security landscape of this country and around the world for years to come." Yet as Mowatt-Larssen acknowledges, there is no evidence that Al-Qaeda is remotely close to getting its hands on such devastating devices, and the probability of it doing so remains low.

Negligible Threat

Furthermore, some seasoned Al-Qaeda-watchers believe the nuclear threat is negligible compared with the possibility of the group carrying out further conventional attacks. Brynjar Lia, an analyst at the

private Norwegian Defense Research Establishment, believes Zawahiri's real goal in 'Exoneration' was to refute Islamist criticism of Al-Qaeda's tactics rather than to justify nuclear weapons. "'Exoneration' was written at a time when Al-Qaeda faced public-relations crises," says Lia. "There were mounting criticisms of its attacks on civilian targets and the fact that more Muslims were killed as a result of Al-Qaeda operations than Westerners and so-called 'Crusaders.' So I think in terms of providing more legitimacy for mass-casualty attacks, one might say that Ayman al-Zawahiri's treatise is a contribution to trying to do that. But I'm not sure that it adds much to our knowledge about Al-Qaeda's intentions in terms of weapons of mass destruction."

Economic Blood-Letting

Denied the safe haven it once had under the Taliban in Afghanistan, Lia argues, Al-Qaeda simply lacks the capacity to develop a nuclear capability. It is now more intent on a strategy of survival coupled with a war of attrition in the form of conventional attacks that it hopes will bleed the West economically, he says. "We did a fairly thorough survey of on-line training and instruction manuals on chemical and biological and radiological devices and also other writings on nonconventional weapons to try to measure Al-Qaeda's interest in these types of weapons," Lia continues. "It's fairly clear that this is a very small literature compared to their interest in conventional weapons and conventional means of warfare and terrorism. And also, when you look more closely at these training manuals, they are very crude, their recipes don't even work. So our impression is that their capacity in this field is very low." The trouble, counters Mowatt-Larssen, is that too many Western intelligence agencies share this assessment — at the risk of being blindsided one day by Al-Qaeda's well-demonstrated capacity for surprise attacks. "I do worry that the intelligence community, not just in the United States but globally, feels that the more likely threats are conventional," he says. "The things we're worried about now logically are things like packages from Yemen and underwear bombers and shoe bombers and European threats. I don't want to diminish the importance of those threats, because they are real. But at the same time, I urge my colleagues not to forget the other side of the [football] field. Somebody could throw a long pass down there and beat our entire defense on a major attack that would be unconventional, like a nuclear or biological weapons attack, and [we need to] take those seriously as well.'"

Threat As A Weapon

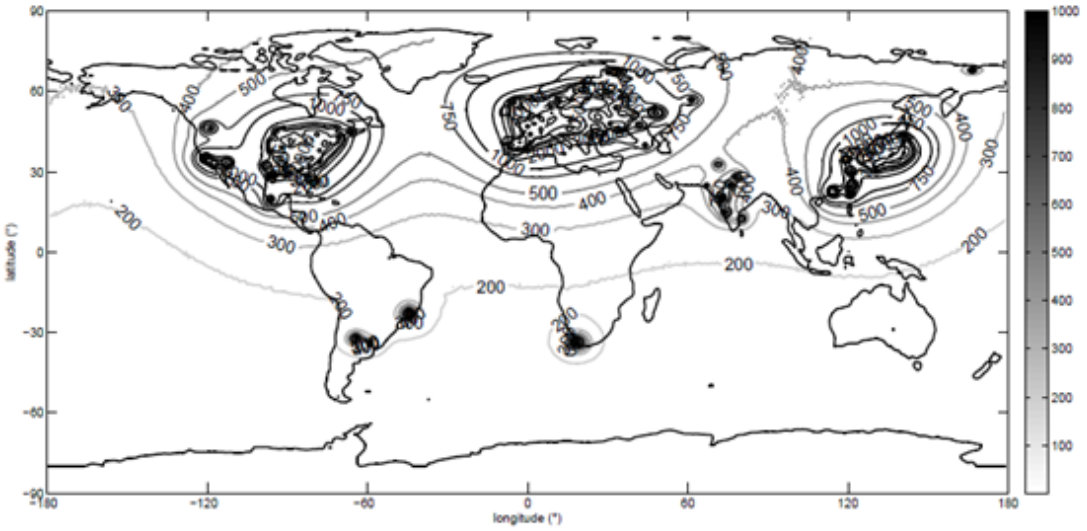
If it all seems alarmist and improbable to the ordinary citizen, it is not to Professor Gabriel Weimann, a professor of communications at Haifa University in Israel, who has spent years monitoring 7,600 websites and chat-room of violent militant groups across the world, including Al-Qaeda and its affiliates. Intensive study shows Al-Qaeda is obsessed with carrying out an attack that will surpass 9/11 in horror and magnitude, Weimann says. That ambition has corresponded with an increase in the volume of threats to use a nuclear bomb and other destructive weapons, including cyber terrorism. While Weimann says it is impossible to assess how realistic such threats are, he echoes Mowatt-Larssen in warning that their importance lies in the fact they are made, not least because it has the effect of spreading psychological terror. "How authentic are those threats? I'm not in a position to tell," Weimann admits. "When they discuss using weapons of mass destruction or cyber terrorism, for example, how close are they to really operating? Are they just talking about it, are they just aiming at psychological warfare, or are they really doing it? I'm not sure that I can really tell from the websites. But the basic step that they do consider it, that they do plan it, that they do disseminate information and try to show that they are acquiring the know-how is already demonstrating their eagerness to do it, their willingness to find information about it. And I think these are already quite alarming signals."

Spotting illicit nuclear activity from a distance

Source: http://homelandsecuritynewswire.com/spotting-illicit-nuclear-activity-distance

French scientists unveil a plan to place antineutrino detectors off the coast of rogue nations suspected of operating clandestine nuclear reactors; their idea is to turn a supertanker into an antineutrino detector by kitting it out with the necessary photon detectors and filling it with 10^34 protons in the form of 138,000 tons of linearalkylbenzene (C13 H30); the plan is to sink the tanker in up to four kilometers of

water off the coast of a rogue state, and the supertanker would then watch for the telltale signs of undeclared antineutrino activity. One of the thornier problems facing the international community is to monitor the spread of nuclear technology and prevent it spreading to rogue regimes. This task falls to the International Atomic Energy Authority (IAEA) based in Vienna and it is not an easy task. This is why the IAEA is exploring various new technologies for monitoring nuclear reactors at a distance. Technology Review reports that these technologies fall into two categories. Near-field devices must sit within a few tens of meters of a reactor to do their job. Look at this promising example of such a device,



developed two years ago at the Lawrence Livermore National Laboratory in California. By contrast, far-field technologies can do the same job from much further afield. The goal here is to spot clandestine reactors in other countries. How might far-field sensors work? Thierry Lasserre of the French Alternative Energies and Atomic Energy Commission and a few colleagues offer an answer. First, a little background. Fission reactors are prodigious sources of antineutrinos. A gigawatt-sized reactor produces some 10^21 antineutrinos each second. By that measure, these reactors light up like Christmas trees. The trouble is that antineutrinos interact only very weakly with ordinary matter so spotting these particles is hard. They can be detected, though, given large enough volumes of matter. The standard technique is to fill a giant swimming pool with water and wait for an antineutrino to smash into a proton, generating a positron and a neutron. The positron produces Cherenkov radiation which can be picked up by light detectors around the pool. Technology Review notes that in principle, a large enough detector could pick up the signal produced by any reactor — but there is a caveat. In analyzing the data from this detector, physicists would have to be able to screen out any background signal. This is tricky because there are numerous sources of noise. These fall into two main classes. First, there are the many legal reactors working around the world which are luminous beacons of antineutrinos themselves. These would all have to be taken into account when analyzing the signal. Then there is the Earth itself, which is full of radioactive stuff that wreaks of antineutrinos. These too would have to be subtracted from the measured signal. Lasserre and colleagues are equal to this task. Their idea is to turn a supertanker into an antineutrino detector by kitting it out with the necessary photon detectors and filling it with 10^34 protons in the form of 138,000 tons of linearalkylbenzene (C13 H30). They call this detector a SNIF (a Secret Neutrino Interactions Finder). The plan is to sail the supertanker to the coast of a suspicious state and temporarily sink it in up to four kilometers of water. The supertanker would then watch for the telltale signs of undeclared antineutrino activity. Lasserre and coll;eagues have even calculated what kind of background signal their detector is likely to see and what a suspicious signal would look like from an undeclared reactor placed in various locations, such as on an island, a peninsula or a flat shore. “Our study attests that 138,000 ton neutrino detectors have the capability to detect and even localize clandestine reactors from across borders,” they say. They also acknowledge, however, that such a detector would present formidable practical, political, and technological challenges. Whether or not we will ever see such a device in action is an interesting question, which is not as easy to answer as the mind-boggling complexities of the task might suggest.

"One interesting clue is that Lasserre and co say that near-field devices are already being tested in Brazil, France, Italy, Japan, Russia, and the United States. That suggests a significant interest in nuclear monitoring technology," TR concludes.

—Read more in Thierry Lasserre et al, "SNIF: A Futuristic Neutrino Probe for Undeclared Nuclear Fission Reactors" arXiv:1011.3850v1 [nucl-ex] (16 November 2010)

CBRNE-TERRORISM Newsletter

Δελτίο ΧΒΡΠΕ-ΤΡΟΜΟΚΡΑΤΙΑΣ

Volume 5 - 2010

EXPL –News

Personal protection equipment Uniform bomb suits standard being developed

Source: http://homelandsecuritynewswire.com/uniform-bomb-suits-standard-being-developed

Several federal agencies are now working with first responders to create the first nationwide standard for minimum bomb suit performance requirements; having a standard will give some assurance of quality to DHS and other agencies that award grants to bomb squads for equipment purchases; if the standard is adopted, DHS will change its g-rants process to ensure awards are spent on bomb suits that meet the requirements. Federal agencies are looking to protect the first responders and soldiers who check out and defuse potentially explosive devices with improved bomb suits. These bulky protective suits worn by bomb technicians essentially serve as the only defense they have should a device go boom. Bomb suit manufacturers run tests on their protective suits to ensure they can withstand an explosion, but there currently is no single set of requirements that the suits must meet before they can be sold. echNewsDaily reports that several federal agencies are now working with first responders to create the first nationwide standard for minimum bomb suit performance requirements. "The bomb suit is such an important piece of equipment that a standard and certification program was needed to ensure a bomb technician's safety," said Martin Hutchings, a retiree of the Sacramento County, California sheriff's department bomb squad and the National Institute of Standards and Technology liaison to the National Bomb Squad Commanders Advisory Board. To develop the standard, federal agencies first researched the most common types of explosives bomb squads encounter, according to Philip Mattson, deputy director of the Office of Standards at DHS's Science and Technology Directorate (S&T) Test & Evaluation and Standards Division. Personnel at the U.S. Army Natick Soldier Research Development and Engineering Center blew up, burned, and projected fragments at suits to determine what kinds of tests the suits would need to pass to ensure they protect bomb technicians adequately.

The new drafted standard contains requirements for:

- cushioning the spine and head during impact;
- blast and thermal heat protection;
- freedom of motion to work efficiently;
- maximum weight restrictions;
- rapid removal, such as for emergency medical treatment;

- freedom of motion (allowing sufficient dexterity to pick up a coin from the ground); and
- defogger performance to prevent the helmet visor from clouding.

Having a standard will give some assurance of quality to DHS and other agencies that award grants to bomb squads for equipment purchases, according to Mattson. If the standard is adopted, DHS will change its grants process to ensure awards are spent on bomb suits that meet the requirements. The groups that worked to develop the standard hope it will be adopted by the end of 2010, and afterwards the standards will be reviewed every three to five years to ensure they meet the current needs of first responders. "When it comes to a bomb suit, the practitioner's life depends on the quality of that garment," said Debra Stoe, senior program operations specialist and physical scientist at the National Institute of Justice.

New TNT detector 1,000 more sensitive than sniffer dogs

Source: http://homelandsecuritynewswire.com/new-tnt-detector-1000-more-sensitive-sniffer-dogs

Israeli researchers develop an explosives detector that can detect extremely small traces of commonly used explosives in liquid or air in a few seconds; the device is a thousand times more sensitive than the current gold standard in explosives detection: the sniffer dog

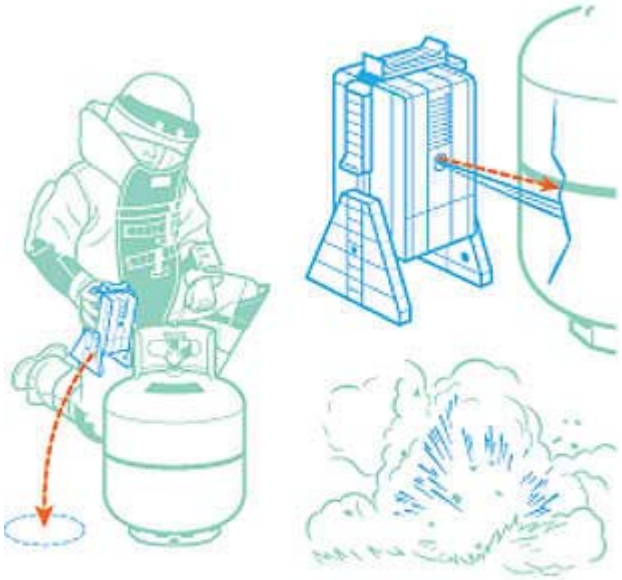
To thwart possible terrorist attacks and to detect contamination on sites of former military installations, researchers have been concentrating their efforts in recent years on methods for the detection and analysis of explosives. Fernando Patolsky and his team at the University of Tel Aviv have now developed a novel sensor chip that detects trinitrotoluene (TNT), as well as other explosive species, with high sensitivity and without a concentration step. As the Israeli researchers report in the journal Angewandte Chemie, their detector is superior to sniffer dogs and all other previous detection methods for this explosive. The difficulty with the detection of explosives such as TNT is their extremely low volatility. Methods available for the analysis of air samples are expensive and time-consuming, and require large, bulky instruments, laborious sample preparation, and expert handling. "There is a need for an inexpensive, miniaturizable method that allows for quick, easy, and robust high-throughput analysis in the field," says Patolsky. The scientists built their sensor using the principle of a nanoscale field-effect transistor. In contrast to a current-controlled classical transistor, a field-effect transistor is switched by means of an electric field. At the core of the device are nanowires made of the semiconductor silicon. These were coated with a molecular layer made from special silicon compounds that contains amino groups (NH_2). TNT molecules bind to these amino groups in the form of charge-transfer complexes. The binding process involves the transfer of electrons from the electron-rich amino groups to the electron-poor TNT. This change in the charge distribution on the surface of the nanowires modulates the electric field and leads to an abrupt change in the conductivity of the nanowires, which is easily measured. To improve the signal-to-noise ratio and thus increase the sensitivity, the scientists equipped their chip with an array of about 200 individual sensors. "We are thus able to analyze liquid and gaseous samples without prior concentration or other sample preparation at previously unattainable sensitivities," says Patolsky. "We were able to analyze concentrations down to 0.1 ppt (parts per trillion); that is, one molecule of TNT in 10 quadrillion other molecules." The sensor can be quickly regenerated by washing and is selective for TNT; other related molecules do not react the same way. "We are now creating a chip based on large arrays of nanosensors chemically modified with a large number of chemical receptors, with different binding capabilities, in order to detect a whole spectrum of explosive species in parallel," says Patolsky. Prachi Patel writes in Technology Review that the nanowire array is not the first device to achieve canine levels of explosive-sniffing sensitivity. A system developed by ICx Technologies, based in Arlington, Virginia, can detect vapors given off by explosives with a sensitivity matching that of a canine nose. Instead of nanowires, the ICx system uses polymers that glow or stop glowing in response to traces of explosive in a vapor in a few seconds. This device is being used in battlefields in Iraq and Afghanistan, and the U.S. Transportation Security Administration (TSA) recently started using it at airports, but most airports still rely on microwave oven-sized instruments that take minutes, rather than seconds, to detect explosives in swabs taken from luggage or passengers' skin.

The new Tel Aviv University device is a thousand times more sensitive than any existing detector, including the ICx device. The researchers have used it to detect TNT and the plastic explosives RDX and PETN at concentrations lower than one part per trillion in a few seconds. MIT chemistry professor Timothy Swager agrees, pointing out that currently the array only works convincingly when detecting explosives in a solution. It is less effective at picking out vapors of explosives from a person's skin or belongings, he says, noting that the array works best when TNT vapor-containing air samples are blown directly at the nanowires. Harvard University chemistry professor Charles Lieber says that the nanowire sensor approach is much more sensitive than the ICx polymer technology, which was developed in Swager's lab, but it has not yet been proven the way the ICx technology has. Lieber, who focuses on biomedical applications of nanowire transistors, says the Israeli research shows that nanowire sensing could be applied for explosives detection and could be readily commercialized. "There are no limitations to the methodology from my perspective…it has potential to revolutionize explosives detection."

Sandia Labs developed an IED-disabling water-blade device

Source: http://homelandsecuritynewswire.com/sandia-labs-developed-ied-disabling-water-blade-device

A device developed by Sandia National Laboratories researchers that shoots a blade of water capable of penetrating steel is headed to U.S. troops in Afghanistan to help them disable deadly IEDs; the portable clear plastic device is filled with water and an explosive material is placed in it that, when detonated, creates a shock wave that travels through the water and accelerates it inward into a concave opening; when the water collides, it produces a thin blade. A device developed by Sandia National Laboratories researchers that shoots a blade of water capable of penetrating steel is headed to U.S. troops in Afghanistan to help them disable deadly improvised explosive devices, or IEDs — the No. 1 killer and threat to troops in Afghanistan, according to the Pentagon. Sandia licensed the patent-pending technology to a small minority-owned business, Albuquerque, New Mexico-based TEAM Technologies Inc. The company made its first shipment of about 3,000 new water disruptors to Afghanistan this summer. "The fluid blade disablement tool will be extremely useful to defeat IEDs because it penetrates the IED extremely effectively," said Greg Scharrer, manager of the Energetic Systems Research Department at Sandia. "It's like having a much stronger and much sharper knife." Soldiers who had served in Afghanistan and Iraq field-tested the device during training at the federal laboratory and suggested improvements while the product was being developed. The fluid blade disablement tool was invented by Steve Todd, a mechanical and materials engineer with extensive Navy experience fighting IEDs, Chance Hughs, a retired Navy SEAL explosives expert on contract to Sandia, and mechanical engineer Juan Carlos Jakaboski in Sandia's Energetic Systems Research Department for a National Nuclear Security Administration sponsor. The portable clear plastic device is filled with water and an explosive material is placed in it that, when detonated, creates a shock wave that travels through the water and accelerates it inward into a concave opening, Todd said. Therefore, when the water collides, it produces a thin blade. "That allows you to have a high-speed, very precise water blade to go through and do precision type of destruction on whatever improvised explosive device it's going up against. Immediately behind the



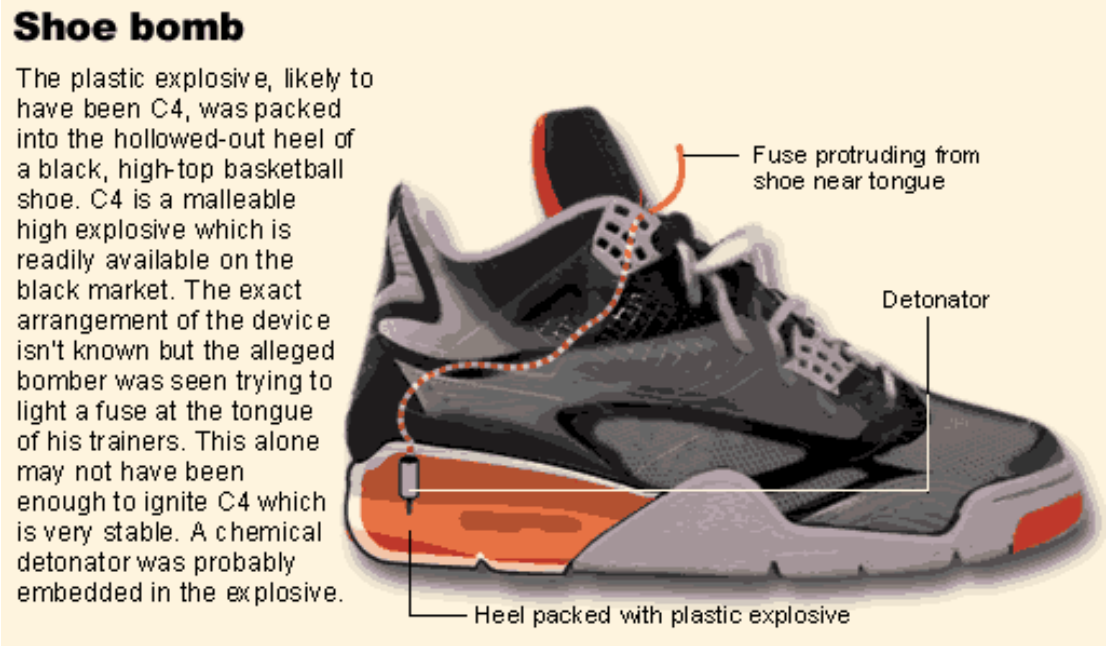
precision water blade is a water slug, which performs a general disruption that tears everything apart," Todd said. Unlike traditional explosives, which release energy equally in all directions when they go off, researchers use shaped-charge technology to deliberately manipulate the explosives so that they create a certain shape when they explode, allowing the operator to focus the energy precisely where it's needed. The inventors of the fluid blade disablement tool took a different tack. Rather than changing the shape of the explosive, Todd, Hughs and Jakaboski used an explosive modeling tool to figure out

how to change the shape of the water when designing the water disruptors. "We're putting the explosive in a flat tray and we're shaping the water," Scharrer said. The process happens in microseconds and can't be captured by the human eye, so researchers used computer simulation and high-speed flash X-rays, which can view the interior of imploding high-explosive devices and record the motion of materials moving at ultrahigh speeds, to fine tune the design. They also used another approach. Soldiers rotating out of Afghanistan and Iraq worked hand-in-hand with researchers and developers to test the device for several months in the New Mexico desert. Paul Reynolds, TEAM Technologies' program manager, said the company improved the tool based on the soldiers' input after it was exposed to dust, water and banging around by the troops. The improvements included providing a better seal and redesigning the water plug so it is easier to insert. "The soldiers helped on the design to make it more ruggedized and small enough," Todd said. "It was a very good collaboration." TEAM Technologies is a small business of 75 employees based in the Sandia Science & Technology Park adjacent to the Sandia. "The first year we moved into the park here our business just exploded. We grew 70 percent that year," said Bob Sachs, president and CEO of TEAMTechnologies. Jackie Kerby Moore, the park's executive director, said one reason businesses move to the park is so that they can better engage with Sandia. "This is a real-life example of how the research park helps make companies aware of technology transfer opportunities and help fulfill Sandia's mission to license technologies to private companies," Moore said. The company's first priority is to get the device to troops in Afghanistan, but eventually they would like to sell it to law enforcement and airport security agencies. The device also could be used for forced entry into buildings. "We saw the opportunity to move into a product line and we jumped on it," Sachs said "We're very excited about it. We see it as a whole product line." Reynolds said the tool can be placed almost in contact with the target or a distance away without losing its effectiveness. It uses minimal explosive material, its plastic legs can be attached in various configurations so that it can be placed in different positions to disable bombs and it's built so that robots can easily place it near a target, he said. "This is a giant leap forward in technology," Reynolds said. Those researching and developing the fluid blade disablement tool said they felt a sense of urgency to get it into the hands of soldiers as they read nearly daily media reports about deaths of U.S. troops from IED attacks. "When I look back on how this all took place, the thing that comes through to me was that people were motivated to get a lifesaving technology onto the battlefield," Reynolds said. "This is a lifesaving technology."

New way to sniff out shoe bombs

Source: http://homelandsecuritynewswire.com/new-way-sniff-out-shoe-bombs

Triacetone triperoxide (TATP) is a high-powered explosive that in recent years has been used in several bombing attempts. TATP is easy to prepare from readily available components and has been difficult to detect. It defies most standard methods of chemical sensing: It does not fluoresce, absorb ultraviolet light, or readily ionize; University of Illinois researchers offers a solution that overcomes these problems
University of Illinois chemists have developed a simple sensor to detect an explosive used in shoe bombs. It could lead to inexpensive, easy-to-use devices for luggage and passenger screening at airports and elsewhere. Triacetone triperoxide (TATP) is a high-powered explosive that in recent years



has been used in several bombing attempts. TATP is easy to prepare from readily available components and has been difficult to detect. It defies most standard methods of chemical sensing: It does not fluoresce, absorb ultraviolet light, or readily ionize. The few methods available to screen for TATP aren't feasible for on-the-ground use in airports, as they require large, expensive equipment, extensive sample preparation, or relatively high concentrations of TATP in solid or liquid form. There is no simple way to detect TATP vapor. Kenneth Suslick, the Schmidt Professor of Chemistry at the U. of I., and postdoctoral researcher Hengwei Lin have developed a colorimetric sensor array that can quantitatively detect even very low levels of TATP vapor — down to a mere two parts per billion. They wrote about their findings in an article published in the Journal of the American Chemical Society. To create the sensor array, the researchers print a series of sixteen tiny colored dots — each a different pigment — on an inert plastic film. A solid acid catalyst breaks down TATP into detectable components that cause the pigments to change color, like litmus paper. Each pigment changes colors depending on the concentration of TATP in the air. The array is digitally imaged with an ordinary flatbed scanner or an inexpensive electronic camera before and after exposure to the air. "Imagine a polka-dotted postage stamp sensor that can sniff out the shoe-bomber explosive simply by using a digital camera to measure the changing colors of the sensor's spots," Suslick said. "The pattern of the color change is a unique molecular fingerprint for TATP at any given concentration and we can identify it in a matter of seconds."
The array is uniquely sensitive to TATP. Unlike many other chemical sensors, Suslick and Lin's array is unaffected by changes in humidity or exposure to other chemicals, such as personal hygiene products or laundry detergents. It also has a long shelf life, so airport security and other users can keep a supply on hand. In addition to demonstrating their sensing technique with an ordinary flatbed scanner, the researchers also developed a functional prototype hand-held device. The portable instrument, designed to easily screen luggage or shoes, uses inexpensive white LED illumination and an ordinary digital

camera similar to a cell-phone camera. “The hand-held device makes the whole process portable, sensitive, fast and inexpensive,” Suslick said. The hand-held sensor now is being commercialized by iSense, a senor manufacturer based in Palo Alto, California. “One of the nice things about this technology is that it uses components that are readily available and relatively inexpensive,” said David Balshaw, Ph.D. program administrator at National Institute of Environmental Health Sciences, which supported the project. More information: The paper, “A colorimetric sensor array for detection of triacetone triperoxide vapor,” is available online at the Journal of the American Chemical Society website.

Palestinian Jihad Gaza has camera-fitted suicide vests as in Iraq

Source: http://www.debka.com/article/9102/

debkafile's military and counter-terror sources confirm the WikiLeaks revelation that Iran developed camera-equipped suicide vests for al Qaeda's attacks on US troops under the instruction of the Palestinian Islamic Jihad Center in Tehran. Our sources have discovered that the Islamic Jihad's "Jerusalem Brigades" in the Gaza Strip have been equipped with those same SVIED (Suicide Vest Improvised Explosive Devices) and have transferred some to al Qaeda cells at large in the territory. This sophisticated suicide vest is fitted with miniature cameras which enable the bomber to monitor and relay images of an attack before he reaches his target, our military sources report. The bomber can thus stay in close touch with, and receive instructions, from his handlers every step of the way and also obtain images of the environment he is entering and the obstacles ahead. An Israeli officer told debkafile that these mini-cameras "make it almost impossible for a suicide bomber to miss his aim. It makes him a human guided missile." The presence of these SVIEDs in Islamic Jihad and al Qaeda hands in the Gaza Strip was recently brought to light by the Palestinian Hamas's intelligence agents as part of their report on the deepening collaboration between the Iranian proxy Islamic Jihad and local Salafi groups which have pledged loyalty to al Qaeda and Osama bin Laden and are a thorn in the sides of the Hamas rulers. Jihad commanders are training the al Qaeda squads in the use of the novel suicide weapon of exactly the same type as Iran gave al Qaeda in Iraq and are joining them for missions against Israeli targets across the Gaza border. Thus far, Israeli troops have managed to thwart their attempts at encroachment, wiping them out as they crossed the border fence. Most of these incidents are not brought to the public's knowledge. Hamas has meanwhile cautioned the Jerusalem Brigades to stop cooperating with al Qaeda in the Gaza Strip or else their training facilities and weapons caches will be destroyed, including their rockets, mortars and suicide belts. However, the Islamic Jihad, which is not about to succumb to Hamas's dictates and disobey its masters in Tehran, sent back a two-part reply:

1. Any members carrying out attacks on Israel by firing rockets, planting bombs or using explosive vests without explicit instructions from their commanders will be expelled from the Islamic Jihad and ostracized.
2. Jihad leaders are ready for dialogue with Hamas, provided that its fighters are attached to the Hamas special force known to the IDF as the "Hamas Covert Unit," which was recently established to keep random missile fire against Israel in check.

Jihad did not refer to Hamas' primary demand, to terminate its operational collaboration with al Qaeda cells which challenge Hamas authority. In Iraq, Al Qaeda is described in the ground-level view of the war offered in WikiLeaks 391,831 classified documents covering six years from early 2004 until Jan. 1, 2010 as "the strongest organization among the insurgent groups."

Cargo bomb aftermath: end for in-flight cellular, Wi-Fi connection

Source: http://homelandsecuritynewswire.com/cargo-bomb-aftermath-end-flight-cellular-wi-fi-connection

The aviation industry is gearing up to provide broadband in-flight entertainment systems that feature both cell phone and Wi-Fi connections for passengers; in-flight communications is a fast-growing market at the moment -- but the discovery last week of the cargo bomb plot now casts doubt on the wisdom of in-flight communications; we now know that the cell phones in the printer bombs were not intended to be triggered remotely, and were intended simply as timers, as in the 2004 Madrid train bombings; future devices, though, could take advantage of wireless communication, meaning that on-board bombs could be triggered remotely, from the ground, by a cell phone.

This is something you won't see on a flight // Source: scienceline.org

The long-awaited ability to use a cell phone or Wi-Fi connection on an aircraft may well become a casualty of the latest aviation security threat. It was revealed on 29 October that parcels containing a powdered explosive packed in laser printer cartridges had traveled undetected on aircraft to the United Kingdom and to Dubai in the UAE. A cell phone connected to a detonation circuit could have allowed a terrorist to trigger an explosion by calling or texting the phone. Paul Marks writes in New Scientist that this comes as the aviation industry is gearing up to provide broadband in-flight entertainment systems that feature both cell phone and Wi-Fi connections for passengers. These systems would mean that passengers would no longer need to use their cell phones illicitly when they come into range of ground masts at low altitudes near airports — a potentially dangerous activity that could interfere with the aircraft's avionics. Marks notes that in-flight communications is a fast-growing market at the moment. Market researcher InStat of Scottsdale, Arizona, says that 2000 passenger aircraft are expected to have this kind of satellite broadband communications technology by the end of this year, compared with just "a couple of dozen" in 2008. Last week's cargo bomb discoveries cast doubt on the wisdom of in-flight communications, says Roland Alford, managing director of Alford Technologies, an explosives consultancy in Chippenham, Wiltshire, United Kingdom. He says he expects the technology to be scrutinized in the security reviews being undertaken by the U.K. government and U.S. DHS in the wake of the discovery of the printer bombs. The U.K. Department of Transport would not confirm whether the issue would in fact be on its agenda. We now know that cell phones in the printer bombs were intended simply as timers, as in the 2004 Madrid train bombings. Future devices, though, could take advantage of wireless communication. In-flight Wi-Fi "gives a bomber lots of options for contacting a device on an aircraft," Alford says. Even if ordinary cell phone connections are blocked, it would allow a voice-over-internet connection to reach a handset. "If it were to be possible to transmit directly from the ground to a plane over the sea, that would be scary," says Alford's colleague, company founder Sidney Alford. "Or if a passenger could use a cell phone to transmit to the hold of the airplane he is in, he could become a

very effective suicide bomber." Marks writes that manufacturers of the technologies will not welcome this fresh security concern, having finally gained airworthiness approval for their in-flight cell phone and Wi-Fi systems by proving that their microwave transmissions do not interfere with avionics. "There are many ways of coordinating an attack without using a mobile phone," says Aurélie Branchereau-Giles of OnAir, a company based in Geneva, Switzerland, that Airbus is backing as a maker of in-flight cellphone and Wi-Fi systems. "The position of our security experts is that the use of mobile phones on planes does not constitute any additional security threat."

Only 20 percent of U.S.-bound cargo screened for bombs

Source: http://www.homelandsecuritynewswire.com/only-20-percent-us-bound-cargo-screened-bombs

About 20 percent of the nine billion pounds of air cargo that comes from overseas each year is physically checked for bombs; at some overseas airports, cargo is checked for bombs before being put on planes, but that screening could be below U.S. security standards, according to the U.S. Government Accountability Office (GAO); the TSA may start forcing airlines to inspect suspicious cargo before a plane takes off from overseas. the agency is studying whether the tracking system can target certain U.S.-bound air cargo for screening prior to departure. Billions of pounds of packages bound for

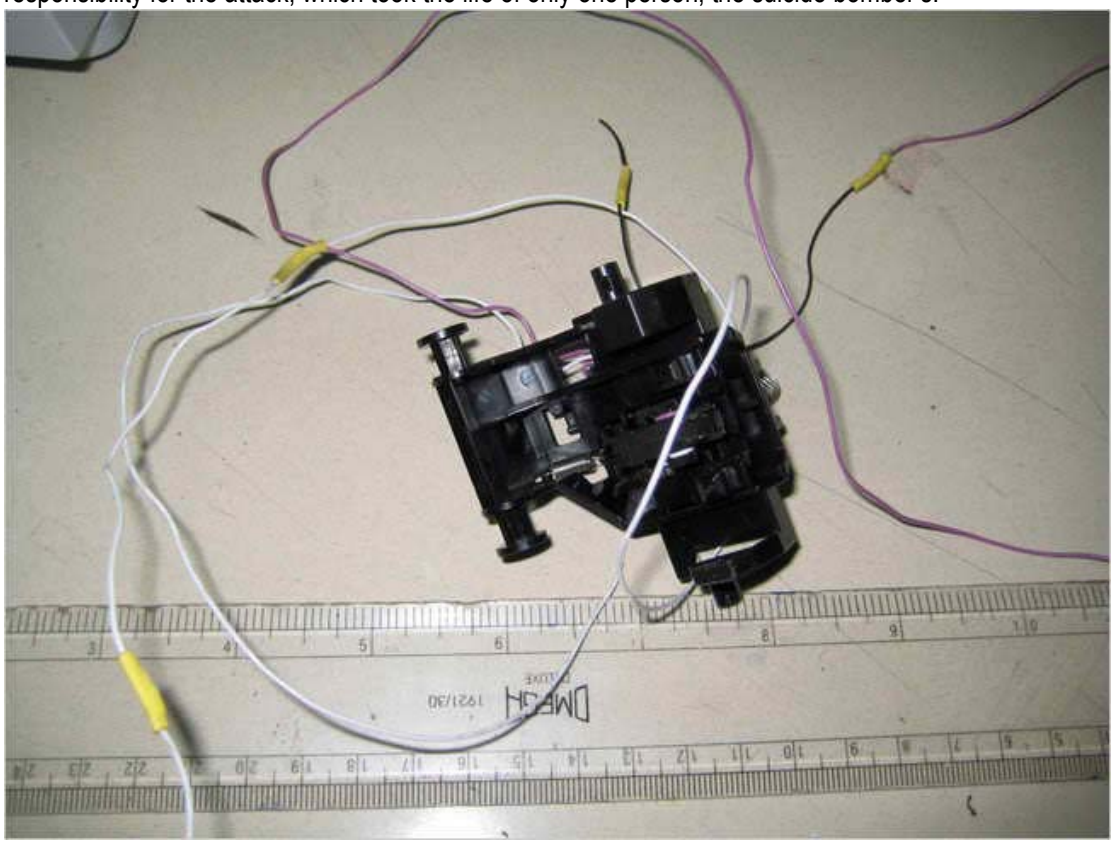
the United States each year are delivered on passenger flights in which cargo is checked with an electronic system that does not screen for bombs, lawmakers and security experts said earlier this week. DHS uses computers to identify possibly dangerous cargo, usually after flights are already in the air and en route to the United States. Many of those flights are passenger planes carrying cargo in the hold. "That's too late. A bomb will go off while a plane is in the air," said aviation security consultant Glen Winn, a former United Airlines security chief. USA Today's Thomas Frank reports that the tracking system is under scrutiny following last week's plot to sneak bombs into U.S.-bound planes using cargo packages sent from Yemen. At some overseas airports, cargo is checked for bombs before being put on planes, but that screening could be below U.S. security standards, according to the U.S. Government Accountability Office (GAO). Robert Bonner, former head of Customs and Border Protection (CBP), said, "It makes sense to have the (cargo) information pre-departure so you can not only deny entry on arrival but can potentially deny access to the airplane." About 20 percent of the nine billion pounds of air cargo that comes from overseas each year is physically checked for bombs, according to the Transportation Security Administration, which says the tracking system picks out all "high risk" air cargo.

Representative Ed Markey (D-Massachusetts), said he worries about cargo that is high-risk but not identified "because that's where the real threat will come from." Frank writes that after the 9/11 attacks, CBP began receiving electronic manifests listing each cargo package coming to the United States by ship, truck, rail, and airplane. The lists show each shipment's contents, origin, destination, and other information that is run through a database filled with shipping histories and intelligence. Maritime companies must send the lists twenty-four hours before a ship sets sail from a foreign port. Suspicious cargo is inspected overseas with X-ray machines and radioactive detectors, Bonner said. The TSA may start forcing airlines to inspect suspicious cargo before a plane takes off from overseas, the GAO said. The TSA is studying whether the tracking system can target certain U.S.-bound air cargo for screening prior to departure. That could improve security while the TSA figures out how to make sure that all U.S.-bound air cargo traveling on passenger planes is physically inspected, as Congress has ordered, the GAO said. Bonner said the tracking system is as effective as screening all cargo because it focuses scrutiny. "You have a better chance of inspecting in a thorough way things that are truly risky instead of inspecting everything," Bonner said.

Explosive on Planes Was Used in Past Plots

Source: http://www.nytimes.com/2010/10/31/world/middleeast/31petn.html?_r=1&ref=terrorism

Pentaerythritol tetranitrate, or PETN, the explosive found in two bombs hidden in printer cartridges that were being shipped via jets from Yemen to the United States, is a hallmark of earlier Qaeda-linked terrorism attempts on airplanes. In 2001, PETN was found hidden in the shoes of Richard C. Reid during an American Airlines flight. Last Christmas, Umar Farouk Abdulmutallab had three ounces of PETN hidden in his underwear on a Northwest flight from Amsterdam to Detroit. An assassination attempt in August 2009 on Saudi Arabia's intelligence chief, Prince Mohammed bin Nayef, also employed PETN. Al Qaeda in the Arabian Peninsula, an arm of the terrorist network, claimed responsibility for the attack, which took the life of only one person, the suicide bomber's.



But other terrorist groups have also used PETN, and the presence of the explosive itself does not decisively point to Al Qaeda. "That's a very common explosive," said Jimmie C. Oxley, a professor of chemistry at the University of Rhode Island. "There's no reason to think a lot of people didn't have

access to do that." PETN, a white powder that was introduced after World War I, belongs to the same chemical family as nitroglycerin. It is about 70 percent more powerful than T.N.T., and is stable. PETN generally does not explode when dropped or set on fire. Usually, a strong shock wave from a blasting cap or an exploding wire detonator is needed to set it off. Those properties make it well suited for a variety of commercial applications. PETN is a major ingredient of the plastic explosive Semtex and is used in detonation cables. For terrorists, PETN is an attractive choice for package bombs. Its stability means it is unlikely to explode prematurely, but at its destination, it will go off with deadly force when detonated. (Conversely, the stability of PETN also thwarted the attacks of Mr. Reid and Mr. Abdulmutallab, who were not able to detonate their explosives.) Dubai officials said that the printer cartridge bomb intercepted there on Friday included lead azide, an explosive to detonate the PETN, and a cellphone circuit, presumably to allow the bomb to be set off remotely. Neal Langerman, president of Advanced Chemical Safety, a consulting firm in San Diego, said it appeared "to be a fairly sophisticated device." Judging from photos of the Dubai bomb, Dr. Oxley estimated that the printer cartridge contained about two pounds of PETN. The British home secretary, Theresa May, said Saturday that the second bomb, intercepted in Britain on Friday, contained enough explosive to bring down a plane. The target of the bombs remains unclear; they could have been directed at the synagogues or Jewish community centers in Chicago to which they were addressed. Placement of a bomb in a plane can be as important as its size in determining the amount of damage it could cause, Dr. Oxley said. While the printer cartridge contained more PETN than Mr. Reid's shoes or Mr. Abdulmutallab's underwear, the bomb maker could not be certain where in the airplane the package would be located. Mr. Reid and Mr. Abdulmutallab tried to detonate their devices close to the wall of the respective planes on which they were flying, to increase chances that the explosion would blow a hole in the aircraft. "Last year, the guy had more control," Dr. Oxley said, referring to Mr. Abdulmutallab. But the printer cartridge bomb, she said, had so much more PETN that "my guess, and this is only a guess, it may have had a higher probability" of taking down an airplane. Dr. Langerman said it was curious that the two most recently intercepted devices apparently were different in design. That may indicate that the explosive makers had different targets in mind.

Increasing counter-IED role for robots

Source: http://homelandsecuritynewswire.com/increasing-counter-ied-role-robots

U.S. and coalition military operating in Afghanistan have experienced about 10,500 roadside bomb incidents so far this year, up from 8,994 in 2009 and 2,677 in 2007; robots continue to play ever-more important combat roles in the air and on the ground in Afghanistan and Iraq, and their responsibilities will only continue to grow.

IED killer during training // Source: theage.com.au

Hardly a day seems to pass without a new report of a soldier or civilian being killed or maimed an improvised explosive device (IED) in Afghanistan or Iraq. Just such a weapon killed two coalition

members on Monday in Iraq's volatile southern region, according to NATO. Meanwhile, data published 22 October by Wikileaks indicates that IEDs are the biggest killers of British and U.S. troops in Afghanistan, accounting for more than half of all fatalities. Larry Greenemeier writes in Scientific American that to protect people from these weapons, the U.S. military increasingly relies on robotic bomb detection and disposal units (in addition to the scores of UAVs overhead with reconnaissance and strike capabilities), creating life-and-death combat relationships between man and machine that will only deepen and proliferate over time. U.S. and coalition military operating in Afghanistan have experienced about 10,500 roadside bomb incidents so far this year, up from 8,994 in 2009 and 2,677 in 2007, Army Lt. Gen. Michael Oates, director of the Joint Improvised Explosive Device Defeat Organization (JIEDDO), reported 21 October. A significant portion of these are IED-related incidents. The success of such attacks ensures that they will continue for at least the short-term, which means the military is searching for new ways of addressing the problem. In Afghanistan U.S. soldiers conduct month-long Explosive Hazard Reduction courses to train Afghan soldiers about how IEDs work, the threats they pose and techniques for finding them. Coalition forces have spent about $2 billion since 2006 to train soldiers stationed worldwide about IEDs, according to Oates. A lot of money is also being spent on anti-IED robots. Earlier this month the U.S. Army TACOM Contracting Center in Warren, Michigan, ordered $14 million worth of robot intelligence software and spare parts for its PackBot tactical mobile robots, made by iRobot in Bedford, Massachusetts. This was TACOM's twentieth such order for iRobot technology and part of the unit's larger $286-million "xBot" contract for purchasing bomb-detection robots. There are more than 3,500 iRobot devices serving in the U.S. military as well as the armed forces of another twenty allied countries, says Joseph Dyer, iRobot's chief operating officer and a retired U.S. Navy vice admiral.

Real-time detection of PETN explosive with PTR-MS

Source: http://homelandsecuritynewswire.com/real-time-detection-petn-explosive-ptr-ms

PETN is an extremely powerful explosive, belonging to the nitroglycerine family, but is very stable; it is therefore a preferred explosive used by terrorists; a major problem for security personnel is that PETN is difficult to detect; academic, commercial organizations collaborate to develop PTR-MS technology for the detection of explosives -- not only PETN, but also TNT, RDX, Semtex, and HMX

Detonation of 0.5 grams of PETN // Source: sciencemadness.com

The recent terror plot to transport printers containing the explosive pentaerythritol tetranitrate, or PETN, from Yemen to Chicago synagogues has once again focused attention on the need to detect explosives reliably and in real-time. PETN is the same explosive that the shoe-bomber tried to set-off on an American Airlines jet to Miami in 2001. More recently PETN was involved in the failed attempt at setting off a bomb on an airliner in midair (Northwest Airlines Flight 253, 25 December 2009) by the Nigerian born Umar Farouk Abdulmutallab and in the attempted assassination of a member of the Saudi royal family this summer. PETN is an extremely powerful explosive, belonging to the nitroglycerine family, but is very stable. It is therefore a preferred explosive used by terrorists. A major problem for security personnel is that PETN is difficult to detect. Analytical methods generally rely on the presence of residues left on the surfaces of freight containing explosives. A major difficulty associated with any analytical instrument, however, is to achieve high selectivity, thereby reducing false positives and negatives, whilst maintaining the high sensitivity required for trace detection. In collaboration with researchers at the Universities of Innsbruck and New York and the University of Birmingham, Ionicon Analytik GmbH has been investigating the potential of the PTR-MS technology for the detection of explosives. Together, these organizations have

demonstrated the capabilities of using PTR-MS for the detection of trace quantities of PETN (and other explosives (for example, TNT, RDX, Semtex, and HMX) on contaminated surfaces with extremely high selectivity (see Mayhew et al., Int. Journal of Mass Spectrometry 289 [2010] 58). Crucially, the identification of explosives, such as PETN, with a high level of confidence in real-time and in trace quantities is of great importance to the military, to emergency responders, and for applications in checkpoint security areas such as airports, harbors, and train stations.

Pentagon: dogs better than technology at bomb detection

Source: http://homelandsecuritynewswire.com/pentagon-dogs-better-technology-bomb-detection

The most sophisticated detectors the Pentagon came up with tend to locate only 50 percent of IEDs in Afghanistan and Iraq; when soldiers are accompanied by bomb-sniffing dogs, this number goes up to 80 percent; the Pentagon now spends less money on IED detection and more money on drones to find those planting IEDs, radio jammers to disrupt the frequencies used to detonate the bombs, and lots of aerial sensors to scan bomb-heavy areas. After six years and nearly $19 billion in spending, a Pentagon task force assigned to create better ways to detect bombs has reached this conclusion: The best bomb detector is a dog. Spencer Ackerman writes that the Joint Improvised Explosive Device Defeat Organization, or JIEDDO has been working on this problem for years, but it is only getting more serious. There have been more roadside bombs in Afghanistan in the first eight months of this year than in the same period in 2009, so the work JIEDDO is doing is under extra scrutiny. Dan Nosowitz writes that this made it even more embarrassing when the director of the organization told a conference the other day that "Dogs are the best detectors." As it turns out, the most sophisticated detectors JIEDDO could come up with tend to locate only 50 percent of IEDs in Afghanistan and Iraq. When soldiers are accompanied by bomb-sniffing dogs, this number goes up to 80 percent. That director, Lieutenant General Michael Oates, said that his organization now focuses on disrupting the use of IEDs, rather than flat-out detecting them, because they have not made all that much progress on the detection front. Instead of detection, JIEDDO now spends money on drones to find those planting IEDs, radio jammers to disrupt the frequencies used to detonate the bombs, and lots of aerial sensors to scan bomb-heavy areas. All this is useful, but Congress has recently shown a lack of confidence in the group's accomplishments, its focus, and in the way its funds are being spent. In response, the House Armed Services Committee cut the group's budget by nearly half a billion dollars ("Senate panel rejects Pentagon counter-IED group $400 million emergency funding request," 27 May 2010 HSNW) — which, as Nosowitz points out, can train a whole lot of bomb-sniffing dogs, or at least buy some sweet dog armor.

Operation damage control

Source: http://www.washingtonpost.com/wp-dyn/content/article/2010/10/29/AR2010102906991.html

AT BAGRAM AIRFIELD, AFGHANISTAN It's a heart-stopping and heartbreaking catalogue of the mayhem, heroics and human toll of modern war. Every Thursday afternoon doctors, nurses and medics gather in a conference room at the military hospital here, linked by telephone or videocam to colleagues at all the combat hospitals in Afghanistan, and at military hospitals in Europe and the United States. Over two hours, this virtual assembly of about 80 people reviews the care of every U.S. service member critically injured in Afghanistan in the previous week.

Among the 13 discussed at one recent meeting, nine will have permanent disabilities: Two lost one leg; two lost a leg and a foot; two lost both legs; two lost both legs and a hand; and one was paralyzed from the waist down. Three of the nine also lost their genitals. The conference helps ensure no injuries are overlooked in patients who often have a dozen wounds or more. It's a way of double-checking innumerable pieces of information that have been entered into a database and will be studied to help improve practice. It's also a way of gently monitoring everyone's performance.

Lots of people take care of these patients, but few see them for more than the 36 hours before they are flown out of Afghanistan. The weekly conference assembles, for everyone's benefit, the chapters of a narrative whose only common character is the broken body of the soldier himself. These trans-continental medical rounds reflect a revolution in the care of battlefield casualties. No longer are grievously injured soldiers kept in one place until they're stable and have had their wounds fully addressed. Instead they're moved in a seamless process that combines treatment and transport from the battlefield to a combat hospital, to Bagram, to a military hospital in Landstuhl, Germany, and then to one of the giant medical centers in Washington, Bethesda or San Antonio. The system is based on an approach called "damage control surgery," imported from civilian medicine but perfected in the past nine years in the Iraq and Afghanistan wars. Wounds are addressed in stages. Surgery is kept as short as possible. Most soldiers with critical injuries get two operations in two hospitals in the first 24 hours. Experience has shown that fewer trauma victims die if you treat them in step-wise fashion. But most Afghanistan trauma is caused by make-shift bombs or IEDs that inflict such extensive damage that fixing the body in two or three operations is impossible anyway. "Twenty years ago, if you left the operating room without fixing everything, you weren't a good surgeon," said Rodd Benfield, a 39-year-old Navy surgeon from San Diego deployed to Kandahar field in Afghanistan. "We don't believe that anymore." IEDs not only blow limbs off the body, they drive dirt deep into flesh and often peel skin back a foot or more above the bone's jagged end. The shock wave kills tissue that initially looks normal and takes days to "declare" its true condition. With damage-control surgery, these wounds are washed out, and dead tissue removed, under general anesthesia every day for a week or more. Similarly, abdominal cavities are explored and re-explored, as surgeons look for wounds overlooked in the first operation, or that have developed since. Pelvic injuries, often massive because of between-the-legs IED blasts triggered by soldiers on foot patrol, are left open, protected with bandages and taken step by step. Inevitably, inhabiting this near-death state for a prolonged period results in hard-to-avoid complications - pneumonia, collapsed lungs, blood clots - that require their own procedures.

"It's like one long operation," said Eric Elster, a transplant surgeon at the naval hospital in Bethesda who's in Kandahar. The conference is run by Col. Brian Eastridge, a 47-year-old trauma surgeon with 23 years in the Army. He grew up in Damascus, Md., graduated from Virginia Tech and the University of Maryland School of Medicine. He now heads the Joint Theater Trauma System, which organizes trauma care in both wars. Over five deployments, Eastridge has seen the arc of worsening wounds and

increasing survival that has marked trauma care in the Iraq and Afghan wars. Dressed in brown camouflage battle dress, he sits halfway around a large U made of wooden tables. Around him on the walls are idealized scenes of Afghan life painted by a local artist - a girl leading a caravan of camels, children being taught arithmetic at the base of a tree, kids flying kites. Eastridge runs the conference with somber efficiency, offers comments sparingly and addresses his listeners mostly by location- "Kandahar," "Landstuhl," "Walter Reed." The rapid-fire reports are dense with medical jargon and anatomical description. It's a narration of one disaster after another, and of how things were kept from getting worse, and made better, by skill, speed and attention. It's the aural equivalent of watching a dozen high-wire acts in which some people are rescued mid-fall.

Here's just one.

"Dismounted IED" injury is jargon for wounds caused by a bomb or mine that are suffered outside a vehicle. The soldier had tourniquets placed for partial amputation of both legs. One liter of a special IV fluid was given in the helicopter, and the patient arrived at the Kandahar hospital in and out of consciousness and in shock. In the operating room, surgeons tied off the arteries going to the legs and repaired a tear in a major vein. There was massive damage to the area between the legs. One leg was amputated at the knee. In a second operation the next day his wounds were rewashed and a finger, broken in the explosion, was fixed with external hardware. That same day the soldier was evacuated to Bagram, where his wounds were washed out and the pelvic region was re-explored. A "foreign body"- the speaker didn't say whether it was dirt, metal or something else - not seen in the first operation was removed. His lung collapsed after surgery, which was fixed. He stayed there two days before flying by critical care transport to Landstuhl. There the process was repeated. Seven days after suffering his wounds the soldier arrived at a hospital in the United States. He had another collapsed lung, and pneumonia. His right foot, initially thought to be salvageable, wasn't healing and the surgeons planned to amputate it at the ankle. He had further surgery to his abdomen and numerous operations to start reping the missing floor of his pelvis. "This was one of the biggest pelvic injuries I've ever seen," said one of the surgeons in the United States. Eastridge later said he hears that a lot from surgeons in the United States who haven't been deployed yet. This case was not uncommon.

'Tremendous saves'

After a litany of such descriptions, the group filed out. "None of these kids would have survived in the civilian world," said Jay Johannigman, one of the surgeons. "And we never would have saved them five years ago." The last thing Eastridge said before ringing off was: "Another busy week. There was a bunch of tremendous saves. There are several really tremendous saves that are going to be coming up next week, too." But do the doctors sometimes wonder if the lives they've saved will be worth living? It's an extremely delicate question and not one anyone asks in the heat of the moment. But sometimes, afterward, they do. "The efforts we take are not futile at all," said Elster, the Navy surgeon at Kandahar. "We've seen a few of these guys move through Bethesda and recover. This is not in vain. Between prosthetics and rehabilitation, these folks can go on to lead a very productive life." Eastridge would not disagree with any of that. But he wonders how he would feel if he had the disabilities of his patients. "A lot of my colleagues have similar questions," he said the next day, after operating all night. "We talk about it amongst ourselves. Did we do the right thing by saving that 90 percent burn patient, or the casualty who has all four extremities amputated?" He continues: "But there are so many stories of people who have gone on to be functional and appreciative that they had the chance to live the rest of their lives. We definitely struggle with the ones that are out there that don't feel that way." The surgeons here have a fierce dedication to saving every life. Only in mass casualty events must some patients be put aside and treated "expectantly," the euphemism for the assumption they will die. Even getting someone alive to Landstuhl, where their family can see them before they die, counts as a victory. "We try not to withdraw care here in theater," Eastridge said. But every once in a while it happens. It's usually someone with brain injuries so severe they're likely to die during transport. They're allowed to die here, with troops at the bedside. "That just affords them that last little bit of dignity," he said. He stopped, and his eyes filled with tears.

The sick Iraqi terrorist plot to bomb a U.S. plane with exploding DOGS

Source: http://www.dailymail.co.uk/news/article-1327052/Kamikaze-canines-The-sick-Iraqi-terrorist-plot-bomb-U-S-plane-exploding-DOG.html#ixzz14RMTu1Mq

Sick Islamic terrorists tried to bring down a US cargo plane using two exploding DOGS, it was revealed today. The Kamikaze canines - whose stomach had been stuffed with bombs and detonators - were discovered at Baghdad airport two years ago, French daily Le Figaro said. They had been primed to explode in mid-flight, but were never loaded aboard the aircraft because freight handlers spotted both dogs had died in their cages. A cargo plane was targeted by terrorist who loaded two dogs up with explosives on a flight from Baghdad International Airport, formerly named Saddam International Airport, to Los Angeles. Post mortem examinations on the animals uncovered explosives and detonators set to go off several hours into the flight from the Iraqi capital to Los Angeles, Le Figaro said. The paper learned the information from a US military source earlier this week, it said. The horrifying revelations come after one of two bombs sent from Yemen concealed inside printer ink cartridges was discovered at Britain's East Midlands airport last week. France's interior ministry claimed the device was defused just 17 minutes before it was due to explode. The shock discovery of the live animal bombs two years ago was investigated by the International Civil Aviation Organisation at the time and airlines and cargo flight operators were immediately alerted to risk of exploding pets, Le Figaro said. The paper added: 'This discovery was made two years ago but kept secret from the public. 'The dogs were discovered in a freight area at Baghdad airport, but because they were dead, they were never loaded aboard the plane.'

A US soldier is seen stroking a stray dog, which have multiplied since the US invasion. In 2008, when the canine bombs were found, Baghdad started to cull dog packs. By 2010 there were over 1m strays

and officials sent out sharp shooters to cull them. French terrorism expert Christophe Naudin said: 'This highlights the determination of al-Qaeda militants to wreak destruction by literally any means possible. 'Live animals are transported on passenger planes as well as cargo planes, and airlines and airports need to be on constant alert. 'Western security services are also aware of the possibility that terrorists could use children carrying bombs inside them to destroy aircraft.' In 2001, Briton Richard Reid tried to set off a bomb hidden in his shoe on an American Airlines jet to Miami in 2001. This summer a suicide bomber tried to assassinate a member of the Saudi royal family with a bomb inside his body.

Al Qaeda plot to use kamikaze dogs failed

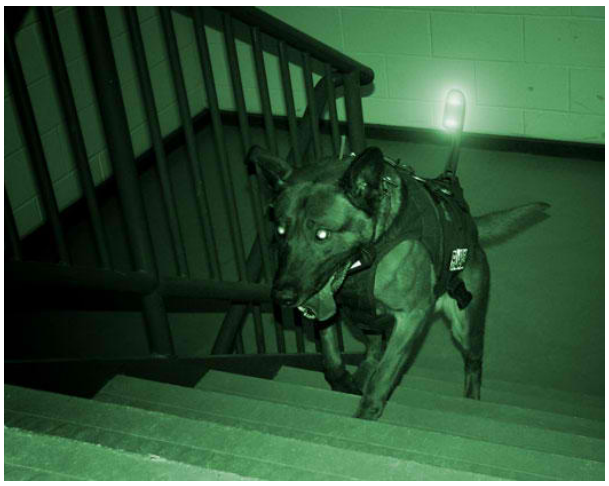
Source: http://www.homelandsecuritynewswire.com/al-qaeda-plot-use-kamikaze-dogs-failed

Al Qaeda operatives in Iraq tried to bring a plane down by deploying a pair of kamikaze canines on a U.S.-bound airplane; terrorists placed the bombs inside the dogs' bodies, then took the dogs to the Baghdad airport in kennel carriers, destined for a flight to the United States; the plot failed because the bombs were so poorly stitched inside the dogs, that the dogs died. Al Qaeda operatives in Iraq attempted to unleash terror in the skies by deploying a pair of kamikaze canines on a U.S.-bound

airplane, a French newspaper reports. The canine-centered plot failed because the bombs were so poorly stitched inside the dogs that they — the dogs — died, Paris daily Le Figaro reports (see Jean-Marc Leclerc, “Avions de ligne : la menace des chiens kamikazes,” 1 November 2010 Le Figaro). “This case illustrates the determination of al Qaeda militants, who are trying to circumvent terrorism controls by any means,” French criminologist and aviation expert Christophe Naudin told the newspaper. The plot unfolded roughly two years ago, when al Qaeda militants grabbed two stray dogs off the street and surgically implanted powerful explosives and detonators in each. The dog were then taken a Baghdad airport in kennel carriers, destined for a flight to the United States, the newspaper reports. The plot was discovered when an American military patrol found the bodies of the two dogs in a secure area of the airport. An autopsy found the explosives inside the dogs’ bodies. The information about the kamikaze dogs was circulated to the U.S. security agencies and the international governing body of civilian aviation, but was kept secret for nearly two years. Le Figaro notes that the Saudi suicide bomber who, on 28 August 2009, tried to kill a Saudi prince by carrying explosive inside his body, used a methodology similar to that tried with the dogs.

Tactical vests for military dogs

Source:http://www.popsci.com/technology/article/2009-12/high-tech-canine-flak-jacket-lets-tactical-dogs-operate-far-handlers



K9 Storm Vest in Action

He is man's best friend after all, so doesn't he deserve the tactical body armor commensurate with that title? K9 Storm, a Canadian body armor specialist, pulls in millions a year manufacturing body armor for dogs serving in the line of duty on police forces and in militaries around the world. In 2010, their newest line of doggie defense, the K9 Storm Intruder, will pull Fido into the digital age.

K9 Storms Tactical Vests for Dogs: K9 Storm

The Intruder not only protects canines with a sturdy flak jacket enveloping their vital organs, but it sports a wireless camera so the handler can see what the dog sees, as well as speakers so the handler can issue audio commands. As a result, dogs can operate up to 300 yards from their handlers, a big advantage in emergency situations where dogs are often sent into areas deemed too unsafe for humans to operate.

At $20,000 each, the Intruder vests aren't cheap. But considering a military or police dog can cost upwards of $50,000, keeping a well-trained canine from going down in the line of duty is paramount. Not to mention, the operational enhancement from the extended range should up each dogs value on the battlefield or in emergency situations substantially. For our part, we'd be happy with a remote rig that lets us take the dog out to the curb without us ever leaving the couch.

A New and Simple Sensor for Explosive Chemicals Could Sniff Out Shoe Bombs

Source: http://www.medicalnewstoday.com/articles/205238.php

University of Illinois chemists have developed a simple sensor to detect an explosive used in shoe bombs. It could lead to inexpensive, easy-to-use devices for luggage and passenger screening at airports and elsewhere. Triacetone triperoxide (TATP) is a high-powered explosive that in recent years has been used in several bombing attempts. TATP is easy to prepare from readily available components and has been difficult to detect. It defies most standard methods of chemical sensing: It doesn't fluoresce, absorb ultraviolet light or readily ionize. The few methods available to screen for TATP aren't feasible for on-the-ground use in airports, as they require large, expensive equipment, extensive sample preparation, or relatively high concentrations of TATP in solid or liquid form. There is no simple way to detect TATP vapor. Kenneth Suslick, the Schmidt Professor of Chemistry at the U. of I., and postdoctoral researcher Hengwei Lin have developed a colorimetric sensor array that can quantitatively detect even very low levels of TATP vapor - down to a mere 2 parts per billion. They wrote

about their findings in an article published in the Journal of the American Chemical Society. To create the sensor array, the researchers print a series of 16 tiny colored dots - each a different pigment - on an inert plastic film. A solid acid catalyst breaks down TATP into detectable components that cause the pigments to change color, like litmus paper. Each pigment changes colors depending on the concentration of TATP in the air. The array is digitally imaged with an ordinary flatbed scanner or an inexpensive electronic camera before and after exposure to the air. "Imagine a polka-dotted postage stamp sensor that can sniff out the shoe-bomber explosive simply by using a digital camera to measure the changing colors of the sensor's spots," Suslick said. "The pattern of the color change is a unique molecular fingerprint for TATP at any given concentration and we can identify it in a matter of seconds." The array is uniquely sensitive to TATP. Unlike many other chemical sensors, Suslick and Lin's array is unaffected by changes in humidity or exposure to other chemicals, such as personal hygiene products or laundry detergents. It also has a long shelf life, so airport security and other users can keep a supply on hand. In addition to demonstrating their sensing technique with an ordinary flatbed scanner, the researchers also developed a functional prototype hand-held device. The portable instrument, designed to easily screen luggage or shoes, uses inexpensive white LED illumination and an ordinary digital camera similar to a cell-phone camera. "The hand-held device makes the whole process portable, sensitive, fast and inexpensive," Suslick said. The hand-held sensor now is being commercialized by iSense, a senor manufacturer based in Palo Alto, Calif. "One of the nice things about this technology is that it uses components that are readily available and relatively inexpensive," said David Balshaw, Ph.D. program administrator at National Institute of Environmental Health Sciences, which supported the project.

Bomb-sniffing dogs in Afghanistan, Iraq may not be up to the task

Source: http://homelandsecuritynewswire.com/bomb-sniffing-dogs-afghanistan-iraq-may-not-be-task

The U.S. State Department uses nearly 200 bomb-sniffing dogs in Iraq and Afghanistan to protect U.S. diplomatic facilities; the department inspector general says that bomb-sniffing dogs in Afghanistan and Iraq are not being tested properly and may not be able effectively to detect explosives

The U.S. State Department's inspector general said that bomb-sniffing dogs in Afghanistan and Iraq are not being tested properly and may not be able effectively to detect explosives. The inspector general's review found that the companies hired to supply and train the animals were not testing them for all of the scents of the most commonly encountered explosives, increasing the chance of a dog missing a bomb in a vehicle or luggage. That puts U.S. diplomats at risk, the inspector general said. The Los

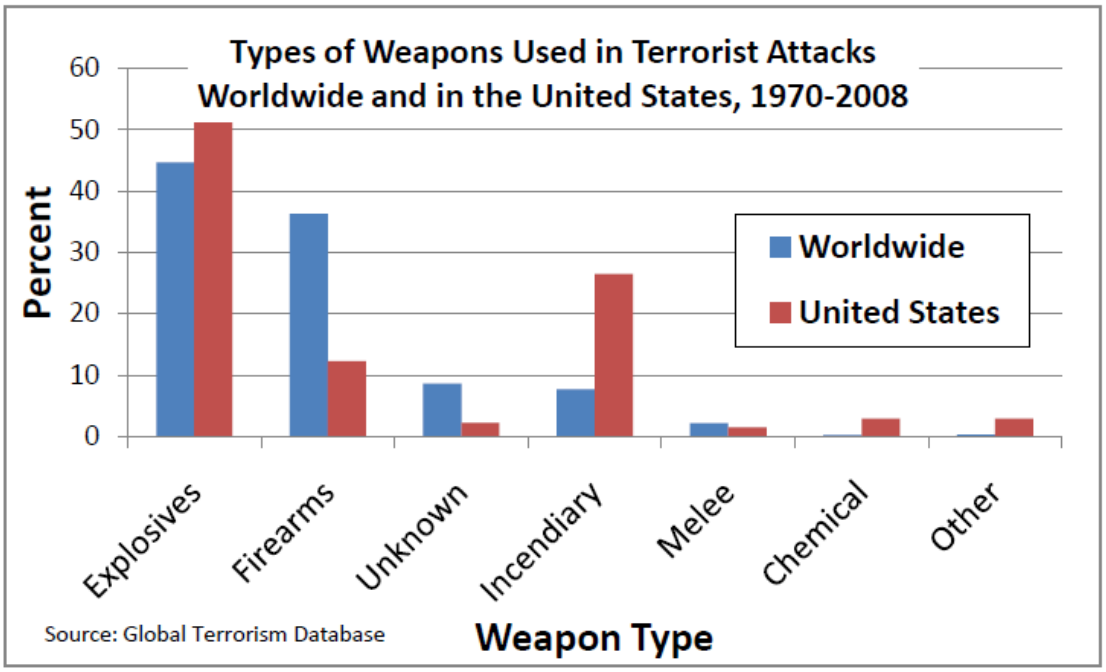
Angeles Times quotes the inspector general to say that the companies — U.S. Training Center in Moyock, North Carolina, a business unit of the company formerly known as Blackwater, and RONCO Consulting Corp. in Washington — also used expired or potentially contaminated materials for the scent tests. Susan Pitcher, a spokeswoman for Wackenhut Services, RONCO's parent company, called the inspector general's review "inaccurate." She said a canine expert engaged by the State Department to verify the detection capabilities of the dogs concluded that they complied with the required standards. Pitcher, however, said that the company had not been provided the expert's report, receiving instead what she described as "on-site briefings" about the results. The inspector general's office said it had not been given the results of the expert's inspection when it released its report. The L.A. Times reports that the inspector general's review was limited to three canine programs handled by U.S. Training Center and RONCO. The report did not say how many dogs each contractor provides. Overall, the State Department uses nearly 200 bomb-sniffing dogs. The report only offers a glimpse of the costs of these services, saying the State Department pays $24 million a year alone for canine services at the U.S. Embassy in Baghdad. The report faults the department's Bureau of Diplomatic Security, which is responsible for managing the canine program, for weak oversight. Investigators found that the contractors, not the bureau, were running the program and policing themselves. During visits to Afghanistan and Iraq, the investigators did not meet any bureau personnel with expertise in bomb-sniffing dogs. "They depended upon the knowledge and expertise of the contractors to ensure all contractual requirements and other standards were met," according to the report. The contractors told the investigators "that no outside organization with expertise in explosive detection canines had ever reviewed their operations in Iraq or Afghanistan," the report said. In comments printed in the report, the Bureau of Diplomatic Security said it is taking steps to improve the canine program and plans to hire an independent expert who will ensure all the contract requirements are met properly.

START: Background Report: Package Bombs on Cargo Planes

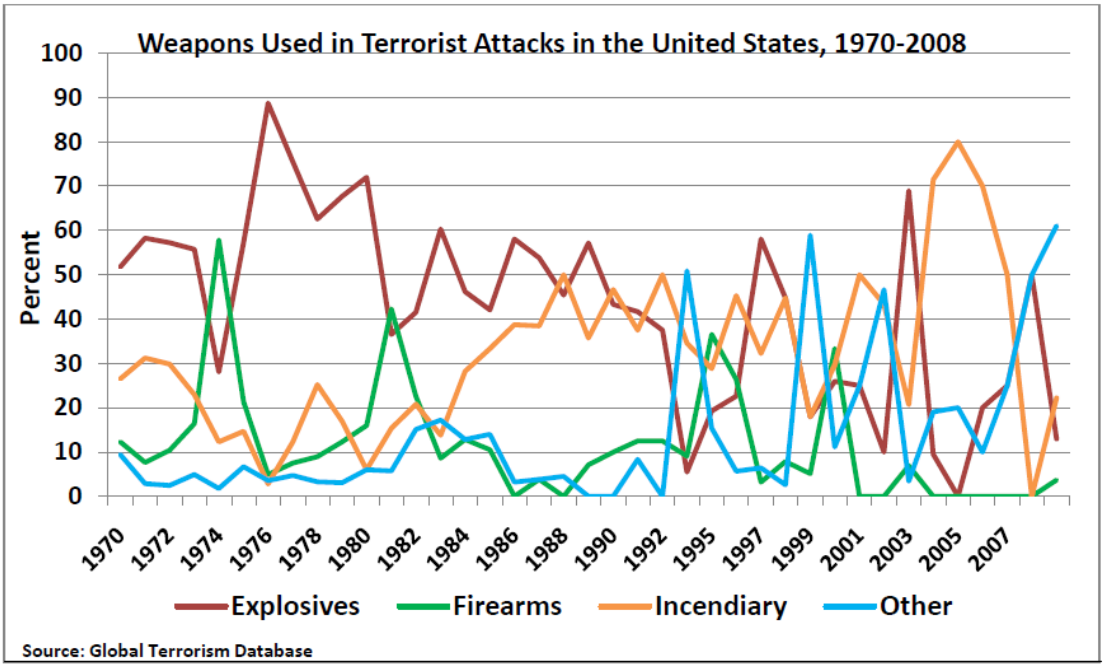
Source: http://www.start.umd.edu/start/announcements/announcement.asp?id=212

Terrorists' use of explosives

In the United States and around the world, explosives are the type of weapon most commonly used in terrorist attacks. In fact, some type of explosive device was used in 45% of all terrorist attacks worldwide between 1970 and 2008. The United States experienced more than 1100 terrorist attacks involving explosives during that period, with this weapon type being used in more than half of all terrorist attacks in the United States.



However, the prevalence of explosives in terrorist attacks in the United States has dropped dramatically in recent years, from over 60% in the 1970s to just under 25% in the 2000s. During the same time period the prevalence of incendiary weapons, including arson, in terrorist attacks in the United States has increased 160%.



Out of over 1100 attacks using explosives in the United States since 1970, forty-three involved letter or package bombs. This includes those sent to various educational institutions and airlines by Theodore Kaczynski, known as the Unabomber, between 1978 and 1995. Letter bomb attacks are rarely lethal, causing a fatality in only 12% of U.S. cases. The targets in these attacks are most frequently government targets, but have also included private citizens and property, educational institutions, businesses, and—as in the recent Chicago case—religious figures and institutions.

Targeting airplanes with explosives

According to the latest reports, both U.S. and British officials suspect that the explosive devices were meant to detonate while on the planes, rather than at the Chicago destinations. Furthermore, authorities report that at least one of the packages flew on passenger flights before it was discovered. Over 600 attacks worldwide since 1970 have used explosives to target airports and airlines. At least 75% of these attacks caused no fatalities, however a small percentage have been extremely lethal. These cases include the 1985 attack on Air India flight 182 in which Sikh extremists killed 329; the 1988 bombing of Pan American flight 103 over Lockerbie, Scotland, which killed 270; and the 1989 bombing of UTA flight 772, which killed 170. The most lethal recent attacks involving explosives on planes are the coordinated bombings of Sibir and Volga-Aviaexpress flights in 2004, which killed 90. Responsibility for these attacks was claimed by the previously unknown "Islambouli Brigades of al-Qa'ida." Recently, there have also been several thwarted attacks of this nature, including those perpetrated by Richard Reid in 2001, and Umar Farouk Abdulmutallab in 2009.

Qaida to plant bombs in Xmas toys?

Source:http://timesofindia.indiatimes.com/world/uk/Qaida-to-plant-bombs-in-Xmas-toys/articleshow/6886439.cms#ixzz14gf8JJP3

Al-Qaida's chief bomb maker Ibrahim Hassan al-Asiri is reportedly planting bombs in gift toys, which would be timed to explode once the toys are in stores in the UK for Christmas. According to the Daily

Express, intelligence chiefs believe al-Qaida warlords in Yemen plan to smuggle in their deadly cargo aboard freight ships after airport security was tightened following the failed ink cartridge bomb attacks 10 days back. British surveillance experts in Afghanistan and their American colleagues reportedly uncovered the latest threat last week. They intercepted conversations between terrorists from al-Qaida in the Arabian Peninsula (AQAP), the group responsible for the parcel bombs, revealing they were planning a spectacular hit for the festive season. Its leader, American- born cleric Anwar al-Awlaki , and his right-hand man al-Asiri are aiming to use seaports because they believe security is more relaxed there. With so much Christmas stock arriving in the UK, they are confident their toy bombs can remain undetected. " AQAP sees the festive season as the ideal time to strike because of its importance in the

Christian calendar. The bombs found at East Midlands Airport and Dubai escaped scrutiny until the last moment. It would be much easier to plant a similar bomb inside a Christmas toy," an MI5 officer said. Al-Qaida is rumoured to have control of at least 23 ships, nicknamed "Osama bin Laden's navy" , and registered in the names of companies that support the terror group. MI5 and MI6 agents fear the vessels could be used to ferry toys filled with the same explosive used in the ink bombs and last year's failed Christmas Day bomb plot.

Saudi suicide bomber hid IED in his anal cavity

Source: http://www.homelandsecuritynewswire.com/saudi-suicide-bomber-hid-ied-his-anal-cavity

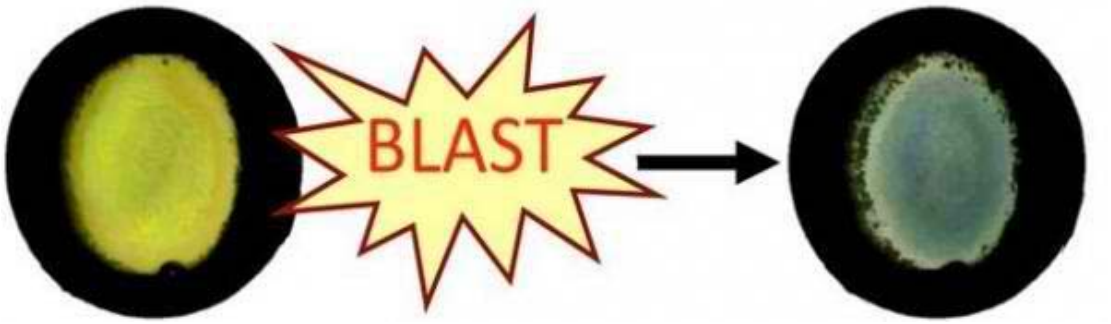
An al-Qaeda-affiliated Saudi suicide bomber, carrying explosives in his anal cavity, managed to get close to the Saudi deputy interior minister and detonate himself (the minister was unharmed); analysts fear this may be a new method of carrying explosives on a plane. An affiliate of al Qaeda has taken a page from the drug mule's playbook, hiding an improvised explosive device (IED) in the anal cavity of a suicide bomber who detonated himself in late August in Saudi Arabia, the Australian Associated Press (AAP) reports. The terrorist, a wanted militant from al-Qaeda on the Arabian Peninsular (AQAP), pretended to renounce terrorism and repent in order to get close to Prince Mohammed bin Nayef, Saudi Arabia's deputy interior minister who leads the kingdom's counter-terrorism campaign. In the attack on August 28, the bomber obliterated himself but the prince survived shaken but unharmed. AQAP claimed credit for the attack in an Internet statement but was coy about the method, declaring: "No one will be able to know the type of this device or the way it was detonated." The AAP credits the U.S. private intelligence services firm, STRATFOR, with the intimate details of the suicide bombing. According to the firm's intelligence report, the bombing signals a paradigm shift in suicide bombing tactics. The third tactical shift is perhaps the most interesting, and that is the use of an IED hidden in the anal cavity of the bomber. Suicide bombers have long been creative when it comes to hiding their devices. In addition to the above-mentioned IED in the camera gear used in the Masood assassination, female suicide bombers with the Liberation Tigers of Tamil Eelam have hidden IEDs inside brassieres, and female suicide bombers with the Kurdistan Workers' Party have worn IEDs designed to make them look pregnant. However, this is the first instance we are aware of where a suicide bomber has hidden an IED inside a body cavity. It is fairly common practice around the world for people to smuggle contraband such as drugs inside their body cavities. This is done not only to get items across international borders but also to get contraband into prisons. It is not unusual for people to smuggle narcotics and even cell phones into prisons inside their body cavities (the prison slang for this practice is "keistering"). It is also not at all uncommon for inmates to keister weapons such as knives or improvised stabbing devices known as "shanks." Such keistered items can be very difficult to detect using standard search methods, especially if they do not contain much metal. Matthew Harwood reports that the firm says that the modest amount of explosives able to fit inside a human anal cavity means the tactic is ideal for assassination. "It does pose real issues for airline security if the bomb is inside the person," Dr. Carl Ungerer, national security policy director for the Australian Strategic Policy Institute."That's why perhaps there is now going to be a real push for these scanning type machines." It is still a mystery how the suicide bomber detonated the IED inside him, although a remote control is the

most likely culprit. The incident does reveal another insecurity. If someone can conceal an IED inside their body, they could carry it on a plane, remove it, and then detonate it in "a strategic location," says STRATFOR.

Color-changing "blast badge" detects exposure to explosive shock waves

Source: http://homelandsecuritynewswire.com/color-changing-blast-badge-detects-exposure-explosive-shock-waves

Researchers develop a color-changing patch that could be worn on soldiers' helmets and uniforms to indicate the strength of exposure to blasts from explosives in the field; blast-induced traumatic brain injury is the "signature wound" of the current wars in Iraq and Afghanistan; with no objective information of relative blast exposure, soldiers with brain injury may not receive appropriate medical care and are at risk of being returned to the battlefield too soon. Mimicking the reflective iridescence of a butterfly's wing, investigators at the University of Pennsylvania School of Medicine and School of Engineering and Applied Sciences have developed a color-changing patch that could be worn on soldiers' helmets and



uniforms to indicate the strength of exposure to blasts from explosives in the field. Future studies aim to calibrate the color change to the intensity of exposure to provide an immediate read on the potential harm to the brain and the subsequent need for medical intervention. The findings are described in the ahead-of-print online issue of NeuroImage. "We wanted to create a 'blast badge' that would be lightweight, durable, power-free, and perhaps most important, could be easily interpreted, even on the battlefield", says senior author Douglas H. Smith, M.D., director of the Center for Brain Injury and Repair and professor of Neurosurgery at Penn. "Similar to how an opera singer can shatter glass crystal, we chose color-changing crystals that could be designed to break apart when exposed to a blast shockwave, causing a substantial color change." D. Kacy Cullen, Ph.D., assistant professor of Neurosurgery, and Shu Yang, Ph.D., associate professor of Materials Science and Engineering, were co-authors with Smith. Blast-induced traumatic brain injury is the "signature wound" of the current wars in Iraq and Afghanistan. With no objective information of relative blast exposure, soldiers with brain injury may not receive appropriate medical care and are at risk of being returned to the battlefield too soon. "Diagnosis of mild traumatic brain injury [TBI] is challenging under most circumstances, as subtle or slowly progressive damage to brain tissue occurs in a manner undetectable by conventional imaging techniques," notes Cullen. There is also a debate as to whether mild TBI is confused with post-traumatic stress syndrome. "This emphasizes the need for an objective measure of blast exposure to ensure soldiers receive proper care," he says. The badges are comprised of nanoscale structures, in this case pores and columns, whose make-up preferentially reflects certain wavelengths. Lasers sculpt these tiny shapes into a plastic sheet. Yang's group pioneered this microfabrication of three-dimensional photonic structures using holographic lithography. "We came up the idea of using three-dimensional photonic crystals as a blast injury dosimeter because of their unique structure-dependent mechanical response and colorful display," she explains. Her lab made the materials and characterized the structures before and after the blast to understand the color-change mechanism. "It looks like layers of Swiss cheese with columns in between," explains Smith. Although very stable in the presence of heat, cold or physical impact, the nanostructures are selectively altered by blast exposure. The shockwave causes the columns to collapse and the pores to grow larger, thereby changing the material's reflective properties and outward color. The material is designed so that the extent of the color change

corresponds with blast intensity. The blast-sensitive material is added as a thin film on small round badges the size of fill-in-the-blank circles on a multiple-choice test that could be sewn onto a soldier's uniform. In addition to use as a blast sensor for brain injury, other applications include testing blast protection of structures, vehicles and equipment for military and civilian use.

Police radar can identify suicide bombers

Source: http://homelandsecuritynewswire.com/police-radar-can-identify-suicide-bombers

The radar guns police use to spot speeding motorists fire microwave pulses at a car and measures the Doppler shift of the reflected signal to calculate its velocity; researchers found that the strength and polarization of the reflected signal -- the "radar cross section" -- can also measure the reflected signal created by the most common arrangements of looped wiring typically used by suicide bombers. The

radar guns police use to spot speeding motorists have inspired a version that aims to identify a would-be suicide bomber in a crowd. A radar gun fires microwave pulses at a car and measures the Doppler shift of the reflected signal to calculate its velocity. Researchers say that the strength and polarization of the reflected signal — the "radar cross section" — can provide additional information about the size and shape of the reflecting object and the material it is made from. Paul Marks writes that William Fox of the Naval Postgraduate School in Monterey, California, and John Vesecky of the University of California, Santa Cruz, wondered whether the wiring in a suicide vest would alter the radar cross section of a bomber enough to allow a radar gun to pick him or her out in a crowd. To find out, the pair used software to simulate how radar signals at 1 gigahertz and 10 gigahertz would be reflected by the most common arrangements of looped wiring typically used by suicide bombers. They found that the clearest reflected signals were in the 10 gigahertz range. Together with colleague Kenneth Laws, they then fired low-power 10 gigahertz radar pulses at groups of volunteers, some wearing vests wired up like suicide vests. About 85 percent of the time, telltale factors in the polarization of the reflected signals allowed them correctly to identify a "bomber" up to ten meters away. The team hopes the U.S. Army will fund further development of the system, allowing them to boost the detection rate and include refinements to avoid false alarms being triggered by metal in underwired bras, jewellery, and earphone leads. The inventors suggest military checkpoints would be major users of such a system — but it could also be installed alongside CCTV cameras in shopping malls, railway stations, airports, and high streets. Overcoming false alarms will be a major challenge, says radar engineer Sam Pumphrey of the U.K.-based research and development company Cambridge Consultants, which is developing a radar system to detect explosives that may have been concealed within the walls of buildings as they were constructed. He thinks a bomb detection system that relies on radar guns alone might well be prone to false positives. Fox agrees. He says that radar can be used in combination with other technologies, including smart surveillance cameras that can identify suspicious behavior , and infrared imaging, which exploits the fact that explosives belts are often cooler than the body. Such a system could help security staff spot bombers from afar and discreetly begin an evacuation.

—Read more in William P. Fox, "Sensing and identifying the improvised explosive device suicide bombers: people carrying wires on their body," Journal of Defense Modeling and Simulation (11 October 2010) (doi: 10.1177/1548512910384604)

X-Flex Blast Protection

Source:http://www.time.com/time/specials/packages/0,28757,2029497,00.html #ixzz17PsI94lq

X-Flex wallpaper won't make your walls aesthetically pleasing, just safe from collapsing from lethal force. This startlingly resilient covering is designed to reinforce buildings against man-made blasts, flying shrapnel and destabilizing natural disasters. Once the wallpaper is applied, its Kevlar-like material, combined with an elastic polymer wrap, becomes virtually stronger than the wall it's shielding — so strong that it's being considered to protect U.S. military bases overseas. Now if only they could make some to cover the windows.

CBRNE-TERRORISM Newsletter

Δελτίο ΧΒΡΠΕ-ΤΡΟΜΟΚΡΑΤΙΑΣ

Volume 5 - 2010

NEW Events

IAEM 58th Annual Conference & EMEX 2010

Event Date(s): Friday, October 29, 2010 to Thursday, November 04, 2010
Location: San Antonio, TX

The IAEM (International Association of Emergency Managers) Annual Conference provides a forum for discussion of current trends and other topics, as well as information about the latest tools and technology in emergency management and homeland security, and otherwise advances IAEM committee work.

3rd Annual CBRNe Convergence Conference

Event Date(s): Tuesday, November 02, 2010 to Friday, November 05, 2010
Location: Orlando, FL
The annual convergence conference provides the opportunity of hearing lessons learned on CBRN, EOD, and IED threats from military and civil agencies covering the merging of response, recent terrorism, conflict, experimentation, real-life exercises, and research & development.

Cincinnati Meta-Leadership Summit for Preparedness

Event Date(s): Wednesday, November 03, 2010 to Thursday, November 04, 2010

Location: Cincinnati, OH

The Meta-Leadership Summit for Preparedness is a unique national initiative to better prepare business, government, and nonprofit leaders to work effectively together during a public health or safety crisis. Leaders learn skills needed for effective action during times of crisis and build organizational connections to strengthen community preparedness for responding to and recovering from emergencies.

Counter CBRN Operations 2011

Event Date(s): Wednesday, February 02, 2011 to Thursday, February 03, 2011
Location: London, UK
Hear the most up-to-date review of international CBRN (chemical, biological, radiological, nuclear) Programmes and Operational Experiences, featuring speakers from the UK, USA, Australia, Spain, Canada, Germany & NATO - and designed to help participants understand how new training methods are preparing CBRN first responders for future operations.

Executive Seminar: Behind the Scenes Seminar of Israel's Counter-Terrorism & Security Operations

Chameleon Associates
Improving Security Through Intelligence

Event Date(s): Saturday, February 19, 2011 to Sunday, February 26, 2012
Location: Israel
Join an international mix of Security, HLS and law enforcement executives in Israel to meet with top security and government officials responsible for protecting some of the highest profile targets in the world. Attendees are granted very special access and insight into Israel's counter-terrorism and security apparatus. Issues on the agenda include securing critical infrastructure, protecting open environments, transit hubs, border control, the role of technology, civilian preparedness and - finding practical solutions to take home.

Global Security Asia 2011

Event Date(s): Tuesday, March 15, 2011 to Thursday, March 17, 2011
Location: Singapore
The GSA Conference Series seeks to discuss the challenges Governments and Homeland Professionals face in their fight against terrorism, and offer possible technological solutions to counter the lurking threats.

Counter Terror Expo 2011

Event Date(s): Tuesday, April 19, 2011 to Wednesday, April 20, 2011
Location: Olympia, London
Counter Terror Expo is the world leading gathering of internationally renowned experts in the field together combined with the world's leading exhibition of technique and technology solutions. Held annually in the host city of the 2012 Olympic Games, this world beating gathering is the principal calendar event of the year for counter terrorism professionals from across the globe.

http://www.sofexjordan.com/

Event Date(s): Monday, May 07, 2012 to Thursday, May 10, 2012
Location: Amman, Jordan
SOFEX is an international exhibition and conference featuring fully integrated Special Operations Forces equipment and solutions. SOFEX showcases the latest counter terrorism and homeland security solutions to combat today's ever increasing security challenges.

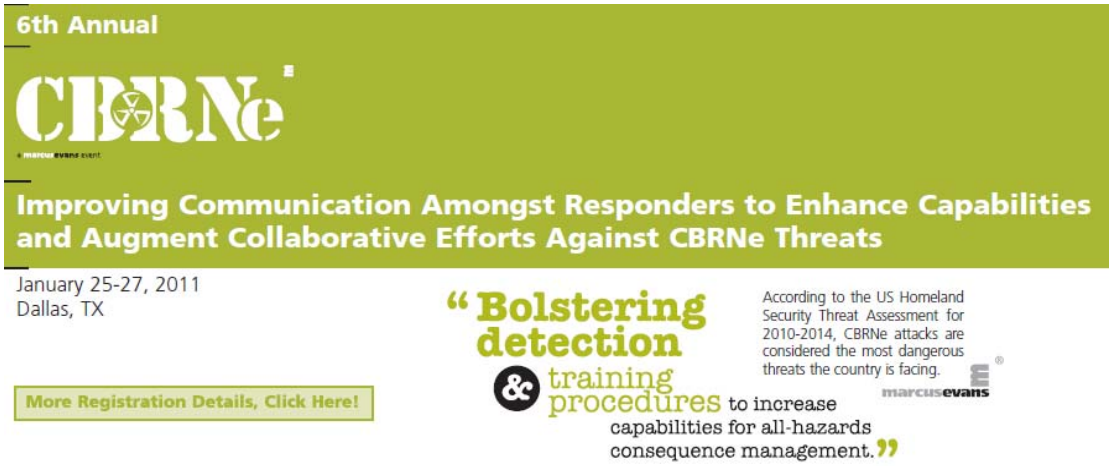
2012 Eurosatory

Event Date(s): Monday, June 11, 2012 to Friday, June 15, 2012
Location: Paris, France
As a forum for meeting and interacting with all the defense players, Eurosatory allows all political-military decision-makers and industry players to obtain, in a single place within five days, all the information they need and to find solutions to all their equipment requirements for military and security forces.

INTERSCHUTZ 2015

Event Date(s): Monday, June 08, 2015 to Saturday, June 13, 2015
Location: Hannover, Germany

INTERSCHUTZ is where all specialists in disaster prevention and rescue whether technicians or managers, volunteers or full-time professionals come to exchange ideas and experience the latest innovations.



ASM BIODEFENSE and Emerging Diseases Research Meeting

February 6-9, 2011 | Omni Shoreham Hotel | Washington, DC

As technology changes and research evolves, professionals involved in biodefense are being challenged to move faster to respond to the growing threat of bioterrorism. In February, scientist, physicians, public health researchers, and policy makers from around the world will converge on Washington, DC to:

- Discover the latest research from microbial sciences related to biodefense and bioterrorism
- Discuss new information on preventative modalities, therapeutics, and clinical diagnoses related to biothreat agents
- Learn about the most recent trends in the management and planning of biodefense programs

Stay up-to-date with the recent advances, participate in sessions led by luminaries in the field, and network with the decision makers who are shaping the future of the bidefense research agenda at the 9th Annual Biodefense and Emerging Disease Research Meeting.

The 2011 ASM Biodefense website is currently under development. The complete website will launch on Thursday, November 11.

GROUP AND REGIONAL DISCOUNTS ARE AVAILABLE FOR SERVING MILITARY, GOVERNMENT AND PUBLIC SECTOR

SMi
LINKING BUSINESS *with* INFORMATION

Introducing the leading forum for CBRN-E professionals in Asia Pacific

CBRN-E Asia-Pacific

Preparing for the Modern Threat

11th & 12th April 2011
Grand Copthorne Waterfront Hotel, Singapore

CONFERENCE HIGHLIGHTS:

- ✔ Attend a dedicated CBRN-E forum unique to Asia Pacific
- ✔ Hear the latest prevent and prepare case studies from key nations in Asia Pacific
- ✔ Stream sessions will let you pick and choose which focus sessions are best for you
- ✔ Interactive panel discussions will let you get your opinion across to the people that matter
- ✔ Network with an eclectic mix of regional and international CBRN-E experts

OUR INTERNATIONAL LINE-UP OF SPEAKERS INCLUDES:


Lieutenant General Chalermsuk Yugala, Senior Army Expert (CBRN), Royal Thai Army


Major General (Professor) Pham Quang Cu, Vice Director General Police Logistics and Technology, Ministry of Defence, Vietnam


Brigadier General Jonathan Treacy, Commanding Officer, Joint Task Force Civil Support, US NORTHCOM


Professor Rohan Gunaratna, Head, International Centre for Political Violence and Terrorism Research (ICPVTR), Singapore


Dr Rajagalopalan Vijayaraghavan, Director, Defence Research and Development Establishment, India


Dr. Abu Hassan Assari Abdullah, Head of Department, Kuala Lumpur General Hospital, Malaysia


Kevin Salim, CBRN Expert, Indonesia


Eric Stevenson, Deputy Director, CBRN Domain, Department of Defence, Australia


Dr Tetsu Okumura, Office of Assistant Chief Cabinet Secretary for National Security and Crisis Management, Cabinet Secretariat, Government of Japan


Major Nick Bowden, Officer Commanding, EOD CBRN-E, New Zealand Defence Force

PLUS TWO FULL DAY POST-CONFERENCE WORKSHOPS

Protecting Critical Infrastructure against CBRN-E Terrorism: Singapore Metro Case Study

In association with ib consultancy

Countering the Terrorist Threat of an IED with a Chemical Payload

In association with ELS Explosive Learning Solutions

DAY ONE Monday 11th April 2011

8:30 Registration and Coffee

OPENING SESSION

9:00 **Welcome Address from the Chairman**
Brian Clesham, Principal CBRN Consultant, **SVGC, UK**

9:10 **KEYNOTE ADDRESS**
Current and Emerging Threat of CBRN-E Terrorism
- Al Qaeda's first and second anthrax programmes
- Jemaah Islamah's chemical and biological programme
- CBRN-E Terrorism in a context
- Future considerations

Professor Rohan Gunaratna, Head, **International Centre for Political Violence and Terrorism Research (ICPVTR), Singapore**

9:40 **SPECIAL ADDRESS**
Countering CBRN-E Terrorism in Asia Pacific
Bill Patterson, Australian Ambassador for Counter Terrorism*

REGIONAL PREPARE & PREVENT PROGRAMMES

10:20 **Detector Development and Medical Countermeasures**
- India's nuclear and radiological threats and the work of the DRDE
- The institute of Nuclear Medicine in Delhi and DRDE Gwalior
- Examining organophosphates for pesticides and the link to chemical defence
- Detector development and medical countermeasures
- The technical and testing requirements for the Commonwealth Games – interoperability and lessons learned
- CBRN research and budget predictions for the future

Dr Rajagalopalan Vijayaraghavan, Director, **Defence Research and Development Establishment, India**

10:50 Networking Coffee Break

11:20 **The Vietnamese Experience of CBRN-E**
- An overview of the CBRN-E programme in Vietnam
- Current organisation and capabilities
- Coordinating the CBRN-E response programme
- Technology and systems integration in Vietnam for CBRN-E response
- Getting the right technology to the correct people
- Training for the military and first response teams
- Future capabilities and evolution

Major General (Professor) Pham Quang Cu, Vice Director General Police Logistics and Technology, **Ministry of Defence, Vietnam**

11:50 **Using Tactical Technologies to Prepare for & Prevent the CBRN-E Threat**
- Training, awareness, coordination and technology – prepare for and prevent the threat
- PDX Basilisk Decontamination System
- PDX Fire Mist
- Cooperation with military partners
- Examples from Operations

Carl Hayton, Engineering Project Manager, **Pursuit Dynamics**
David Crouch, Principal Scientist, **Pursuit Dynamics**

12:20 Networking Lunch

1:30 **Terrorists and CBRN in Indonesia**
- Terrorist activities in Indonesia
- CBRN and Indonesia – an ideal tool for sabotage
- Using chemical agents to disrupt critical national infrastructure
- Al-Qaeda's interest in CBRN and the threat to SE Asia
- 3 pronged deterrent – awareness, detection and legal
- The role of the government in building and improving the capacity to deal with a CBRN threat
- CBRN training being given to first responder teams
- How can we improve?

Kevin Salim, CBRN Expert, Indonesia

2:00 **ANSTO Regional Security of Radioactive Sources Project**
- Overview of activities at the Australian Nuclear Science and Technology Organisation
- Prevention by improving physical protection and security management of radioactive sources
- Emergency preparedness and response for a radiological event involving a dirty bomb or sabotage of a radiation facility

Allan Murray, Manager, Regional Security of Radioactive Sources Project, **Australian Nuclear Science and Technology Organisation**

2:30 **Terrorist CBRN-E Operations against Pakistani Troops Engaged in Counter Terrorism Operations**
- Nuclear threats to Pakistan
- Partnerships with other nations
- Al-Qaida and CBRN capabilities against Pakistan
- Terrorist activities using CBRN-E
- Training military and first response teams to prevent and prepare for the challenge
- Detection and other technologies being used

Assistant Professor Aqab Malik, Department of Strategic and Nuclear Studies, **National Defence University, Pakistan** and Consultant, **National Counter Terrorism Authority, Pakistan**

3:00 Networking Coffee Break

STREAM ONE

Chaired by:
Naoko Noro, Associate Fellow, Research Institute of Science and Technology for Society, Japan Science and Technology Agency

CBR INCIDENTS AND THREATS AGAINST METRO SYSTEMS

3:30 **The Tokyo Sarin Attacks**
- The attacks in a context
- What happened on the day?
- Treating the affected patients on the day – experiences of onsite physician Dr Tetsu Okumura
- CCTV footage – what does the footage from the day teach us?
- Going from slow time thinking to quick time doing
- How Japan has grown stronger after the attacks and current security procedures in place

Dr Tetsu Okumura, Senior Officer on the Countermeasure against NBC (Nuclear, Biological, and Chemical) Threats, Office of Assistant Chief Cabinet Secretary for National Security and Crisis Management, Cabinet Secretariat, **Government of Japan**
Katsuhisa Furukawa, Fellow, Research Institute of Science and Technology for Society, **Japan Science and Technology Agency**

4:00 **Seoul Metropolitan Network Service and CBR Security**
- Assessment of current security procedures and protocols in place on the South Korean Subway
- Guarding against CBR threats and the Daegu subway fire
- Lessons learned following on from attacks against other nation's metro systems
- Increasing CCTV surveillance in Seoul Metropolitaion Network Service

Jong Ho Kim, Seoul Metropolitan Rapid Transit Corporation, South Korea

STREAM TWO

Chaired by:
Brian Clesham, Principal CBRN Consultant, SVGC

CBRN-E MEDICAL COUNTERMEASURES

3:30 **Medical Hospital CBRN Defence in an Urban/Megapolis Environment**
- CBRN threats and targets
- Hospital CBRN operations
- Case study 1: Tokyo's subway sarin incident
- Case study 2: The Goiânia Incident
- Medical/nursing community – the weak link in CBRN planning
- 2004 Olympic Games CBRN defence planning – personal experience
- Case study 3: Singapore's hospital CBRN defence
- The way ahead

Brigadier General (Ret'd) Ioannis Galatas, Medical CBRN Planner/Senior Asymmetric Threats Analyst, Formally Commandant, **2004 Olympic Hospital CBRN Response Unit, Greece**

4:00 **Medical CBRN-E Countermeasures in Vietnam**
- Overview of activities in the Vietnam National Institute of Hygiene and Epidemiology
- Infectious disease in Vietnam
- Preparing preventive vaccines
- Working with other agencies
- Future steps

General (Ret'd) Le Trung Hai, Vice Director, Military Hospital 103, **Ministry of Defence, Vietnam**
Professor Dr Phung Dac Cam, Head, **National Institute of Hygiene and Epidemiology (NIHE), Vietnam**

CLOSING CEREMONY

4:30 **CLOSING KEYNOTE ADDRESS**
Countering CBRN-E Operations in Thailand
- Terrorist use of CBRN-E in Thailand
- Coordinating an effective first response team
- Research and development programmes
- Medical programmes

Lieutenant General Chalermsuk Yugala, Senior Army Expert (CBRN), **Royal Thai Army**

5:00 **Chairman's Closing Remarks and Close of Day One**

DAY TWO Tuesday 12th April 2011

8:30 Registration and Coffee

OPENING SESSION

9:00 Re-Cap from Day One and Setting the Scene for Day Two
Brian Clesham, Principal CBRN Consultant, SVGC, UK

9:30 INTERACTIVE PANEL DISCUSSION
Coordinating an International Response to the Global Threat of Weapons of Mass Destruction
Chairman: Brian Clesham, Principal CBRN Consultant, SVGC, UK
Panellists:
- Brigadier General Jonathan Treacy, Commanding Officer, Joint Task Force Civil Support, US NORTHCOM
- Eric Stevenson, Deputy Director, CBRN Domain, Department of Defence, Australia
- Dr Rajagalopalan Vijayaraghavan, Director, Defence Research and Development Establishment, India
- Assistant Professor Aqab Malik, Department of Strategic and Nuclear Studies, National Defence University, Pakistan and Consultant, National Counter Terrorism Authority, Pakistan

10:30 Networking Coffee Break

INTERNATIONAL CASE STUDIES

11:00 KEYNOTE ADDRESS
US NORTHCOM and CBRN Civil Support Operations
- US NORTHCOM functions and responsibilities
- Homeland defence, civil support and security cooperation to guard against the CBRN-E threat
- Responding to the effects of a CBRN-E incident after civilian resources have been utilized first and fully
- Interoperability with civilian forces before, during and after a CBRN-E incident

Brigadier General Jonathan Treacy, Commanding Officer, Joint Task Force Civil Support, US NORTHCOM

11:30 Military First Responder: Multi Hazard Protection
- Preparing for the CBRN-E threat
- Demron and multi-hazard protection
- Military first responder – The first line of defence
- Military partners - Case studies and examples

Ronald DeMeo, President and Chief Executive Officer, Radiation Shield Technologies

12:00 Australia's Approach to CBRN-E Prevention
- The Australian Ministry of Defence and CBRN-E national security
- Contribution to the government plan
- Australia's approach to prevent
- CBRN terrorism and the countermeasures in place
- Examples from recent case studies
- Securing our future

Eric Stevenson, Deputy Director, CBRN Domain, Department of Defence, Australia

12:30 Advanced Vacuum Technology for B and C Decontamination of Sensitive Equipment & Material
- Operational need of new technology
- Physical properties of C-Contaminants
- B-Decontamination aspects
- Decontamination process
- Hardware to carry out the decontamination
- Applications of vacuum technology

Helmut Stelzmüller, Managing Director, Kaercher Futuretech

1:00 Networking Lunch

2:00 The New Zealand Army CBRN-E Defence Capabilities
- Prevent & prepare – the approach in New Zealand
- Identifying current capabilities
- Situational awareness
- Civil-military cooperation
- Lessons learned and the future of CBRN-E related terrorism in the region

Major Nick Bowden, Officer Commanding, EOD CBRN-E, New Zealand Defence Force

2:30 Threat and Risk Assessment for the EDA and EU DG Home
- Assessing the motivations and capabilities of an actor, actors or actor types
- Using classified government information
- IBC Methodology - use of open source intelligence, making the results accessible for the people that need them
- European Defence Agency - simplified model for threat assessment that can be used for planning of missions
- European Commission DG Home - methodology to deliver three studies for the EU CBRN Action Plan List Groups

Ilja Bonson, Managing Director and Founder, ib Consultancy

3:00 Networking Coffee Break

STREAM ONE
Chaired by:
Brian Clesham, Principal CBRN Consultant, SVGC, UK

COUNTER IED

3:30 Terrorist IED Attacks in the Philippines
- The role of the Office of Transportation Security and C-IED
- Terrorists and IED in the Philippines – case study
- Coordinated IED attacks used against transportation and infrastructure hubs – case study
- The daily threat to critical national infrastructure
- Coordinating a response

Colonel (Ret'd) Dante S Dinsay, Deputy Director, Intelligence and Operations Bureau, Office of Transportation Security, DOTC, Philippines

4:00 The Use of IEDs and Analysis of Serial Blasts in Mumbai in 1993 and 2006
- What, when, where and why's of the coordinated IED attacks in Mumbai in 1993 and 2006. Detailed analysis with focus on reasons for failure. Coordinated IED attacks against Mumbai
- Lessons for LEA (Law Enforcement Agencies), City councils and public
- Preparedness and capacity building for facing such CBRN threats in Metros
- Preventive measures and efficacy
- Protection of critical infrastructure and vital assets

Commodore (Ret'd) Seshadri Vasan, Head, Strategy and Security Studies, Centre for Asia Studies, India & Director Asia Secretariat, Borderpol

STREAM TWO
Chaired by:
Katsuhisa Furukawa, Fellow, Research Institute of Science and Technology for Society, Japan Science and Technology Agency

BUSINESS CONTINUITY

3:30 Community Resilience in Singapore
- Preparing the community in Singapore for a CBRN-E attack
- Managing information and public information during a crisis
- Youth Olympic Games 2010 & Formula One – how to educate and prepare for major sporting events in Singapore
- How can we improve?

Dr Moh Heng Goh, President, Business Continuity Management Institute, Singapore

4:00 How the Commercial World is Dealing with the Threat of CBRN-E
- What to look for when preparing and implementing a CBRN-E emergency response and business continuity plan
- Factors for consideration – study, plan, development, and approval, training and drills
- Incident response and support
- Recovering from a CBRN-E disaster

Industry Speaking Slot Required

CLOSING CEREMONY

4:30 CLOSING KEYNOTE ADDRESS
Malaysia's CBRN Medical Defence Capabilities
- CBRN-E Medical Defence Capability Programme and Committee
- Achieving the vision of the MAFHS – defining the long term strategic plan
- The forward field hospital – laboratory, blood bank, radiology, induction and resuscitation rooms and theatre
- Training doctors and medics in the armed forces
- Case studies from recent operations

Dr. Abu Hassan Assari Abdullah, Head of Department, Kuala Lumpur General Hospital, Malaysia

5:00 Chairman's Closing Remarks and Close of Conference

*subject to final confirmation

POST-CONFERENCE WORKSHOP A 13TH APRIL 2011

Protecting Critical Infrastructure against CBRN-E Terrorism: Singapore Metro Case Study

In association with:

ib consultancy

8:30	Registration
9:00	Introduction and coffee
9:30	Presentation on the modeling effort for the zero situation and the consequences
10:00	Networking coffee break
10:15	Vulnerability assessment and functionality approach
11:30	Heading to the metro station *
12:00	Tour of the facility *
1:30	Networking lunch
2:45	Presentation on actual situation and consequences of an incident
3:45	Questions and answers
4:30	Close of workshop

BENEFITS OF ATTENDING

- Insight into the approach to threat and risk assessments in the European Union,
- Understanding the Comis model and the benefits of its use
- Visit of metro facility and state of the art countermeasures
- Insight into the interactions of countermeasures and the benefits of a system approach
- Improving the understanding of the participants on the consequences of a CBRN attack on a critical infrastructure

Overview:

Attend this workshop where you will receive timely updates on a methodology for risk and threat assessment of critical infrastructure. The assessment will be performed using a real infrastructural object with a relatively high threat level, a metro station. Using the methodology two assessments will be performed, one is fictive a so called zero situation of the metro station where we assume that no countermeasures against CBRN attacks are implemented and one for the actual situation in the station including the active countermeasures. The actual situation which will be assessed during a tour of the facility will be compared to the zero situation. This comparison will show the added value of the countermeasures in terms of lives saved and improved resilience against CBRN attacks.

Andrew Proudlove is a recently retired UK Royal Air Force officer. His last 10 years of Service were spent at NATO HQ, Brussels, where he contributed to the development of NATO's Nuclear Safety and Surety policies and a new policy to combat WMD proliferation.

Rutger Gaasbeek participated in a number of projects related to threat and risk assessment for institutions like the EDA, NATO, the Dutch MOD and the office of internal affairs. In May 2010, Rutger became a fulltime consultant at IB Consultancy, and is currently the research coordinator of CBRN threat analyses.

Who should attend?

- First responders
- Proprietors of critical infrastructure
- Private security staff and personnel
- Policy makers

*subject to final confirmation

POST-CONFERENCE WORKSHOP B 13TH APRIL 2011

Countering the Terrorist Threat of an IED with a Chemical Payload

In association with:

ELS Explosive Learning Solutions

8:30	Registration
9:00	Introduction and coffee
9:30	Chemical IED threat; device design influences and strategic to tactical objectives
10:00	Networking coffee break
10:20	Conventional EOD and IEDD approaches; the shift to non-battlefield techniques in support of civil agencies
11:30	WMD approaches; the paradox of unacceptable events and the risk of hazard reduction actions
12:30	Networking lunch
1:30	Chemical IED options; the utility of remote equipments and manual procedures for diagnostics, containment, segregation and neutralisation
3:00	Networking coffee break
3:20	Task conclusion; forensic, intelligence and criminal follow-up and the residual problem for the supporting agencies.
4:00	Questions and answers
4:45	Summary
5:00	Close of workshop

BENEFITS OF ATTENDING

- Form the linkage to the terrorist threats and consequence risk assessments in order to make an informed investment decision for the allocation of scarce resources
- Be able to review the range of IED chemical payload problems and through scaling prioritise the response options within an understanding of the associated action and residual risks
- Discuss the European direction and implications for counter terrorist operations with any potential reaction of an adaptive thinking terrorist group
- Share the experiences of building a capability that is both tuned to the national requirement, adaptive to the transnational threat and enduring

Overview:

This workshop will set in context the threat from IEDs with a chemical payload and underline the importance of understanding the terrorist objectives in developing a response capability. Traditional EOD concepts of using remote equipment to place hazardous or suspect items into containment vessels for movement may not be appropriate. Where the risk of the device functioning is considered unacceptable then this may require additional approaches. The EDA is piloting an initiative for the capability development of manual neutralisation techniques which support CBRN incidents. Attend this workshop and discuss the requirements and development of a range of counter chemical IED capabilities.

James Convery is co-founder and Director of Explosive Learning Solutions. After a military career delivering national IEDD capability, including close support to UK Special Forces, he now provides non-partisan consultancy to government bodies and assists industry in developing products for the security and defence market.

Graham Brooks works in capability development and has authored plans for NATO, EDA and at national level. He is a retired Army officer with long staff and operational experiences in UK IEDD capability including the delivery and training for national contingencies. He researches terrorist adaption in IED attacks and planning.

Who should attend?

- Military EOD and CBRN staffs and units
- Interior Ministries and Law enforcement
- Civil Defence and Contingency Organisations
- Fire, Rescue and Disaster responders
- HAZMAT and Toxic Chemical specialists
- Command staffs and training directors
- Counter Terror Units
- Crime Scene Investigators and Forensics

RIEAS (www.rieas.gr) supports this very important CBRN conference

CBRNE-TERRORISM Newsletter

Δελτίο ΧΒΡΠΕ-ΤΡΟΜΟΚΡΑΤΙΑΣ

Volume 5 - 2010

OF INTEREST

Selected Literature on Terrorism and CBRN Threats

Source:http://www.terrorismanalysts.com/pt/index.php?option=com_rokzine&view=article&id=140&Itemid=54

Monographs, Edited Volumes, Non-conventional Literature and Prime Articles published since 2000,

Selected by and Compiled by **Eric Price** – Professional Information Specialist

NB: some of the items listed below are clickable and allow access to the full text; those with an asterix [*] only have a clickable table of contents.

Adelman, D.S. & Legg, T.J. (2009). *Disaster nursing: a handbook for practice.* Sudbury, Mass.; Jones and Bartlett Publishers.

[*http://www.loc.gov/catdir/toc/ecip0822/2008028606.html]

Cocciardi, J.A. (2004). *Weapons of mass destruction and terrorism response: field guide.* Sudbury, Mass.; Jones and Bartlett Publishers.

Cummings, C. E. & Stikova, E. (Eds.) (2007). *Strengthening national public health preparedness and response to chemical, biological and radiological agent threats.* [NATO Advanced Study Institute on Strengthening National Public Health Preparedness and Response for Chemical, Biological and Radiological Agents Threats; 2006, Skopje, Republic of Macedonia] Amsterdam, Netherlands: Washington, DC.; IOS Press.

[*http://www.loc.gov/catdir/toc/fy0802/2007930109.html]

Davis, L.E. (2003). *Individual preparedness and response to chemical, radiological, nuclear, and biological terrorist attacks: a quick guide.* Santa Monica, CA.; RAND Public Safety and Justice.

Dolnik, A. (2007). *Understanding terrorist innovations: technology, tactics and global trends.* New York, NY.; Routledge.

[*http://www.loc.gov/catdir/toc/ecip072/2006034183.html]

Drielak, S.C. (2004). *Hot zone forensics: chemical, biological, and radiological evidence collection.* Springfield, Ill.: Charles C Thomas.

Dunston, A. (et al.) (Eds.) (2003). *A citizen's guide to terrorism preparedness and response: chemical, biological, radiological, and nuclear.* New York; American Council on Science and Health.
[*http://www.loc.gov/catdir/toc/fy0711/2003106430.html]

Dunston, A. (et al.) (Eds.) (2003). *New Yorker's guide to terrorism preparedness and response: chemical, biological, radiological, and nuclear.* New York: American Council on Science and Health.

Dwyer, A. (2002). *Jane's Chem-bio Handbook.* Coulsdon, Surrey; Jane's Information Group.

Fountain, A.W. & Gardner, P.J. (Eds.) *Chemical, biological, radiological, nuclear, and explosives CBRNE) sensing X.*[proceedings of SPIE; 14-16 April 2009, Orlando, Florida, United States.] Bellingham, Wash.; SPIE.

Gonenc, I.E. (et al.) (2007). *Assessment of the fate and effects of toxic agents on water resources.* [Proceedings of the NATO Advanced Study Institute on Advanced Modeling Techniques for Rapid Diagnosis and Assessment of CBRN Agents Effects on Water Resources, Istanbul, Turkey, 4-16 December 2005]

[*http://www.loc.gov/catdir/enhancements/fy0825/2007425775-t.html]

Gowen, A.E. (2004). *Surviving terrorism: recognition and response guide to chemical, biological, radiological and nuclear attacks.* Lawrenceville, NJ.: Pinninti.

Howard, R.D. (2008). *Weapons of mass destruction and terrorism.* Dubuque, IA : McGraw Hill.

[*http://www.loc.gov/catdir/enhancements/fy0902/2008298857-t.html]

James, A. D. (Ed.,) (2006). *Science and technology policies for the anti-terrorism era.*

[Proceedings of the NATO Advanced Research Workshop on Science & Technology Policies for the Anti-Terrorism Era. Manchester, United Kingdom, 12-14 September 2004]

[*http://www.loc.gov/catdir/toc/fy0709/2006929619.html]

Jane's Information Group (2011). *Jane's NBC Defence Systems.* Coulsdon, Surrey; Jane's Information Group.

Johnson, T.A. (Ed.,) (2007). *National security issues in science, law, and technology.* Boca Raton: CRC Press.

[*http://www.loc.gov/catdir/toc/ecip073/2006035229.html]

Koenig, K.L. & Schultz, C.H. (Eds.) (2010). *Koenig and Schultz's disaster medicine : comprehensive principles and practices.* Cambridge & New York; Cambridge University Press.

Langford, R.E. (2004) *Introduction to weapons of mass destruction: radiological, chemical, and biological.* Hoboken, N.J.; Wiley-Interscience.

[*http://www.loc.gov/catdir/toc/wiley041/2004299036.html]

Lawson, J. R. & Jarboe, T.L. (2002). *Aid for decontamination of fire and rescue service protective clothing and equipment after chemical biological, and radiological exposures.* Boulder, CO: U.S. Dept. of Commerce, Technology Administration, National Institute of Standards and Technology; Washington, DC.

Lebaron, W.D. (2007). *Five deadly arrows of terrorism: radiological dispersion devices, chemical weapons, biological weapons, nuclear weapons, cyber terrorism: a manual of information and practice.* New York; Nova Science Pub Inc.

Lindstrom, G. (2004). *Protecting the European homeland: the CBR dimension.* Paris : Institute for Security Studies; European Union.

[*http://www.loc.gov/catdir/toc/fy0611/2005455798.html]

MacArthur, S.A. (2002). *Preparing for mass-casualty incidents: hospital readiness for biological, chemical, and radiological disasters.* Marblehead, Mass.; Opus Communications.

Maniscalco, P.M. & Christen, H.T. (2006). *Security officer's terrorism response guide*. Sudbury, Mass.; Jones and Bartlett Publishers.

[*http://www.loc.gov/catdir/toc/ecip062/2005029508.html]

Maniscalco, P.M. & Christen, H.T. (2003). *Terrorism response: field guide for fire and EMS organizations.* Upper Saddle River, N.J.; Prentice Hall.

[*http://www.loc.gov/catdir/toc/fy0711/2003275909.html]

Marmiroli, N. (et al.,) (2007). *Advanced science and technology for biological decontamination of sites affected by chemical and radiological nuclear agents.* [Proceedings of the NATO Advanced Study Instititute on Advanced Science and Technology for Biological Decontamination of Sites Affected by Chemical and Radiological Nuclear Agents, Zhitomir, Ukraine, 17-28 August 2005]Dordrecht: Springer.

[*http://www.loc.gov/catdir/enhancements/fy0825/2007943836-t.html]

Mauroni, A. J. (2006). *Where are the WMDs: the reality of chem-bio threats on the home front and the battlefront.* Annapolis, Md.; Naval Institute Press.

[*http://www.loc.gov/catdir/toc/ecip066/2005037935.html]

McFee, R.B. & Leikin, J.B. (Eds.,) (2008). *Toxico-terrorism: emergency response and clinical approach to chemical, biological, and radiological agents.* New York; McGraw-Hill, Health Professions Division.

[*http://www.loc.gov/catdir/enhancements/fy0708/2007005124-t.html]

McIsaac, J.H. (Ed.,) (2006). *Hospital preparation for bioterror: a medical and biomedical systems approach.* Amsterdam & Boston; Elsevier Academic Press.

[*http://www.loc.gov/catdir/enhancements/fy0634/2006011115-d.html]

Melnick, A.L. (2008). *Biological, chemical, and radiological terrorism: emergency preparedness and response for the primary care physician.* New York; London: Springer.

[*http://www.loc.gov/catdir/enhancements/fy0823/2007940366-t.html]

National Disaster Management Authority (India) (2007). *National disaster management guidelines. Management of* [type of disaster] In 6 vols. [1] Landslides and snow avalanches [2] Chemical (terrorism) disasters [3] Nuclear and radiological emergencies [4] Earthquakes [5] Cyclones [6] mergencies [4] Earthquakes [5] Cyclones [6] Biological disasters. New Delhi: National Disaster Management Authority; Govt. of India.

Phillips, T. A. (2008). *Weapons of mass destruction: the threat of chemical, biological, and nuclear weapons.* Berkeley Heights, NJ.; Enslow Publishers.

[*http://www.loc.gov/catdir/toc/ecip076/2006101161.html]

Prasad, K.N. (2008). *Bio-shield: antioxidants against radiological, chemical and biological weapons.* New York; Strategic Book Publishing.

[*http://www.loc.gov/catdir/toc/fy1001/2009284481.html]

Ranstorp, M. & Normark, M. (Eds.,) (2009). *Unconventional weapons and international terrorism: challenges and new approaches.* London & New York; Routledge.

[*http://www.loc.gov/catdir/toc/ecip0826/2008036719.html]

Read, R.J. & Sussman, J.L. (Eds.,) (2007). *Evolving methods for macromolecular crystallography: the structural path to the understanding of the mechanisms of action of CBRN agents.* Dordrecht; Springer Verlag.

[*http://www.loc.gov/catdir/toc/fy0802/2007475948.html]

Sanyasi, A. (2004). *Extreme emergencies: humanitarian assistance to civilian populations following chemical, biological, radiological, nuclear, and explosive incidents – a sourcebook.* Rugby; ITDG.

Schreier, F. (2009). *WMD proliferation: reforming the security sector to meet the threat.* Washington, D.C.: Potomac Books.

Smith, J. (2009). *A law enforcement and security officers' guide to responding to bomb threats : providing a working knowledge of bombs, preparing for such incidents, and performing basic analysis of potential threats.* Springfield, Ill.; Charles C Thomas.

Sheehan, M. A. (2008). *Crush the cell: how to defeat terrorism without terrorizing ourselves.* New York; Crown Publishers.

[*http://www.loc.gov/catdir/toc/ecip085/2007048444.html]

Terry, E. & Oxer, J. P. (2003). *Survival handbook for chemical, biological, and radiological terrorism.* Philadelphia, Pa.; Xlibris.

Theriault, J-M. & Jensen, J. O. (Eds.). *Spectral sensing research for surface and air monitoring in chemical, biological and radiological defense and security applications.*New Jersey; World Scientific.

Thurman, J.T. (2006). *Practical bomb scene investigation.* Boca Raton; CRC/Taylor & Francis.

[*http://www.loc.gov/catdir/toc/ecip061/2005028445.html]

Urie, R.L. (2001). *Gas masks and civil defense: a practical guide to biological, chemical, and radiological protection*. Pine, CO.; Diomo Books.

Veenema, T.G. (2003). *Disaster nursing and emergency preparedness for chemical, biological, and radiological terrorism and other hazards.* New York: Springer Pub. Co.,

Veenema, T.G. (2009). *Ready RN: handbook for disaster nursing and emergency preparedness.* St. Louis, Mo.; Mosby/Elsevier.

[*http://www.loc.gov/catdir/toc/fy0903/2008036566.html]

Wilkinson, P. (Ed.,) (2007). *Homeland security in the UK: future preparedness for terrorist attack since 9/11*. New York, NY.; Routledge.

[*http://www.loc.gov/catdir/toc/ecip077/2006102050.html]

Wingfield, W.E. (et al.,) (2009). *Veterinary disaster medicine: working animals.* Ames, Iowa: Wiley-Blackwell .

[*http://www.loc.gov/catdir/toc/ecip0826/2008035482.html]

Woolard, D.L. & Jensen, J.L. (Eds.) (2008). *Spectral sensing research for water monitoring applications and frontier science and technology for chemical, biological and radiological defense.* Singapore; Hackensack, NJ.; World Scientific.

[*http://www.loc.gov/catdir/toc/fy0904/2009278866.html]

Non-conventional Literature

Baines, P. (2007). *Hazardous Materials: Chemical Biological Radiological; a review: 2004 to 2007.* [15th International Forensic Science Symposium] INTERPOL; Paris.

[http://www.interpol.int/Public/Forensic/IFSS/meeting15/Papers04.pdf]

Center for Nonproliferation Studies. (2010). *Global Partnership Against the Spread of Weapons and Materials of Mass Destruction.*

[http://www.nti.org/e_research/official_docs/inventory/pdfs/g8.pdf]

Central Intelligence Agency (2007). *Terrorist CBRN.*

[http://www.cia.gov/cia/reports/terrorist_cbrn/CBRN_threat.pdf]

Chalk, P. & Hoffman, B (et al.,) (2005). *Trends in Terrorism; Threats to the United States and the Future of the Terrorism Risk Insurance Act.* Santa Monica; RAND.

[http://www.rand.org/pubs/monographs/2005/RAND_MG393.pdf]

Cilluffo, F.J. (et al.,) (2001). *Combating chemical, biological, radiological, and nuclear terrorism: a comprehensive strategy: a report of the CSIS Homeland Defense Project.*Washington D.C.: CSIS.

[http://www.survivalring.org/nbcprep/combatchembiorad.pdf]

Council of Europe. Committee of Experts on Terrorism. (2007). *Profiles on counter-terrorist capacity: United Kingdom.*

[http://www.coe.int/t/e/legal_affairs/legal_co-operation/fight_against_terrorism/4_theme_files/apologie_-_incitement/CODEXTER%20Profiles%20(2007)%20UK%20E.pdf]

Dixon, L.S. (et al.,) (2007). *Trade-offs among alternative government interventions in the market for terrorism insurance: interim results.* Santa Monica, Calif.; RAND.

[http://www.rand.org/pubs/documented_briefings/2007/RAND_DB525.pdf]

Doesburg, J.C. (2004). *Changes in CBRN Threat.* U.S. Army RDE Command.

[http://proceedings.ndia.org/430C/john_doesburg.pdf]

European Conference of Ministers of Transport - ECMT (2005). *Container Transport Security Across Modes.* OECD; Paris.

[http://www.internationaltransportforum.org/europe/ecmt/pubpdf/05ContainerSec.pdf]

Fradkin, H., Haqqani, H. & Brown, E. (2004). *Current Trends in Islamist Ideology.*Hudson Institute.

[http://www.e-prism.org/images/Paz..pdf]

Frisell, E.H & Oredsson, M. (2006). *Building Crisis Management Capacity in the EU.* Defense Research Agency (FOI); Stockholm, Sweden.

[http://www.foi.se/upload/ASEK/foir1920_building_crisis_management.pdf]

Grlicarev, I. (2008). *Emergency preparedness and response to 'Not-in-a-Facility' radiological accidents.* [Source: IRPA 12: 12. International Congress of the International Radiation Protection Association (IRPA)]

[http://www.iaea.org/inis/collection/NCLCollectionStore/_Public/41/092/41092742.pdf]

HHS Public Health Emergency Medical Countermeasures Enterprise (U.S.) (2007).

*HHS Public Health Emergency Medical Countermeasures Enterprise strategy and implementation plan for chemical, biological, radiological and nuclear threats.*Washington, DC (330 Independence Ave., SW, Washington 20201)

[http://www.phe.gov/Preparedness/legal/boards/nbsb/meetings/Documents/nbsb-mcmreport.pdf]

International Atomic Energy Ageny (IAEA) (2006). *Member State Responsibilities according to International Conventions.*

[www.iaea.org/inis/collection/NCLCollectionStore/_Public/41/067/41067369.pdf]

International Atomic Energy Agency (IAEA) (2006). *The IAEA Nuclear Security Programme Combating Nuclear Terrorism.*

[www.iaea.org/inis/collection/NCLCollectionStore/_Public/41/067/41067362.pdf]

International Student Model United Nations (2010). *Strategic-Level Policy for Preventing the Proliferation of Weapons of Mass Destruction (WMD) and Defending Against Chemical, Biological, Radiological, and Nuclear (CBRN) Threats.* [Thesis, University of Macedonia, Thessaloniki, Greece]

[http://www.thessismun.org/2010/documentation/study_guides/NAC-SG1.pdf]

International Atomic Energy Agency (IAEA) (2006). *Response to Illicit Trafficking of Radioactive Materials.*

[www.iaea.org/inis/collection/NCLCollectionStore/_Public/41/067/41067370.pdf]

Lasker, R.D. (2004). *Redefining Readiness: terrorism planned through the eyes of the public.* New York, N.Y.; New York Academy of Medicine.

[http://tap.gallaudet.edu/emergency/nov05conference/EmergencyReports/RedefiningReadinessStudy.pdf]

McConnell, J.M. (2008). *Annual Threat Assessment of the Intelligence Community.* Senate Armed Services Committee.

[http://armed-services.senate.gov/statemnt/2008/February/McConnell%2002-27-08.pdf]

Moore, G.M. (2010). *International Legal Framework for Nuclear Security.* IAEA; Vienna.

[www.iaea.org/inis/collection/NCLCollectionStore/_Public/41/061/41061875.pdf]

Mwandime, C. (2008). *Country Presentation on Illicit Trafficking of Nuclear Materials.* IAEA; Vienna.

[www.iaea.org/inis/collection/NCLCollectionStore/_Public/41/067/41067359.pdf]

Ramseger, A., Kalinowski, M.B. & Weiss, L. (2009). *CBRN Threats and the Economic*

Analysis of Terrorism.

[www.znf.uni-hamburg.de/OcPaper_No10.pdf]

Reiter, D. (2006). *Preventive war and its alternatives: the lessons of history.* Strategic Studies Institute.

[http://www.strategicstudiesinstitute.army.mil/pdffiles/pub651.pdf]

Reuven, P. (2005). *Global Jihad and WMD: Between Martyrdom and Mass Destruction.*

Intelligence and Terrorism Information Center at the Center for Special Studies (C.S.S)

[http://www.gees.org/documentos/Documen-502.pdf]

Stambaugh, H. (et al.,) (2009). *An airport guide for regional emergency planning for CBRNE events.* Washington, D.C.: Transportation Research Board.

[http://onlinepubs.trb.org/onlinepubs/acrp/acrp_rpt_012.pdf]

Storch, D. & Kenzelmann, M. (2008). *Strategy for responding to nuclear, radiological, biological and chemical threats in Switzerland [ABC- Protection in Switzerland was originally set up primarily for protection against military weapons of mass destruction, such as atomic/nuclear or chemical weapons. Protection against biological weapons..].*

[IRPA 12: 12. International congress of the International Radiation Protection Association - IRPA]

[www.iaea.org/inis/collection/NCLCollectionStore/_Public/41/092/41092722.pdf]

United Kingdom. Secretary of State for the Home Department. *Pursue Prevent Protect Prepare; The United Kingdom's Strategy for Countering International Terrorism.*

[http://www.official-documents.gov.uk/document/cm78/7833/7833.pdf]

United Nations Counterterrorism Implementation Task Force – CTITF (2010).

Interagency Coordination in the Event of a Nuclear or Radiological Terrorist Attack: Current Status, Future Prospects. New York: UN.

[http://www.un.org/terrorism/pdfs/10-48863%20CTITF%20WMD%20Working%20Group%20Report%20Interagency%20coordination%20web.pdf]

United States. Dept. of Defense. Office of Force Transformation. (2003). *Military transformation :a strategic approach.*

[http://www.iwar.org.uk/rma/resources/transformation/military-transformation-a-strategic-approach.pdf]

United States. Federal Emergency Management Agency.(2002). *Are you ready? a guide to citizen preparedness.* Washington, DC.; Federal Emergency Management Agency.

[http://federalhandbooks.lettercarriernetwork.info/A%20Guide%20to%20Citizen%20Preparedness.pdf]

US Army Training and Doctrine Command. (2007). *Terrorism and WMD; in the Contemporary Operational Environment.*

[www.fas.org/irp/threat/terrorism/sup4.pdf]

Prime Journal Articles

Arpad P. (2003). Weapon system selection and mass-casualty outcomes. *Terrorism and Political Violence,* 15 (2, June) pp.81-95.

Becker, S. M. (2009) Preparing for terrorism involving radioactive materials: three lessons from recent experience and research. *Journal of Applied Security Research.* 4 (1) pp.9-20

Blos, M. (et al.,) (2009). The threat of outsourcing US ports operation to any terrorist country supporter: a case study using fault tree analysis. *International Journal of Information and Decision Sciences,* 1 (4, 10 August), pp.411-427.

Bulkeley, J. C. (2007) Decontamination and remediation after a dirty bomb attack; technical and political challenges. *The Nonproliferation Review.* 14 (1), pp.113-138

Bunn, M. (2009). Nuclear bomb squad - looking for a nuclear needle in the haystack. *The Nonproliferation Review.* 16 (3), pp.533 -538.

Cone, D. (et al.,) (2008). Pilot test of a proposed Chemical/Biological/Radiation/ Nuclear-Capable Mass Casualty Triage System. *Prehospital Emergency Care*, 1, (2, April), pp. 236-240.

Carpintero-Santamaría, N. (2010). The incidence of illegal nuclear trafficking in proliferation and international security. *Behavioral Sciences of Terrorism and Political Aggression.*

[*http://www.informaworld.com/10.1080/19434472.2010.512156]

Chalk, P. (2007). Trends in transnational terrorism and implications for U.S. National Security and U.S. Terrorism Risk Insurance Act. *Studies in Conflict and Terrorism*, 30, (9, September), pp.767-776.

Chaput, C. (et al.,) (2007). Disaster training for pre-hospital providers. *Pre-hospital Emergency Care*, 11, (4, October) pp.458-465.

Chyba, C. (2001) Biological terrorism and public health. *Survival: Global Politics and Strategy.* 43 (1), pp.93-106.

Coirier, W. (et al.,) (2005). A computational fluid dynamics approach for urban area transport and dispersion modeling. *Environmental Fluid Mechanics*, 5 (5, October), pp. 443-479.

Cooper, H. H. A. (2006). All bombs are dirty, but some are more dirty than others. *Journal of Police Crisis Negotiations.* 6(2), pp.3-16

Corr, A. (2005) Deterrence of Nuclear Terror; a negligence doctrine. *The Nonproliferation Review.* 12 (1), pp. 127-147.

Currie, J., Caseman, D. & Renee, A.T. (2009). The evaluation of CBRN canisters for use by firefighters during overhaul. *Annals of Occupational Hygiene*, 53 (5, 27 July), pp.523-538.

Cwojdzinski, D. (et al.) (2007). Kontaminationsverdacht: Erstmaßnahmen in der Notaufnahme. *Notfall & Rettungsmedizin*, 10 (5, August), pp.336-342.

Davis, S. & McHenry, K. (2005). A retrospective analysis of mass casualty presentation resulting from the release of toxic chemicals. *International Journal of Emergency Management*, 2 (3, 11 July), pp.231-238.

Desouza, K. C. & Lau, K. A. (2008). Managing the proliferation of weapons of mass destruction: an information management perspective. *International Journal of Public Administration.* 31 (13), pp.1457-1512.

Difilippo, A. (2003). Japan's anti-nuclear weapons policy misses its target, even in the war on terrorism. *Medicine, Conflict and Survival.* 19 (3), pp.235-248.

Eisenkraft, A. (et al.) (2009). Phase I study of a topical skin protectant against chemical warfare agents. *Military Medicine,* 174 (1, January), pp.47-52.

Eisenman, D. P. (et al.,) (2005). Terrorism's psychologic effects and their implications for primary pare policy, research, and education. *Journal of General Internal Medicine*, 20 (8, August), pp.772-776.

Ellingsen, S. A. (2008). Strengthening the second line of defense. *The Nonproliferation Review.* 15 (2), pp.399-402.

Etchegary, H. (et al.) (2008). Canadians' representation of chemical, biological, radiological, nuclear, and explosive (CBRNE) terrorism: a content analysis. *Human and Ecological Risk Assessment: An International Journal.* 14 (3), pp.479-494.

Gao, P. (et al.) (2007). Review of chamber design requirements for testing of personal protective clothing ensembles. *Journal of Occupational and Environmental Hygiene,* 4 (8, June), pp.562-571.

Gressang, D. (2001) Audience and message: assessing terrorist WMD potential. *Terrorism and Political Violence.* 13 (3), pp.83-106.

Hansell, C. (2008). Nuclear medicines's double double hazard - imperiled treatment and the risk of terrorism. *The Nonproliferation Review.* 15(2), pp.185-208.

[http://cns.miis.edu/npr/pdfs/152_hansell_nuclear_medicine.pdf]

Hansell, C. (2008). Practical steps towards a world without civilian HEU. *The Nonproliferation Review.* 15 (2), pp.289-310.

Hochstein, C. (et al.) (2008). Selected resources for emergency and disaster preparedness and response from the United States National Library of Medicine. *Medical Reference Services Quarterly.* 27 (1) , pp. 1-20.

Hoffman, B. (2009) The first non-state use of a chemical weapon in warfare: the Tamil Tigers' assault on East Kiran. *Small Wars & Insurgencies.* 20 (3), pp.463-677.

Hopkins, M. F. (2008).Teaching and Research on the Cold War in the United Kingdom. *Cold War History.* 8 (2), pp.241-258.

Ivanova, K. & Sandler, T. (2007). CBRN Attack Perpetrators: an Empirical Study. *Foreign Policy Analysis,* 3 (4, October), pp.273-294.

Karam, P. A. (2005). Radiological terrorism. *Human and Ecological Risk Assessment: An International Journal.* 11 (3), pp.501-523.

Khripunov, I. (2006). The social and psychological impact of radiological terrorism. *The Nonproliferation Review.* 13 (2) pp.275-316

Kmec, M. (2003) Bioterrorism internet resources for consumers. *Journal of Consumer Health On the Internet.* 7 (4), pp.53-60.

Lane, R. (2004). NATO transformation: the development of a CBRN defence capability. *The RUSI Journal,* 149 (4, 1 August), pp.40-41.

Leitenberg, M. (2009). The self-fulfilling prophecy of bioterrorism. *The Nonproliferation Review.* 16 (1), pp.95-109.

Lemyre, L. (et al.,) (2007). Differential perception of chemical, biological, radiological and nuclear terrorism in Canada. *International Journal of Risk Assessment and Management,* 7 (8, 2 October), pp.1191-1208.

Lien, F. S. (et al.) (2006). Progress and challenges in the development of physically-based numerical models for prediction of flow and contaminant dispersion in the urban environment. *International Journal of Computational Fluid Dynamics,* 20, (5, June), pp. 323-337.

Lugar, R.G. (2008). Reviving up the cooperative nonproliferation engine. *The Nonproliferation Review.* 15 (2), pp.349- 352.

[http://cns.miis.edu/npr/pdfs/152_viewpoint_lugar.pdf]

Martin, B. (2007). Nuclear power and antiterrorism: obscuring the policy contradictions. *Prometheus: Critical Studies in Innovation.* 25 (1), pp.19-29.

Mattox, J.M. (2010). Nuclear terrorism: the 'Other' extreme of irregular warfare. *Journal of Military Ethics.* 9 (2), pp.160-176.

Mauroni, A.J. (2010) Homeland Insecurity: Thinking About CBRN Terrorism.

Homeland Security Affairs, Vol.VI, (3, September), pp.1-17.

Miller, M. (2007) Nuclear attribution as deterrence. *The Nonproliferation Review.* 14 (1), pp.33-60.

[http://www.hsaj.org/pages/volume6/issue3/pdfs/6.3.3.pdf]

Mohtadi, H. & Panini, A. (2009). Risk Analysis of chemical, biological, or radionuclear threats: implications for food security. *Risk Analysis,* 29, (9, September), pp. 1317-1335.

Paltin, D. M. (2003).Chemical and biological violence; predictive patterns in State and terrorist behavior. *Journal of Threat Assessment..* 2 (3), pp.41-68.

Potter, W. C. (2008). Nuclear terrorism and the global politics of civilan HlEU elimination. *The Nonproliferation Review.* 15 (2), pp.135-158.

Quillen C.(2002). A Historical Analysis of Mass Casualty Bombers. *Studies in Conflict and Terrorism,* 25 (5, 1 September), pp.279-292.

Regens, J. L. & Gunter, J.T. (2010). Predicting the magnitude and spatial distribution of potentially exposed populations during IND or RDD terrorism incidents. *Human and Ecological Risk Assessment: An International Journal.* 16 (2), pp.236-250.

Roberts, G. B. (2009). Hostis humani generis: the threat of WMD terrorism and how NATO is facing the ultimate threat. *Defence Against Terrorism Review*. 2, (1, Spring), pp. 1-13

[http://www.tmmm.tsk.tr/publications/datr3/01_Guy%20Roberts.pdf]

Rogers, M. (et al.,) (2007) Mediating the social and psychological impacts of terrorist attacks: The role of risk perception and risk communication. *International Review of Psychiatry*, 19, (3, June), pp.279-288.

Romano, J. A. & King, J. M. (2002). Chemical warfare and chemical terrorism: psychological and performance outcomes. *Military Psychology.* 14 (2), pp.85-92

Salama, S. & Hansell, L. (2005). Does intent equal capability? Al-Qaeda and weapons of mass destruction. *The Nonproliferation Review.* 12 (3), pp.615-653.

Sidel, V. W. (2003). Bioterrorism in the United States: a balanced assessment of risk and response. *Medicine, Conflict and Survival.* 19 (4), pp.318-325.

Sinai, J. (2005). Forecasting terrorists' likelihood to embark on “Conventional” to CBRN warfare. *The International Studies Review,* 7 (1, March), pp.151-153.

Srikrishna, D. (et al.) (2005). Deterrence of nuclear terrorism with mobile radiation defectors. *The Nonproliferation Review.* 12 (3), pp.573-614.

Stavroulakis, P. & Stavroulakis, S. (2008). *International Journal of Technology Transfer and Commercialisation,* 7, (1, 18 June), pp.68-82.

Streeper, C. (2010). Preventing dirty bombs; addressing the threat at the "Source". *The Nonproliferation Review.* 17 (3), pp.531-550.

Sullivan, T.J. & Perry, W.L. (2004). Identifying indicators of chemical, biological, radiological, and nuclear (CBRN) weapons development activity in sub-national terrorist groups. *Journal of the Operational Research Society,* 55 (4, April), pp.361-374.

Swartz, B. J. (2001). Nuclear terrorism - a selection of internet resources. *Internet Reference Services Quarterly.* 6 (3), pp. 7-98.

Tarvainen, T. (2007-8). NATO and the CBRN terrorism - mission: an overview. *Journal of Security Issues* 2(1), pp.24-47.

[http://www.jsiss.net/vols/vol2/Vol2.No1.Art2.pdf]

Tucker, D. (2001). What is New about the New Terrorism and How Dangerous is It?

Terrorism and Political Violence. 13 (3), pp.1-14.

Wilson, R.M. (2008). An overview of U.S. initiatives and technologies to secure shipping containers at overseas ports. *Journal of Applied Security Research.* 3 (2), pp.241-267.

Terrorism Research Centres: 100 Institutes, Programs and Organisations in the Field of Terrorism, Counter-Terrorism, Radicalisation and Asymmetric Warfare Studies

Source:http://www.terrorismanalysts.com/pt/index.php?option=com_rokzine&view=article&id=139&Itemid=54

Compiled by Benjamin Freedman - Editorial Assistant, Terrorism Research Initiative

Who is doing research – academic and otherwise – on terrorism? The field of terrorism research is broad and ever-expanding. Governments sponsor intelligence-driven analytical research agencies. Commercial intelligence firms like J*ane's*, sell their research to corporate and governmental clients. There are think tanks likeRAND, which work closely with government agencies. An increasing number of universities house terrorism research centres, the oldest one being the Centre for the Study of Terrorism and Political Violence at the University of St. Andrews. Then there are virtual networks, such as the Terrorism Research Initiative (TRI), that try to create synergies between a wide array of researchers and topics.

Beyond organizational makeup, notable differences in research approach also exist ,For instance, the gulf between those who work as contractors for homeland security departments and those who work in the policy world. Or, the gap between those who work with classified intelligence and those who work only with open source material. Then there is a divide between those who are considered 'orthodox' scholars and those who call themselves 'critical terrorism scholars' (CTS). The latter, at times, call the former 'terrorologists'; those, in turn, label some from the CTS school 'hypocritical'.

Considering the proliferation of government agencies, private firms, research organizations and internet-based initiatives, the number of newcomers to the field of Terrorism Studies is substantial. Some focus on more general issues like social conflict, armed conflict or political violence topics that often include terrorism-related research. Still others maintain a national, regional, or even global, focus. Much work comes from English-speaking countries and Israel, while other parts of the world are notably under-represented. Trying to create an inventory of such a broad spectrum of research organizations also proves challenging as there are several website-only "centres" directed by a single individual with little visible – or 'credible' – output.

In the following list we present a collection of 100 centres, organisations, institutes, programs and projects that seek to expand the research community's collective knowledge of terrorism, counterterrorism, political violence, radicalisation and asymmetric conflict. In an attempt to provide an overview, a broad array of entities beyond proper academic research centres and institutes have been

included. Though many of the entries on this list may receive government funding, state agencies and departments involved in terrorism research have not been included.

Our list is incomplete and, as such, might leave off centres well worth including. We have tried to include only credible, professional organizations though might not have been fully successful in doing so.

Center, Project, Program, Issue	Affiliated Organization, Institute	Location
Bangladesh Centre for Terrorism Research (BCTR)	Bangladesh Institute of Peace and Security Studies	Dhaka, Bangladesh
Center for Advancing Microbial Risk Assessment (CAMRA)	Michigan State University; Carnegie Mellon University; Drexel University; Northern Arizona University; University of Arizona; University of California at Berkeley; University of Michigan	East Lansing, Michigan, United States
Center for Applied Counterterrorism Studies (CACS)	University of North Carolina at Charlotte	Charlotte, North Carolina, United States
Center for Asymmetric Warfare (CAW)	Naval Postgraduate School	Monterey, California, United States
Center for Counter-Terrorism Studies	China Institute of Contemporary International Relations	Beijing, China
Center for Interdisciplinary Policy, Education, and Research on Terrorism (CIPERT)	Center for Homeland Defense and Security and the Center on Terrorism and Irregular Warfare, Naval Postgraduate School; Pacific Graduate School of Psychology	
Center for International Research on Terrorism (ITRC)	University of Cincinnati; Turkish National Police Organization	
Center for Law and Counterterrorism (CLC)	Foundation for Defense of Democracies	Washington, DC, United States
Center for Policing Terrorism (CPT)	Manhattan Institute	New York City, New York, United States
Center for Terrorism Law (CTL)	St. Mary's University	San Antonio, Texas, United States
Center for Terrorism Research (CTR)	Foundation for Defense of Democracies	Wollongong, Australia

Center on Global Counterterrorism Cooperation		Washington, DC, United States
Center on Terrorism	John Jay College of Criminal Justice	New York City, New York, United States
Center on Terrorism and Counterterrorism	Foreign Policy Research Institute	Philadelphia, Pennsylvania, United States
Center on Terrorism and Irregular Warfare	Naval Postgraduate School	Monterey, California, United States
Centre for Asymmetric Threat Studies (CATS)	Swedish National Defence College	Stockholm, Sweden
Centre for Policing, Intelligence and Counter Terrorism (PICT)	Macquarie University, Sydney, Australia	Sydney, Australia
Centre for the Study of Radicalisation and Contemporary Political Violence (CSRV)	Aberystwyth University	Aberystwyth, Ceredigion, United Kingdom
Centre for Terrorism and Counterterrorism (CTC)	Campus The Hague of Leiden University, Netherlands	The Hague, Netherlands
Centre for the Study of Terrorism and Political Violence (CSTPV)	University of St. Andrews, Scotland	St. Andrews, Scotland
Centre for the Study of Terrorism (CFSOT)		London, England
Center for the Study of Youth and Political Violence	University of Tennessee - Knoxville	Knoxville, Tennessee, United States
Centre for Transnational Crime Prevention (CTCP)		Wollongong, Australia
Center for Higher Study on the Struggle against Terrorism and Political Violence (Centro Alti Studi per a Lotta al Terrorismo e alla Violenza Politica)		Rome, Italy
Charity & Security Network (CSN)		Washington, DC, United States
Chicago Project on Security and Terrorism (CPOST)	University of Chicago	Chicago, Illinois, United States
Columbia University World Trade Center Archive Project	Columbia University	New York City, New York, United States
Combating Terrorism	United States Military	West Point, New York,

Center (CTC) at West Point	Academy	United States
Consortium for Countering the Financing of Terrorism (CCFT)		Singapore
Consortium for Strategic Communication (CSC)	Hugh Downs School of Human Communication, Arizona State University	Tempe, Arizona, United States
Counterterrorism and Homeland Security	Cato Institute	Washington, DC, United States
Counterterrorism Strategy Initiative	American Strategy Program, New American Foundation	Washington, DC, United States
Counterterrorism Topic	Human Rights Watch	New York City, New York, United States
Dark Web Terrorism Research	Artificial Intelligence Laboratory, Eller College of Management, University of Arizona	Tucson, Arizona, United States
Future of Terrorism Project (FTP)	Foundation for Defense of Democracies	Washington, DC, United States
GCC Security and Terrorism Issues Research Program	Gulf Research Center	
Global Terrorism Analysis Program	Jamestown Foundation	Washington, DC, United States
Global Terrorism Research Centre (GTReC)	Monash University, Australia	Melbourne, Victoria, Australia
Global Terrorism Subtopic	National Security Issue, Center for American Progress	Washington, DC, United States
Homegrown Terror & Radicalization Topic	Homeland Security Policy Institute, George Washington University	Washington, DC, United States
Homeland Security and Counterterrorism Program	Defense and Security Program, Center for Strategic and International Studies	Washington, DC, United States
Homeland Security and Terrorism Program	James A. Baker III Institute for Public Policy, Rice University	Houston, Texas, United States
Institute for National Security and Counterterrorism (INSCT)	Syracuse University	Syracuse, New York, United States
Institute for the Study of Violent Groups (ISVG)	University of New Haven	New Haven, Connecticut, United States

Institut fur Terrorismusforschung & Sicherheitspolitik (IFTUS)		Essen, Germany
Institute of Terrorism Research and Response (ITRR)		Philadelphia, Pennsylvania, United States
Inter-American Committee Against Terrorism (CICTE)	Organization of American States	Washington, DC, United States
International Association for Counterterrorism & Security Professionals (IACSP)		
International Center for Terrorism Studies (ICTS)	Potomac Institute for Policy Studies	Arlington, Virginia, United States
International Center for the Study of Terrorism (ICST)	Pennsylvania State University	State College, Pennsylvania, United States
International Center of Terror Medicine	Hadassah Medical Center	Jerusalem, Israel
International Centre for Political Violence and Terrorism Research (ICPVTR)	S. Rajaratnam School of International Studies, Nanyang Technological University, Singapore	Singapore
International Centre for the Study of Radicalisation (ICSR)	King's College, London; University of Pennsylvania; Interdisciplinary Center Herzliya; Jordan Institute of Diplomacy	London, England
International Institute for Counter-terrorism (ICT)	Interdisciplinary Center Center	Herzliya, Israel
Investigative Project on Terrorism (IPT)		
Italian Team for Security, Terroristic Issues & Managing Emergencies (ITSTIME)	Catholic University of Milan	Milan, Italy
Jane's Terrorism and Insurgency Centre		London, England
Jihad and Terrorism Threat Monitor (JTTM)	Middle East Media Research Institute	Washington, DC, United States
Mackenzie Institute		Toronto, Ontario, Canada
Maritime Terrorism Research Center		
Meir Amit Intelligence & Terrorism Information	Israel Intelligence Heritage &	Gelilot, Israel

Center (ITIC)	Commemoration Center	
Memorial Institute for the Prevention of Terrorism (MIPT)		Oklahoma City, Oklahoma, United States
Monterey Terrorism Research and Education Program (MonTREP)	Monterey Institute of International Studies	Monterey, California, United States
National Center for Foreign Animal and Zoonotic Disease Defense (FAZD Center)	Texas A&M University	College Station, Texas, United States
National Center for Risk and Economic Analysis of Terrorism Events (CREATE)	University of Southern California	Los Angeles, California, United States
National Center on the Psychology of Terrorism (NCPT)	Center for Interdisciplinary Policy, Education, and Research on Terrorism	
National Consortium for the Study of Terrorism and Responses to Terrorism (START)	University of Maryland	College Park, Maryland, United States
National Terrorism Preparedness Institute (NTPI)	St. Petersburg College	St. Petersburg, Florida, United States
Nine Eleven Finding Answers (NEFA) Foundation		Washington, DC, United States
Philippine Institute for Peace, Violence and Terrorism Research, Inc. (PIPVTR)		Teachers Village East, Diliman, Quezon City, Philippines
Program for Terrorism Research & Studies	Faculty of Economics and Political Science, Cairo University	Cairo, Egypt
Program on International Terrorism	Elcano Royal Institute	Madrid, Spain
Project Fikra	Washington Institute for Near East Policy	Washington, DC, United States
Quilliam Foundation		London, England
Radicalization Watch Project (RWP)	Center for Advanced Defense Studies	Washington, DC, United States
Russia-Eurasia Terror Watch (RETWA)		

Society for Terrorism Research (STR)		Boston, Massachusetts, United States
Stein Program on Counterterrorism and Intelligence	Washington Institute for Near East Policy	Washington, DC, United States
Terrorism, Transnational Crime and Corruption Center (TraCCC)	George Mason University	Fairfax, Virginia, United States
Terrorism & National Security	Nelson Center for International and Public Affairs, James Madison University	Harrisonburg, Virginia, United States
Terrorism & Preparedness Data Resource Center	University of Michigan Inter-university Consortium for Political and Social Research	Ann Arbor, Michigan, United States
Terrorism and Counter-Radicalization Issue	Carnegie Endowment for International Peace	Washington, DC, United States
Terrorism and Crime Studies	Federal Research Division, Library of Congress	Washington, DC, United States
Terrorism and Homeland Security Research Area	RAND Corporation	
Terrorism and Internal Security Research Cluster	Institute for Defence Studies & Analyses	New Delhi, India
Terrorism Issue	Council on Foreign Relations	New York City, New York, United States
Terrorism Issue	Heritage Foundation	Washington, DC, United States
Terrorism Issue	Institute of Peace & Conflict Studies	New Delhi, India
Terrorist Media Project	Foundation for Defense of Democracies	Washington, DC, United States
Terrorism Page	Anti-Defamation League	New York City, New York, United States
Terrorism Program	Center for Defense Information	Washington, DC, United States
Terrorism Research Center (TRC)	Fulbright College, University of Arkansas	Fayetteville, Arkansas, United States
Terrorism Research Center, Inc. (TRC)		
Terrorism Topic	Human Rights Watch	New York City, New York, United States
Triangle Center on Terrorism and Homeland	Duke University; University of North	Durham, North Carolina, United States

Security (TCTHS)	Carolina, Chapel Hill; RTI International	
Unconventional Warfare Study Center		
US-Russia Initiative to Prevent Nuclear Terrorism	Belfer Center for Science and International Affairs, John F. Kennedy School of Government, Harvard University	Cambridge, Massachusetts, United States
Violence and Extremism Programme	Demos	London, England
Violent Intranational Political Conflict & Terrorism Research Laboratory (VIPCAT)	Institute for the Theory and Practice of International Relations, College of William and Mary	Williamsburg, Virginia, United States
WMD & CBRN Terrorism Topic	Homeland Security Policy Institute, George Washington University	Washington, DC, United States

CBRNE-Terrorism Newsletter wishes:

To all fellow First Responders – civilian and military – worldwide who do their best to keep our societies, families, friends and countrymn safe and alive!

IN PRESS

RIEAS Research Institute for European and American Studies

Certificate in Asymmetric Threats 2011

Research Institute for European and American Studies is developing the curriculum for its 15-weeks "Certificate in Asymmetric Threats" that will be available in Athens, Greece.

Who is the course for?

The course is invaluable for individuals or organizations who have a remit to protect people, infrastructure and supply chains and is ideal for those seeking to update and refresh their knowledge and far more curious about the topic or interested in a career in security, counter-terrorism or homeland security. The course is suitable for participants from:

Emergency Services:
- Police
- Fire & Rescue Services
- Ambulance Services
- Homeland Security
- Incidence Response Teams

Military:
- Army
- Navy
- Air Force
- Special Forces

Governments:
- Policymakers
- Diplomatic Missions
- Civil Services
- Border Security
- Local Authorities
- Courts Services
- Prisons' Management
- Resilience Forums
- Intelligence Services
- Emergency Response Planners

Business Communities:
- Transport Companies
- Communication Providers
- Utility Suppliers
- Finance Houses
- Private Security Contractors
- Aviation Companies
- Shipping & Port Industry
- Security Co-ordinators
- Civil Responders
- Hotel & Restaurant
- Managers
- Business Continuity Managers

Course Model

The course will introduce graduate students to the scope, history, methodology, process and players connected with asymmetric threats. It will provide an overview of the main components of asymmetric threats and study in depth the main parameters comprising asymmetry such as international terrorism, weapons of mass destruction, organized crime, global security and governance, scarcity of energy resources, water wars and climate change. The students will be asked to use their analytical and critical thinking in discussing the above thematology and proceed to more complex issues such as the holistic inter-relationships between of all emerging threats within the global geopolitical turmoil.

Objectives

- Provide an overview of the major components of asymmetric threats and key-players involved;
- Introduce students to challenges and issues currently debated on challenges and dangers deriving from employment of asymmetric threats in the field but also in urban environment; and
- Engage the students in critical analysis of asymmetric threats and its elements, with regard to how it can influence decision making and global policy delivery.

Course Director

BG(ret) Ioannis Galatas, MD, MSc, MC (Army)
Consultant in Allergology & Clinical Immunology
Medical CBRNE Planner
Senior International Terrorism/WMD Analyst
E-mail: igalatas@yahoo.com