Medical/Hospital CBRNE Defence

CBRNE-TERRORISM Newsletter

Volume 37 - 2011

CBRN security at London 2012

ASSISTEX-3 Exercise

Ready or Not 2010

Iranium – the movie

Al-Qaeda's explosives course

New bomb detection tools: Ferns and mice

Stuxnet worm's true origins are exposed

Al Qaeda aiming at soft targets in U.S.

Extremist groups active inside UK universities

www.cbrne-terrorism-newsletter.com

CBRNE-Terrorism Newsletter
Spring 2011

Volume 37
(Spring 2011)

Copyright® 2011

Editor
BG (ret) Ioannis Galatas MD, MA(Terr), MC
Consultant in Allergy & Clinical Immunology
Medical CBRN Planner
Senior Terrorism/WMD Analyst
CBRN Scientific Coordinator @ RIEAS
VC Greek Intelligence Studies Association (GISA)
Athens, Greece
Contact e-mail: igalatas@yahoo.com

Co-Editors/Text Supervisors
Steve Photiou, MD, MSc
Consultant in Internal Medicine &Emergency Medicine
Senior staff member,Emergency Department,
Ospedale Sant'Antonio ULSS 16, Padua, Italy
EMDM Alumni Association Treasurer
Chief, EuSEM Disaster Medicine Section

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

Cover
Moscow airport bombing
Athens' Judge Hall bombing

DISCLAIMER
The CBRNE-Terrorism Newsletter® is a free online publication for the fellow civilian/military First Responders worldwide. The Newsletter is a collection of papers related to the stated thematology, relevant sources are provided and all info provided herein is from open Internet sources. Opinions and comments from the Editorial group or the authors publishing in the Newsletter do not necessarily represent those of RIEAS or the Publisher.

Contents

Reading Public

Editor's Corner

Original Papers

Chem News

Bio News

Dirty News

Explo News

Cyber News

Terror News

New Upcoming Events

CBRNE-TERRORISM Newsletter

Medical/Hospital CBRNE Defence

CBRNE-TERRORISM Newsletter

Volume 37 - 2011

CBRN security at London 2012

ASSISTEX-3 Exercise

Ready or Not 2010

Iranium – the movie

Al-Qaeda's explosives course

New bomb detection tools: Ferns and mice

Stuxnet worm's true origins are exposed

Al Qaeda aiming at soft targets in U.S.

Extremist groups active inside UK universities

CBRN-E Asia Pacific 11th - 12th April 2011, Singapore

www.cbrne-terrorism-newsletter.com

CBRNE-Terrorism Newsletter is published quarterly and distributed on-line free of charge

Starting from "Summer 2011" issue all advertisements will be charged as following:

Full page (A4)	€1.000
Half page	€ 700
Quarter page	€ 500
Inside front cover	€1.100
Inside back cover	€1.200
Outside back cover	€1.300

Free capability profile will be provided to all advertisers in the same issue (length: 200 words + one picture + logo in .jpg format)

20% reduction for annual ad inclusion

New features	Original papers from around the globe & new format
Distribution	+50 countries
Recipients	Colleagues from more than 550 think tanks, organizations, companies, institutions, ministries
Free download	http://www.rieas.gr http://www.mendor.gr
Contact Editor	igalatas@yahoo.com

Reading Public

Our reading audience comes from **54 countries** all over the world and is constantly expanding. Currently colleagues and affiliates from **over 550** organizations, companies, institutions, ministries and the first responders are recipients of CBRNE-Terrorism Newsletter.

Europe

Greece

- Hellenic Air Force
- General Secretariat of Civil Protection
- Athena Academy & Athena Worldwide LLC
- Carrier Corporation
- US Embassy Athens
- Greek Government (PM Office)
- Dupont Greece
- Presscode Network
- National School of Public Health
- Meditime
- Special Olympics World Summer Games ATHENS 2011
- National Centre of Emergency Care
- PricewaterhouseCoopers
- PwC
- Panteion University of Athens
- National Centre for First Aids (EKAB)
- TUA (ChemEng Department)
- National Technical University of Athens
- iQ Studies
- Kapodistriakon University of Athens (Medical School)
- National Nursing University School
- Ministry of Defence
- National Intelligence Service
- Hellenic Police
- Athens' EOD Squad
- Joint Military Intelligence Division (Hellenic National Defence General Staff)
- Epipleon Security
- Athens' International Airport S.A.
- PNOI S.A.
- National Security School
- National Authority for Chemical Weapons

Netherlands

- Military Hospital (Utrecht)
- VSTEP BV
- TNO Defence, Security and Safety
- Organization for the Prohibition of Chemical Weapons (OPCW)
- Netherlands Defence Academy
- National Security and Intelligence
- TU Delft
- White Queen BV
- Militaire Spectator Journal
- NATO werkgroep Force Health Protection
- Inspector General Military Health Care
- Meander Medical Center Amersfoort
- Joint CBRN Centre of Expertise (MoD)
- Ministry of Education, Science and Culture
- University of Amsterdam
- Blücher NL BV
- The Hague Centre for Strategic Studies
- International Center for Prehospital and Disaster Medicine
- ISAC Foundation
ASIS International
- Chemicals& Safety International (CASI)
- Delft University of Technology
- International Committee of Military Medicine
- Defence Intelligence and Security Service
- CBRN consultancy Bourgondien
- European Stadium and Safety Management Association
- Ministry of Defence (DEOD-DC)
- IB Consultancy
- NLD Ministry of Defence (Regional Military Command South)
- National Operations Centre
- iXeR.nl
- Sperian Protection
- The Hague Airport
- KPMG
- Europol
- Hutter Security

Cyprus

- European University Cyprus
- Cyprus Nurses & Midwives Association
- Ministry of Defence

Serbia

- Institute for Strategic Research
- University of Belgrade (Faculty of Security Studies)
- Academy of Diplomacy and Security
- Media Wizards Company

Romania

- ATC Systems
- Ministry of Defence
- University of Bucarest

Slovak Republic

- Pravda daily
- Euro-Atlantic Quarterly

Monaco

- Aviation Club International

Iceland

- Iceland Fire Authority
- Security Center of Iceland

Sweden

- Swedish Rescue Training Centre (SRTC)
- Gotlands kommun (Safety & Security)
- SIPRI
- Institute for Security and Development Policy
- SECRAB Security Research
- European CBRNE Center
- The Swedish Fire Protection Association (SFPA)
- National Intelligence Section
- University of Umea
- Swedish Fire Research Board
- Swedish Radiation Safety Authority
- Operative Security Academy
- Swedish Defence Research Agency (FOI)

Finland

- Technology Industries of Finland
- Environics Oy
- Observis Oy

Norway

- Norwegian Cruise Lines
- Nordic Safety and Security Academy (NSSA)
- Norwegian Air Shuttle
- MilitærTeknikk

Croatia

- Zaštita (Protection) Journal

Italy

- Zep Italia
- SeMeL.biz
- SeMeL International
- Top Search
- Bonuomo Security
- Protezione Civile Perugia
- University of Milan
- NATO (JFC Naples)
- Padova Hospitals
- EMS 118 Torino
- Istituto Nazionale Malattie Infettive Lazzaro Spallanzani
- Western Defence Studies Institute
- Mediterranean Center for Intelligence Studies (MCIS)
- UNICRI
- Cristanini SA (decontamination)
- Centro di ricerca in Medicina d'Emergenza e dei Disastri (CRIMEDIM –Università Piemonte Orientale)
- CTBTO
- ENI
- San Camillo Forlanini Hospital
- Canadian Embassy Rome
- Link Academy (Link Campus University)
- Italy Legal Focus

Belgium

- Belgian Ministry of Defence
- NATO Naval Mine Warfare Center of Excellence
- Belgian Netherlands Naval Minewarfare School
- European Parliament
- Supreme Headquarters Allied Powers Europe
- NATO (CBRN)
- Integrated Defence Solutions Forum
- European Strategic Intelligence & Security Centre
- JCBRNC Belgium
- Federal Police (K9)
- Rezidor Hotel Group
- Institute of Civil Protection and Emergency Management
- Council European Union
- European Union Military Staff
- European Security Round Table
- G4S Security Services
- Belgian Ministry of Health
- UNDAC (United Nations OCHA)
- Notary Public
- Hatzoloh of Antwerp Medical Emergency Response Team

Denmark

- Danish Institute of Fire and Security Technology
- Danish Technical University
- Danish Emergency Management Agency
- Statens Serum Institut
- Nestle
- ASIS International
- Centre for Military Studies (University of Copenhagen)

Switzerland

- Swiss Federal Office of Public Health
- Centre for Security Studies (Swiss Federal Institute of Technology)
- Federal Office for Civil Protection (FOCS)
- Spiez Laboratory
- ICRC
- FIFA
- i-intelligence
- Event Knowledge Services (EKS)
- ABC Zentrum, Spiez

Estonia

- Baltic Defence College

Luxemburg

- FRS Global
- People Primetime Ltd

Germany

- EU Exchange of Experts in Civil Protection
- Bruker Daltonics GmbH
- George C. Marshall European Centre for Security Studies
- European Organisation for Security
- Kroll Security Group
- Dramaworks GmhH
- DHL Express
- A.I.P.International
- Military Technology Magazine (Mönch Group)
- Joint Movement Operations Center (Special Operations Command Africa)

Austria

- EMS Vienna
- IAEA
- CTBTO/OSI
- Hot Zone Solutions GmbH
- DMAT Consulting KG
- NBC-Defence School "Lise Meitner"

France

- Paul Boye Technologies
- Thales
- NBC-Sys
- Airbus
- The Croissant

Turkey

- GATA

Portugal

- MRINetwork MRIWW
- Presidência do Conselho de Ministros

Spain

- General Directorate of the Guardia Civil
- SCOTT Health & Safety
- University of Cadiz

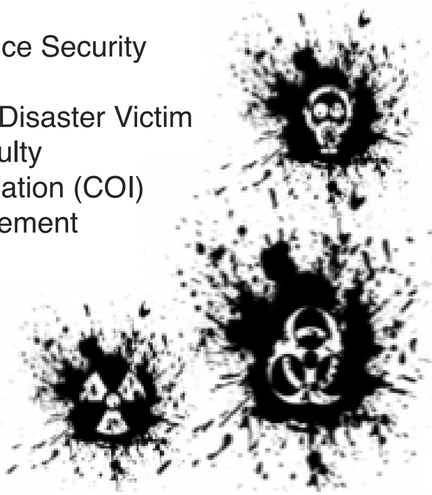
Poland

- RAPORT-wto Defence Magazine

United Kingdom

- Future Intelligence Journal
- RAND Europe
- ISS Pegasus
- Surrey County Counci
- HQ NATO
- Health Protection Agency (HPA)
- NHS London SHA
- NHS South East Coast
- Institute of Risk Management
- Royal United Services Institute (RUSI)
- London Organising Committee of the Olympic Games
- Kent County Council
- Centre for Defence Studies at King's College London
- Organization for the Prohibition of Chemical Weapons (OPCW)
- Ministry of Defence
- Explosive Learning Solutions Ltd
- National Counter Terrorism Security Office (NaCTSO)
- Thales CBRNe Research
- London Ambulance Service (Olympic Games Planning Office)
- Bruhn NewTech
- SMi (Defence & SecurityTeam)
- CBSbutler
- Police National CBRN Centre
- Atkins Global
- CBRNE Ltd
- Pursuit Dynamics
- Union Industries Ltd
- SCS Ltd
- Haztek International
- HazmatLINK Ltd
- Cap SP&CBRN
- Chemical & Biological Warfare Review
- Smiths Detection
- Scott Health & Safety
- Crisis Management Centre
- Chatham House
- Aviation Security International Journal
- Green Light Ltd
- Satovarac Consulting
- Risk Advantage Consulting Services Ltd
- CC Consulting
- S.A.B.R.E
- Public Safety Associates Ltd
- Metropolitan Police Service
- City Security and Resilience Network (CSARN)
- SSR
- Adviser
- Coventry University
- Serco
- East Kent University Hospitals Trust
- North Yorkshire Police
- PSD Group
- Future Intelligence
- NHS London SHA
- Jane's Information Group
- Police Newcastle upon Tyne
- Newcastle City Council
- Milton Keynes Council - Risk & Business Continuity
- NHS Sutton & Merton
- Institute of Civil Protection & Emergency Management
- Institute of Civil Protection and Emergency Management (ICPEM)
- Centre for Disaster Management (Coventry University)
- South West Strategic Health Authority

- Scott Health & Safety
- Bucks New University
- The Salvation Army
- Government Decontamination Service
- University of Brighton
- University of Bath
- Local Authority Olympic Resilience Team at Local Government Association
- Real-Time Consultants
- Government Office East Midlands
- De Boer Structures
- International School for Security & Explosives Education (ISSEE)
- SELEX SAS
- The Counter-IED Consultancy
- Dundee City Council
- Royal Borough of Windsor and Maidenhead
- CitySafe
- University of Leicester (Risk, Crisis & Disaster Management)
- Liverpool City Council
- Police National Search Centre (PNSC)
- Security Watch India @ UK
- London 2012 LOCOG
- IHS Jane's
- Aegis Defence Services Ltd
- Crisis Response Journal
- IAFPA Bulletin
- The Shephard Group
- Andersen Steinberg Consulting
- Allen-Vanguard
- PiPerform Ltd
- SELEX Communications Ltd
- Clarion Events (Counter Terror Expo 2011)
- CBRNe World Journal
- Shadow Robot Co
- London Technology Network (LTN)
- Cranfield University
- Centre for the Study of Terrorism and Political Violence
- University of Leicester
- Ex Military Personnel
- 999team
- EU project COST
- University of Bath
- Hazardous Ops
- Cardiff County Council
- Northrop Grumman Mission Systems Europe (NGMSE) Ltd
- BIOAXIS Healthcare
- Hanover Associates (UK) Ltd
- UK Home Office
- Shaping Tomorrow
- AWICP - Asymmetric Warfare Intelligence for Close Protection Operations Ltd.
- SOFITEL London St. James Hotel
- Zest4 Training Ltd
- NHS East Midlands Ambulance Service
- University of Portsmouth (Security Institute)
- Crisis Solutions
- Circuit Magazine
- CornerStone GRG Ltd
- King's College London (Department of War Studies)
- Top 3 Percent Club
- Infantry Battle School (IBS) Brecon
- Stuart Harrison UK
- Brunel University (Centre for Intelligence and Security Studies)
- Athena Security & Intelligence Consultants Ltd
- radeBytes UK
- Royal Army Medical Corps
- UK Defence Forum
- GDS
- Bucks New University
- Mark Allen Group
- EMS CONSULTANT
- Emergency Planning Solutions Ltd
- London Ambulance Service
- Guy's and St. Thomas' NHS Foundation Trust
- UCL (Jill Dando Institute of Security and Crime Science)
- Smiths Detection (2012)
- G4S
- UK Consultants
- British Red Cross
- 352nd SOG
- Yorkshire Ambulance Service NHS Trust
- PN CBRN Centre (Coventry)
- ISS FS Security (Goldman Sachs)
- Mass Spec Analytical Ltd.
- BDEC Ltd
- Stephenson Resilience
- S.I.S. Service Intelligence Security
- Sefton Council
- Counter Terrorism and Disaster Victim Identification (DVI) Faculty
- Central Office of Information (COI)
- Institute of Risk Management
- Veterus Consulting Ltd.
- Civil Service UK



- Care & Social Services Inspectorate Wales
- 1st Security News
- Royal College of Nursing
- Association of the British Pharmaceutical Industry
- University of Leicester
- Oxfordshire County Council
- Central London Community Healthcare
- Royal Borough of Kingston
- Derby Hospitals NHS Foundation Trust
- The City of Edinburgh Council
- Guy's & St Thomas' NHS Trust
- CIR Magazine
- Sage (UK) Ltd.
- Babcock International Group PLC
- Kratos Enterprises Ltd
- SMi Group
- Cabinet Office
- East of England Ambulance Trust
- BBC
- Matom

Africa

South Africa

- African Centre for Disaster Studies (North West University Potchefstroom Campus)
- Sabre International
- Metropolitan Police (Port Elizabeth)
- Helen Joseph Hospital, Gauteng Department of Health

Kenya

- International Federation of Bio-safety Associations (IFBA)

Burundi

- Burundian Ministry of Defence

Middle East

Israel

- The Interdisciplinary Center, Herzliya
- International Security Academy
- Sabre International Security
- IIR
- Institute for the Study of Asymmetric Conflict (ISAC)
- Global Medical Service
- Adelson Institute for Strategic Studies at Shalem Center
- Institute of Terrorism Research and Response
- Teva Pharmaceutical Industries LTD
- IB Consultancy
- ID-Sec Solutions Ltd
- Beth-El Industries Ltd.
- Arttic
- Community Counter Terror Rapid Reaction Force (Ginot Shomron)
- Denoman International Ltd
- Bar Ilan University
- Maala2
- ISDS Ltd
- Arttic
- National Center for Trauma and Emergency
- The Ben Gurion University
- Israel Airport Authority
- ASERO Worldwide
- Athena GS3 – Security Implementations Ltd
- Imco Industries Ltd.
- IS4 International Ltd

Jordan

- Elite Aviation
- Public Security Directorate
- University of Jordan
- Intercontinental Jordan
- Jordan Gendarmerie Forces

UAE

- Global Strategies Group
- National Bank of Abu Dhabi
- Lysys
- United Arab Emirates University
- Abu Dhabi Police
- UAE Critical National Infrastructure Authority

Saudi Arabia

- Ministry of Defence
- Disaster Recovery
- DSFH
- G4S Security Services
- King Abdullah University of Science and Technology (KAUST)
- EADS

Qatar

- Qatar Olympic Committee - Arab Games 2011

- AFC Asian Cup Qatar 2011 Local Organizing Committee
- Institute for Security, Science and Technology (Imperial College)
- Qatarlyst

Kuwait
- Jumeirah Group

Bahrain
- RTI Group LLC

Asia

Russian Federation
- Sochi 2014
- Biological Threat Reduction Program

India
- Security Watch India
- Mahindra & Mahindra Group (MSSG)
- Environics Oy
- Greentech Foundation
- Totem International Ltd
- CRIDYNE
- SWTECH
- Eldynegroup Electro Systems Pvt Ltd
- Kirkhope Consulting International
- Rockland Hospitals Group
- Lal Bahadur Shastri Institute of Management
- Totem

Japan
- Sompo Japan Risk Management, Inc
- USMC Japan

China
- UNISDR
- International Association of Emergency Managers
- PyeongChang2018
- Heart-to-Heart International

Pakistan
- National Counter Terrorism Authority

Afghanistan
- Counter Insurgency Training Centre
- SOTF Southeast

Azerbaijan
- International Security Research Centre of Azerbaijan

Singapore
- National Security Coordination Centre
- SMi Group Asia-Pacific
- iJet
- NSCS
- Control Risks
- Ministry of Finance
- National Institute of Education
- Nanyang Technological University
- Business Continuity Management Institute

Philippines
- CBRN Defense & Emergency Response

Malaysia
- Avon Protection Systems

Indonesia
- US Embassy Indonesia

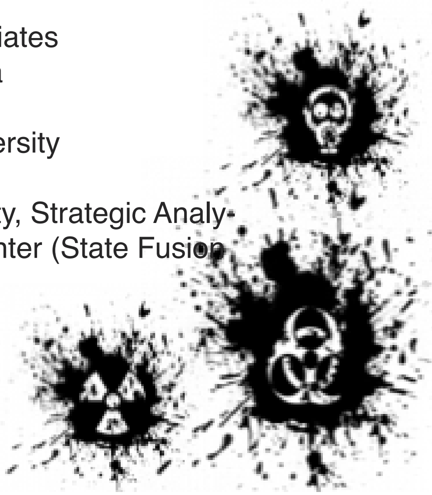
Oceania

Australia
- Explosive Protective Equipment (EPE)
- Centre for Policing, Intelligence and Counter-Terrorism (PICT – Macquarie University)
- Commonwealth Games Federation (CGF)
- Sydney Opera House
- Australian Security Academy

N Zealand
- Ministry of Defence (EOD/CBRNE)

North America

United States
- Remote Medical Associates
- University of Minnesota
- BAE Systems
- American Military University
- Raytheon
- Ohio Homeland Security, Strategic Analysis and Information Center (State Fusion Center)



- Paramount Pictures in Hollywood, California
- Security Cosmopolitan Journal (Las Vegas)
- Center for Hemispheric Defense Studies
- Transportation Security Agency (TSA)
- Notre Dame College (Security Policy Studies)
- Notre Dame College (Center for Intelligence Studies)
- University of Rhode Island (National Institute for Public Safety Research and Training)
- Strategic National Stockpile (CDC)
- The Business Continuity Institute
- Capella University (Public Safety - Criminal Justice/Forensics, School of Public Service Leadership)
- Disaster Recovery Journal
- Yale University
- International Assessment and Strategy Center
- High Alert International
- BCO 22nd Chemical BN
- Institute of Terrorism Research and Response (York)
- NEFA Foundation
- Organum Intelligence Company (OIC)
- Federal Bureau of Investigation (JTF)
- U.S. Secret Service
- American Jewish Committee (Division on Middle East and International Terrorism)
- US Gov (ChemBio Defense T&E Div)
- Harvard School of Public Health
- World Policy Institute
- 22d Chemical Battalion
- Camber Corporation
- Anti Terrorism Accreditation Board
- The Associated Press
- KD Analytical Consulting
- GEOMET Technologies, LLC
- Regent University (International Politics and Terrorism Studies)
- Pentagon Force Protection Agency (CBRNE Response)
- Walt Disney World Swan and Dolphin
- Fletcher School (Institute for National Security Studies)
- The Joint Staff
- Northwestern State University (Criminal Justice Department (Homeland Security)
- DoD Defence Threat Reduction Agency (CBRNE)
- USMC (Antiterrorism Program)
- US Army Korea (CBRN)
- SAIC
- Security Management Resources
- University of Nevada Las Vegas
- George Mason University
- US State Department (CBWs)
- Stress Centre of North Mississippi
- Human Intelligence Productions
- University of Maryland University College
- U.S. Army Chemical Materials Agency
- University of Missouri
- Northrop Grumman Corporation
- Task Force V.I.P.E.R.
- New York State Fire
- Safety Equipment Institute
- The Jamestown Foundation
- Georgetown University
- Missouri Department of Mental Health
- University of Arkansas
- US Army (CBRN Ops)
- Small Wars Foundation
- Naval War College
- Colorado State University
- SAIC
- EOD Technology, Inc
- NEWS OF THE FORCE
- Phoenix Global Intelligence Systems
- Safety Training and Consultations International LLC (STCI)
- US. Dept of Navy
- Coalition for Tactical Medicine
- George Washington University (Homeland Security Policy Institute)
- US Army (TRADOC)
- American Center for Democracy
- Economic Warfare Institute
- Institute for the Future (IFTF)
- Multifaceted Media Group
- US Department of Homeland Security
- Homeland Security Group
- ASIS International
- Camber Corporation
- Advanced Concepts & Technologies International (ACT-I)
- Trelleborg-Viking, Inc.
- Paul R. Laska Forenisc Consulting, Inc.
- USMC
- Tex-Shield, Inc.
- The Galatas Group
- Force 1 Decon

- James Lee Witt Associates
- NBC Industry Group
- BayCare Health Systems
- National Association of EMT's
- New York Downtown Hospital
- Kaiser Permanente Medical Group
- Long Beach Medical Reserve Corp
- Institute for National Security & Counterterrorism (INSCT)
- IEM
- RAND Organization
- The International Association for Counterterrorism & Security Professionals
- CTSERF
- Center for Security and Emergency Management, Inc. (C4SEM)
- International Association of Emergency Managers (IAEM)
- Massachusetts Department of Fire Services
- NATO Allied Command Transformation
- WMD Civil Support Team (New York)
- The Linc Group
- Smiths Detection
- Freeport Rural Ambulance Service
- Star Ambulance
- Battelle
- US Department of Health & Human Services
- Lion Apparel
- Advanced Engineering Solutions
- University of South Florida
- Asymmetric Warfare Center
- WorldThreats.com
- Sandia National Laboratories
- U.S. Naval Postgraduate School
- 21st Century Defence Initiative (The Brookings Institution)
- Environics Oy USA
- Nucsafe Inc.
- CACI International Inc. (CBRN)
- George C. Marshall Centre
- NYS Department of Health
- Crisis Management Group, LLC
- Centre for Advanced Studies on Terrorism (LA)
- The Cato Institute
- Counterinsurgency Center (US Army)
- The Brookings Institution
- Stratfor
- MARFORPAC CBRN (USMC)
- The Washington Post
- COBRA Training Facility (DHS FEMA)
- U.S. Army War College Strategic Studies Institute
- Santa Rosa Consulting
- Centre for Emergency Response and Terrorism
- Joint Special Operations University
- Centre for National Security Law (University of Virginia School of Law)
- DuPont USA

Canada

- Canadian Security Intelligence Service
- Canadian Tactical Training Academy
- Allen-Vanguard Corporation
- GCIS Strategies Group
- MED-ENG SYSTEMS INC
- CBRN Defence
- Royal Military College of Canada
- ContinuityLink

South America

Argentina

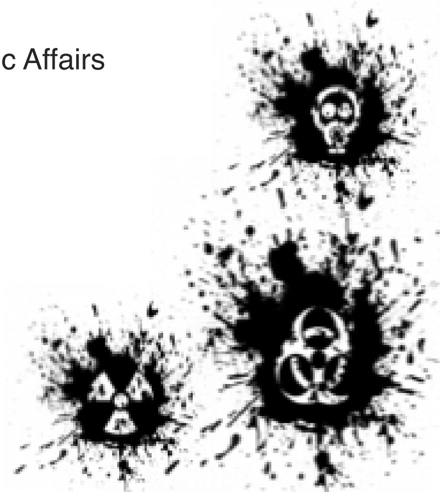
- International Security Defence Systems, LLC
- Dr. Cosme Argerich Acute General Hospital

Brazil

- House of Representatives
- Performance Global
- Sao Paulo State Civil Police Academy
- 2014 FIFA World Cup Brazil Organizing Committee
- Government Federal Administration

Peru

- Council on Hemispheric Affairs



Editor’s Corner

Editorial

Dear Colleagues,

It gives. me great pleasure to complete the “Spring-2011” issue of the CBRNE-Terrorism Newsletter in its new format.

Starting from this issue and with your valuable contribution and enthusiasm, original papers were also included along with the standard articles’ collection and news from around the globe. The new format will give a more professional look to the Newsletter although the target will remain unchanged – tCBRNE and Terrorism issues. Your future contribution will be highly appreciated and sharing knowledge and information will be the tool for a safer world in an era of global turbulence.

Another important development into this lonely until know editorial effort, is that now two colleagues (Steve Photiou MD, MSc from Padova, Italy and Nikolaos Kokkotas, MSc from Athens) joint the editorial team of the Newsletter and with their assistance and supervision we will manage to correct the little details on text editing and the general format and appearance of the content along with the professional assistance of our publisher (Valia Kalatzi, MSc).

A third important issue is that starting from “Summer-2011” issue all advertisements will be charged according with the price table provided in page 3. Prices will be most competitive because our aim is to cover only our functional expenses and save some money in order to subscribe to more specialized webs or journals that will allow us to provide more detailed and updated information to our readers.

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

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

Editor

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

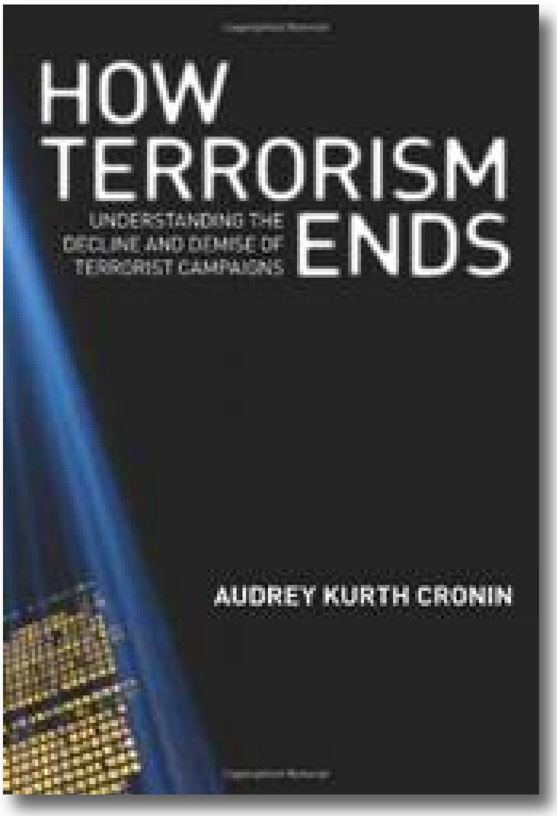
How Terrorism Ends

Understanding the Decline and Demise of Terrorist Campaigns
by Audrey Kurth Cronin
Reviewed by Max Abrahms
Middle East Quarterly: http://www.meforum.org/2797/how-terrorism-ends

A battle is raging in terrorism studies. Proponents of the «strategic model» claim. That rational people participate in terrorist groups mainly for the political return. Proponents of the «natural systems model» claim that rational people participate in terrorist groups mainly for some form of social gain. The first model argues that terrorists attack civilians for the collective benefit of coercing political concessions, whereas the natural systems model claims that individuals engage in terrorism for the personal, selective benefit of participating in an exciting, tight-knit, social group. Although this debate is spearheaded by academics, it is hardly academic: The question of terrorist motives is fundamental to counterterrorism because one cannot expect to cure a malady without understanding its underlying cause.[1]

Cronin, professor of strategy at the U.S. National War College, does not explicitly align herself with either school of thought, but How Terrorism Ends suggests that social calculations are more determinative than political ones. Her analysis of how terrorism ends indicates that it is seldom due to rational, political considerations. Cronin finds, for example, that negotiating with terrorists «very rarely» works since most «terrorist groups choose not to negotiate at all.» This aversion to compromise results because «organizational survival overshadows the [stated] cause.» The logic is clear but sadly familiar: «If violence is part of the identity or livelihood of participants themselves, then the likelihood of negotiations resolving a conflict is miniscule.« The Oslo accords are illustrative: By embracing them, Palestinian terrorists of all persuasions would have unquestionably advanced their stated territorial aims. But groups such as Hamas and Palestinian Islamic Jihad instead ramped up their violence, helping to derail the peace process in order to ensure their organizational survival.

In fact, Cronin notes that what usually brings terrorists to the negotiating table are generally threats to the organization itself rather than to its putative political purpose. She finds that terrorist groups rarely abandon the armed struggle due to achieving their official political goals. This conclusion is expected given the fact that terrorist groups virtually never attain their given political aims, a point underscored in this reviewer's 2006 study in International Security, which compared the abysmal success rate of terrorist campaigns to other forms of protest.[2] Her case studies do, however, bolster the thesis that terrorism is inherently politically counterproductive by hardening governments and discouraging them from making concessions. She sensibly focuses on the handful of terrorist groups in modern history that achieved their policy demands such as the African National Congress and shows that they did so «despite the use of violence against innocent civilians [rather] than because of it.» The au-



thor is quick to point out that this does not mean terrorism accomplishes nothing at all; as previous studies have shown, terrorist acts can undercut the organization’s professed political agenda while simultaneously boosting membership, morale, and cohesion.[3]

So how then does terrorism end? By provoking government repression, its perpetrators have occasionally been stamped out. In fact, Cronin observes that «it is difficult to find cases» where governments did not use repressive measures, digging in their political heels. This does not mean that she endorses a policy of outright repression, however, since this response risks backfiring by turning the local population against the government and ultimately invigorating the terrorist group. A more frequent way for terrorism to end is by alienating potential supporters. She provides numerous examples of terrorist groups that «imploded» due to their lack of appeal to fresh recruits, infighting between organization members, and especially, backlash against the gory violence itself, which she believes is «the most common» way for these organizations to go out of the terrorism business. One example occurred in August 1998 when the Real Irish Republican Army splinter-group spurred a local backlash against it by killing twenty-nine noncombatants in Omagh, Northern Ireland. Similarly, the November 2005 Islamist terror attacks in Amman, Jordan, killed sixty innocent people but dramatically eroded local support for al-Qaeda and its affiliates throughout the country. Finally, Cronin finds that terrorist groups sometimes abandon the armed struggle but remain intact for patently apolitical reasons. A typical reorienting pathway is the transition to purely criminal behavior exemplified in the Abu Sayyaf Group, a Philippines-based al-Qaeda affiliate.

Cronin has written an important book on how terrorism ends. Her analysis is equally illuminating for its insights into why people engage in terrorism in the first place. The evidence is growing that these two areas of study may actually lead to the same conclusions. If so, serious implications for counterterrorism policy should flow from the recognition that social factors tend to trump political ones in the making and unmaking of terrorists.

Max Abrahms is a postdoctoral fellow in the Dickey Center for International Understanding at Dartmouth College, a postdoctoral fellow on the Empirical Studies of Conflict project sponsored by Princeton University, and lectures on terrorism at Johns Hopkins University.

[1] On the debate in terrorism studies between the strategic model and the natural systems model, see Max Abrahms, «What Terrorists Really Want: Terrorist Motives and Counterterrorism Strategy,» International Security, Spring 2008, pp. 78-105.

[2] Max Abrahms, «Why Terrorism Does Not Work,» International Security, Fall 2006, pp. 42-78.

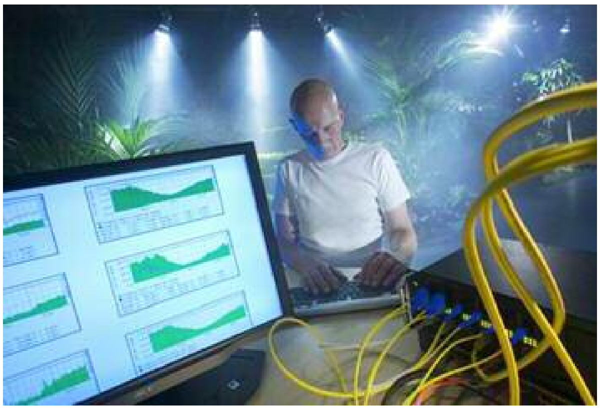
[3] Mia Bloom, Dying to Kill: The Allure of Suicide Terrorism (New York: Columbia, 2005); Marc Sageman, Understanding Terror Networks (Philadelphia: University of Pennsylvania Press, 2004).

CSARN
CITY SECURITY AND RESILIENCE NETWORKS
www.csarn.org
...protecting your business,
preparing your people...

Inside Nuclear Bunker of Wikileaks in Stockholm

Source:http://society.ezinemark.com/inside-nuclear-bunker-of-wikileaks-in-stockholm-77367f8e6beb. html#ixzz180zdvMil

Confidential files of the website WikiLeaks have been stored into a nuclear bunker in Stockholm, Sweden early this week. In particular, WikiLeaks servers are moved to the "Pionen" White Mountains data center, 30 meters below the ground after being dumped by Amazon. According to the Norwegian news site VG Nett, the "Pionen" White Mountains data center is owned by Bahnhof - a Swedish broadband provider. This is the home to WikiLeaks\' sever and confidential national data called «James Bond» styled bunker, or Cold-War-era nuclear bunker. Let\'s take a tour around the nuclear bunker of WikiLeaks in the "Pionen" White Mountains data center in Stockholm, Sweden.



There are two WikiLeaks' servers at least hosted by Bahnhof, a Swedish broadband provider under the granite-housed World-War-II era bunker

WikiLeaks moved into Bahnhof's "Pionen" White Mountains data center for the fist time in August 2010 utilizing servers owned by the Swedish Pirate Party. However, WikiLeaks has currently had a direct contract with Bahnhof in order to have servers hosted

At present, WikiLeaks' web servers are hosted by Bahnhof in a nuclear bunker in Stockholm, Sweden. It may soon move to Germany

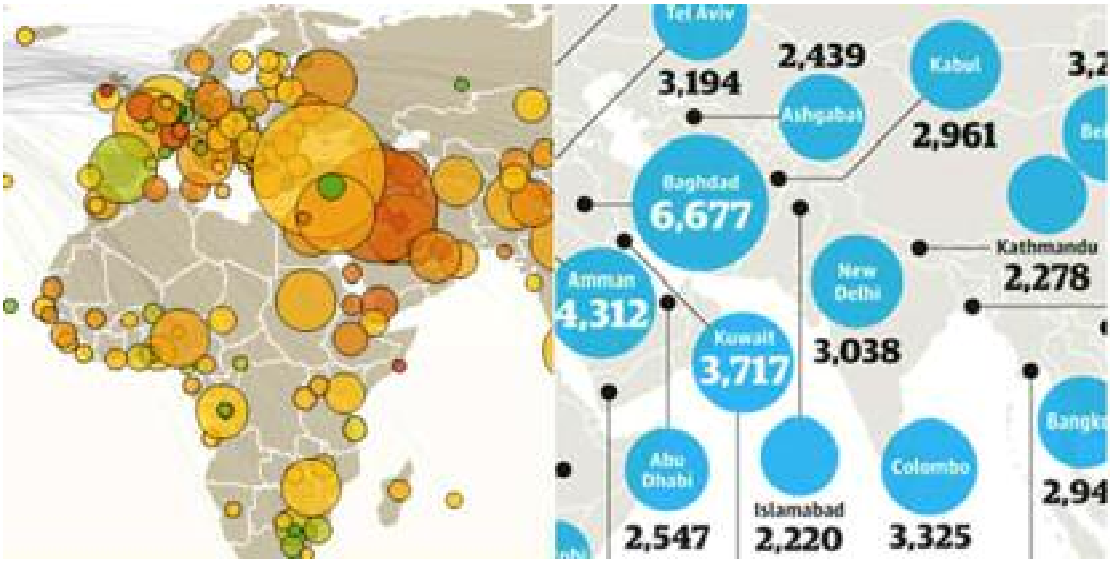
Bahnhof is the oldest and largest internet provider in Sweden providing the first commercial internet connections in 1994

The nuclear bunker in Bahnhof's "Pionen" White Mountains data center featuring with the «floating» conference room and backup generators remind the scenes from «James Bond» film

The Cold-War-era nuclear bunker is equipped with half-meter thick metal doors, backup generators and some powerful military forces with a view to protecting from danger

The move of Wikileads to Bahnhof's "Pionen" White Mountains data center in Stockholm, Sweden is the result of debate last month of the launch of thousands of confidential documents about the Afghanistan war

About 15,000 secret documents related to the Afghanistan war will be released soon



Stockholm suicide-bombing

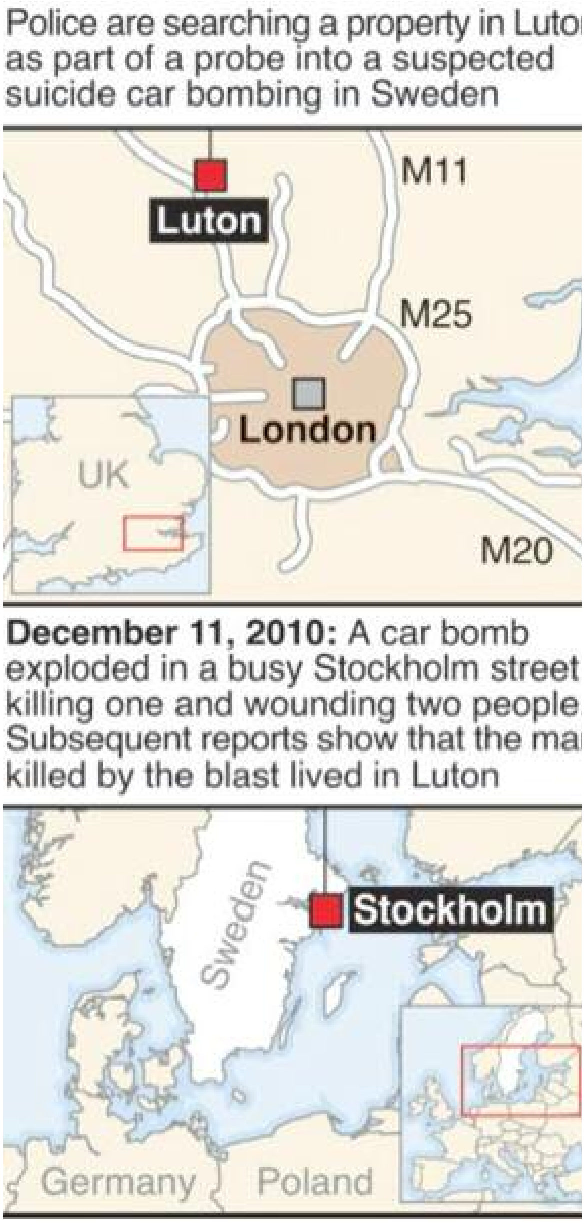
Source: http://www.dailymail.co.uk/news/article-1337930/Sweden-bomb-probe-Stockholm-blast-suicide-bomber-radicalised-Luton.html#

The wife of suicide bomber who was radicalised in Britain before carrying out a suicide bombing on a busy street in Sweden today spoke of her 'devastation'. Iraqi-born Taimour Abdulwahab Al-Abdaly, 28, blew up his car, then himself, in the capital Stockholm. And today it emerged he was thrown out of a Luton mosque three years ago for being too radical. A Swedish prosecutor said it was likely that Abdulwahab was wearing a bomb belt and was possibly on his way to a department store or train station when the explosive detonated by accident. Abdulwahab spent much of the last decade in Luton – long known as a hotbed of terrorism – where he studied for a degree and continued living there with his wife Mona Thwany and three young children.

Terror: A firefighter with a foam hose battles with the car after it was set ablaze by the bomber

Mrs Thwany - who runs her own beauty business Amira Make-up and Hair - said she had no clue about her husband's intentions. Asked if she had been aware of the plot she told Swedish newspaper Expressen: 'No, of course not. I really don't want to talk right now. I am very devastated and upset.' Sources at the Luton Islamic Centre today said Abdulwahab's views were deemed so extreme that he was asked to leave after he began giving sermons three years ago. It is claimed after being kicked out of the mosque he began preaching to the Islamic Society at the University of Bedfordshire. Qadeer Baksh, chairman of the Luton Islamic Centre, said he tried to reason with al-Abdaly but to no avail. 'It was the general public, worshippers, that brought it to the committee's attention that there was someone in here teaching something that is alien to Islam - extremist views,' he said. 'So I went and I faced him. I challenged his thoughts and his ideas and we got into a theological debate.

'I felt he was playing a game with me, just so he gets access to these worshippers. So, basically, I confronted him in front of the whole community and I brought up every single one of the doubts that he had been spreading and that he was debating with me.' Police were searching a property in the town today as part of the probe into the suicide attack. The Bedfordshire town has a Muslim population of 20,000 and has been linked with a string of high-profile extremists. Last year Muslim protesters disrupted a homecoming march of soldiers returning from Afghanistan. It has also emerged Abdulwahab - who had lived in the UK for 10 years - visited radical Islamic websites and Facebook groups including one which offers advice on preparing for Judgement Day. Another website he visited - Yawm Al-Qiyaamah - shows pictures of Tower Bridge engulfed by flames and has more than 8,000 followers. His Facebook page features an Islamic flag being raised over a world in flames. On the page, he says he is a member of the group Islamic Caliphate State, which seeks to establish Islamic rule worldwide and adds: 'I'm a Muslim and I'm proud.' Police



Police are searching a property in Luto as part of a probe into a suspected suicide car bombing in Sweden

December 11, 2010: A car bomb exploded in a busy Stockholm street killing one and wounding two people Subsequent reports show that the ma killed by the blast lived in Luton

were investigating Abdulwahab's British connections last night. Neighbours in Luton suggested that his wife, who herself has fundamentalist views, and their children are still living there. Metropolitan Police officers started examining a house last night, after a warrant was issued under the Terrorism Act 2000. A terraced property in the Bedfordshire town was cordoned off today, with officers seen going in and out.

Neighbour Noreen Hussain, 30, said the person who lived at the house at the centre of police activity was a family man. Although she did not know him by name, she said: 'We just said hello every so often. He had two girls and one boy, and the boy was born this year. 'He loved his kids so much. He used to play with them all the time in the garden on the trampoline.' The involvement of a student from a British university in yet another terrorist incident will raise fresh questions about admissions to UK universities, and the radicalisation of Muslim students when studying in this country.

An apocalyptic image from Abdulwahab's Facebook page which calls for an Islamic state

Police guard: An officer stands outside suspected bomber Taimour Abdulwahab Al-Abdaly's house in Luton

It is less than a year ago that a worldwide alert was sparked when former University College London student Umar Farouk Abdulmutallab, a Nigerian, was arrested on suspicion of trying to blow up an aeroplane with explosives hidden in his underpants. The latest bomber moved to Sweden with his family from Iraq when he was 11. He came to Britain in 2001 to study sports therapy at the University of Luton, now the University of Bedfordshire. He moved back to Sweden more recently and is believed to have separated from his wife, but they have not divorced.

British education: He is believed to have lived in Luton for a number of years after attending university in the UK

Aftermath: The body of a suicide bomber - thought to be Taimour Abdulwahab Al-Abdaly - lies in a Stockholm city centre street covered with a blanket following two blasts yesterday afternoon

Terror came to usually peaceful Stockholm on Saturday afternoon, minutes after Abdulwahab – who was due to celebrate his 29th birthday today – sent a warning of an impending attack to a Swedish news agency and police.

The mosque in Luton, where the suspect preached, threw him out three years ago for being too radical The warning referred to the presence of 500 Swedish troops among the Allies in Afghanistan and caricatures of the Prophet Mohammed drawn three years ago by Swedish cartoonist Lars Vilks. The warning email contained messages to the bomber's family, one asking that his children were told 'Daddy loves them' Immediately after the email arrived, Abdulwahab's car burst into flames on a busy street in the city centre, with a series of explosions following from gas canisters stashed inside the vehicle. Around ten minutes later Abdulwahab shouted in Arabic before detonating a pipe bomb which killed him and wounded two passers-by. Tragedy was only narrowly avoided, as police are understood to have found five more bombs on Abdulwahab's corpse which did not go off. He also wore a rucksack full of nails. It was speculated that the car bomb was designed to attract police and crowds, who would have been killed in their scores if all the suicide bombs had gone off. At a taxi office opposite the Luton flat where Abdulwahab is understood to have lived with his wife, employee Imran Khan, 31, said: 'We used to see him all the time. He lived across the road with his wife, a chubby lady who wore a full veil that covered everything apart from her eyes. 'He was really quiet and she wouldn't say anything. I haven't seen him here for a while but she's still around with their two little kids.'

Ablaze: A firefighter attempts to put out the fire following a car bomb explosion in Stockholm

Firemen pour in foam to douse the flames of the burning car in Stockholm

The woman believed to be Abdulwahab's wife two years ago signed an online petition calling for the wearing of the veil to remain legal worldwide. More than 250 people have joined a group set up on Facebook titled 'RIP Taimour Abdulwahab our brother and friend'.

THE BOMBER'S CHILLING LETTER

The following is the full text of an email sent to a Swedish news agency before the blasts:

'In the name of God the merciful. Prayers and peace to the Prophet Mohammad, peace be upon him.

'Thanks to Lars Vilks and his paintings of the Prophet Mohammad, peace be upon him, and your soldiers in Afghanistan and your silence on all this so shall your children, daughters, brothers and sisters die in the same way as our brothers and sisters and children die.

'Now the Islamic states have fulfilled what they promised you. We are here in Europe and in Sweden, we are a reality, not an invention, I will not say more about this.

'Our actions will speak for themselves, as long as you do not end your war against Islam and humiliation of the prophet and your stupid support for the pig Vilks.

'To all Muslims in Sweden I say: stop fawning and humiliating yourselves for a life of humiliation is far from Islam. Help your brothers and sisters and do not fear anything or anyone, only the God you worship.

'To my family, try to forgive me. I could not sit and watch while all the injustice happens against Islam and the Prophet Mohammad, peace be upon him, when the pig Vilks did what he did.

'Forgive me for my lies. I never went to the Middle East to work or earn money, I went there for jihad. I hope that you can understand me some time. I could never have told you all this or to anyone.'

Scotland Yard said: 'At 10.55pm last night, Metropolitan Police officers executed a search warrant under the Terrorism Act 2000 at an address in Bedfordshire. 'No arrests have been made and no hazardous materials found.'

Al-Abdaly listed himself on Muslim dating website Muslima as a physical therapy graduate from Bedfordshire University. He wrote on Muslima that he was born in Baghdad and moved to Sweden in 1992 before coming to the UK in 2001. He said he was married in 2004 and had two young girls. 'I want to get married again, and would like to have a big family. My wife agreed to this,' he wrote. He said he was looking for a practising Sunni Muslim who loves children and 'wants to please Allah before me'.

He described himself as economically 'OK' and said that when he had extra money he gave it to the needy. 'In the future, am looking

The suspected suicide car bomber lies under a blanket while a police forensic officer removes debris from around the body

Hunting for clues: A police forensics officer takes a mobile phone picture of what appears to be an identity card at the scene of the bomber's body

for to move to an Arabic country and settle down there...' al-Abdaly added. An audio file sent to Swedish news agency TT shortly before the blast referred to jihad, saying: 'Now the Islamic state has been created. We now exist here in Europe and in Sweden. We are a reality. I don't want to say more about this. Our actions will speak for themselves.' Sweden has a military presence in Afghanistan and a Swedish cartoon that depicted the Prophet Mohammed as a dog enraged the Muslim world. The country had never experienced a suicide bombing and has not had a terrorist attack since the 1970s. Prime minister Fredrik Reinfeldt said the attack was 'unacceptable'. He said: 'Sweden is an open society... which has stated a wish that people should be able to have different backgrounds, believe in different gods... and live side by side in our open society.'

LUTON: A MARKET TOWN AND FOCAL POINT FOR RACIAL TENSIONS

Luton, with its large Muslim population, has been the scene of several clashes involving Islamic activists. The market town is home to an estimated 20,000 Muslims and has become something of a focal point for protests against the wars in Iraq and Afghanistan. In March last year, a vocal Muslim anti-war protest during a homecoming parade by British soldiers received widespread condemnation. Protest: Muslim anti-war protesters at a regimental homecoming in Luton Two people were arrested amid angry scenes as the 2nd Battalion, The Royal Anglian Regiment marched to mark their return from Iraq. A group of Muslim protesters, who were hemmed in by police as the parade went past, waved placards with slogans including: 'Anglian Soldiers: Butchers of Basra' and 'Anglian Soldiers: cowards, killers, extremists'. One also read: 'British Government Terrorist Government.' Scuffles broke out two months later during another march through the town, this time directed against the Muslims who organised the March protest. Around 500 demonstrators waved banners bearing slogans such as 'No Sharia Law in the UK' and 'Respect our Troops'.The march was organised by a group called United People of Luton (UPL), and it featured people wearing balaclavas and shirts bearing the cross of St George. In 2005 the town was in the spotlight after it emerged that the July 7 suicide bombers Mohammed Sidique Khan, 30, Shehzad Tanweer, 22, Hasib Hussain, 18, and Jermaine Lindsay, 19, had met at Luton station before travelling to King's Cross in London to carry out their deadly attacks. This weekend it emerged that a controversial US pastor was planning to enter Britain and speak at an English Defence League rally in Luton. Terry Jones sparked condemnation around the world when he threatened to burn the Koran on the anniversary of the 9/11 terror attacks. He intends to preach 'against the evils and destructiveness of Islam' at the rally on February 5. Home Secretary Theresa May said yesterday she was 'actively' considering whether to ban him from entering the country.

WAR IN IRAQ
ANGLIAN SOLDIERS: BUTCHERS OF BASRA
INNOCENT MUSLIMS HELD CAPTIV
CRUSA AGAIN
© PA

per Concordiam

Journal of European Security and Defense Issues

- **SUICIDE BOMBERS**
  What motivates the "martyrs?"
- **NARCO-FINANCING**
  Terror's links to drug trafficking
- **CONDEMNING TERROR**
  European Islam's moderate voices
- **AFGHAN RECONSTRUCTION**
  International effort pays off

PLUS
European economic reform
Stopping passport forgery
Updating Central Asia strategy

How Terrorists Exploit New Information Technologies

Europe Learns No Nation is Immune to Terror

Source: http://www.time.com/time/world/article/0,8599,2040150,00.html

The Dec. 29 arrest of five men suspected of plotting a deadly shooting siege in Denmark - just nine days after a dozen men were seized in Britain on suspicions they were preparing a bombing strike - offers further evidence that the high levels of alert across Europe are well-founded. But the flurry of recent news produced by European terror action also shows that, with the notable exception of the lone extremist who blew himself up in Stockholm on Dec. 11 in an apparently botched bombing, authorities seem to be catching more al-Qaeda-inspired plotters before they manage to attack. So what's behind that apparent success? Are security authorities getting better at picking off increasingly autonomous groups of disparate jihadists as they quietly ready for strikes? Or is it just that the public is hearing more about what's actually routine preventive activity?

The answer, officials say, is a little of both - with an assist from heightened alert levels that make security forces more inclined to move on suspects they've have under surveillance for a while. «The threat of attack is always higher during the holiday season, so services tend to move faster against groups they've already got under watch if it appears action might be on the way,» says a French counter-terrorism official. «It's not a question of getting trigger happy, but rather gauging what you're hearing and seeing of radicals under observation [compared] to the generally higher risk you're facing. Sometimes there's more smoke than fire, other times you stamp out embers being fanned, and sometimes you stop what would have been a big blaze.»

Though information on the Danish plot is limited, reports suggest the police halted what could have been a serious and imminent attack. Authorities say four of the suspects were picked up Wednesday in a suburb of Copenhagen after they'd been followed driving down from Sweden, where the fifth man was arrested. According to Jakob Scharf, head of Denmark's Security and Intelligence Service, the group was allegedly planning to attack the offices of Jyllands-Posten, the newspaper that sparked anger across the Muslim world in 2005 by printing caricatures of the Prophet Mohammed. Scharf said the men were hoping to carry out a «Mumbai-style» shooting spree and «clearly intended to kill as many people as possible». The suspects of diverse ages and nationalities are scheduled to face a hearing Thursday on preliminary charges of possession of illegal weapons and intent to commit terrorism.

The bust in Denmark is only the most recent in a series of anti-terrorism operations carried out across Europe in the past two months. On Nov. 23, coordinated sweeps in Belgium, the Netherlands, and Germany nabbed 11 people who were variously charged with plotting a strike in Belgium and recruiting members for international jihadist activity. In the Netherlands, meanwhile, one man remains in custody on suspicion of what authorities described as plans to stage an «imminent attack» - on Christmas Eve, 12 Somali suspects were arrested in connection with the plot; 11 have since been released or held for deportation. And on Dec. 27, nine of the 12 people apprehended in Wales, central England and London were formally charged with preparing bombing attacks of possible targets that included Big Ben, the London Stock Exchange, and the U.S. Embassy.

As was the case in nearly a dozen preventive sweeps across Europe in the past six weeks, the British action appeared to have begun with the identification of a diffuse group of individuals who didn't display the usual outward signs of increasing extremism, such as recent travel to al-Qaeda's have in Pakistan's tribal region, religious trips to Yemen, or contact with known radical groups or mosques. «A lot of the 'clients' we're seeing now are people who became radicalized, networked, and researched strategies and techniques of terror attack through the Internet,» the French counter-terrorism official says. «The recent series of arrests of otherwise obscure and anonymous Islamists has been a result of improved surveillance of the Internet, and improving communication and sharing between European security forces.»

In large party, that's a response to the realization that all Europe faces the same growing threat - even countries that, not long ago, didn't imagine themselves targets. Though virtually all European countries engage in activity that makes them an enemy of jihadists - whether participating in the war in Afghanistan, or making life hard on extremists at home - some believed they were less at risk of being attacked. «Their culture and self-perception of tolerance and harmony long left some northern European nations feeling less exposed than others,» says the security official. Several recently disrupted plots in Denmark and Norway, the Dec. 11 bombing in Sweden, and Wednesday's arrests in Copenhagen have helped change that perception. And faced with that new reality, nations who once got comfort from the idea that they were among the few immune to terror attacks are now learning there's safety in numbers. «Over time they've seen the threat is just as great in their backyard as anywhere else,» says the terror expert. «Which has made these countries become much more vigilant, and better partners in fighting terrorism.»

Athens blast damages cars, courthouse; no injuries

A powerful explosion wrecked several cars in central Athens and damaged a courthouse and nearby buildings on Thursday, but no one was hurt, police said. Police evacuated the area after a warning call to a local TV station before the attack, which damaged the facade of the court building, shattered windows and blew up at least eight cars. The blast was the most powerful in Greece in at least a year. «An anonymous call to a TV station warned that an explosive device on a parked motorcycle outside the court house would go off in about 40 minutes,» said a police official who did not want to be named. Authorities believe a makeshift explosive device was placed on a motorbike parked outside the Athens courthouse. Flames followed the explosion, buildings shook and thick smoke covered the area. «It was a huge blast. I was in the kitchen with my grandchild and the whole building shook. We saw smoke and flames,» an elderly woman who lives about 50 meters from the courthouse told Flash radio. There was no immediate claim of responsibility. Police suspect one of Greece's extreme leftist or anarchist groups which have stepped up attacks in the last two years. «We condemn the action, there is no point in trying to change the world by risking the death of innocent people,» Deputy Transport Minister Spyros Vougias told Skai TV. Greece has a decades-old history of leftist violence. Some groups became more active after riots in December 2008, triggered by the police killing of a teenager. They usually target government buildings, police stations and banks, mostly at night, and make warning calls. On January 17, 13 suspected members of the anti-capitalist Conspiracy Fire Cells urban guerrilla group go on trial. The group claimed responsibility for mailing parcel bombs to embassies in Athens and foreign governments abroad in November. The police official said the fact that the caller gave a 40 minute warning along with the motorcycle's plate number indicated the perpetrators were not aiming to kill. Authorities cordoned off the area for fear shattered glass may hurt passersby. Television showed firemen on emergency ladders checking if building facades were intact. In September 2009, the strongest blast to date seriously damaged the Athens stock exchange. The Revolutionary Struggle group claimed responsibility.

www.ambu.com

Ambu

Ideas that work for life

Ambu® Military Mark III – RDIC

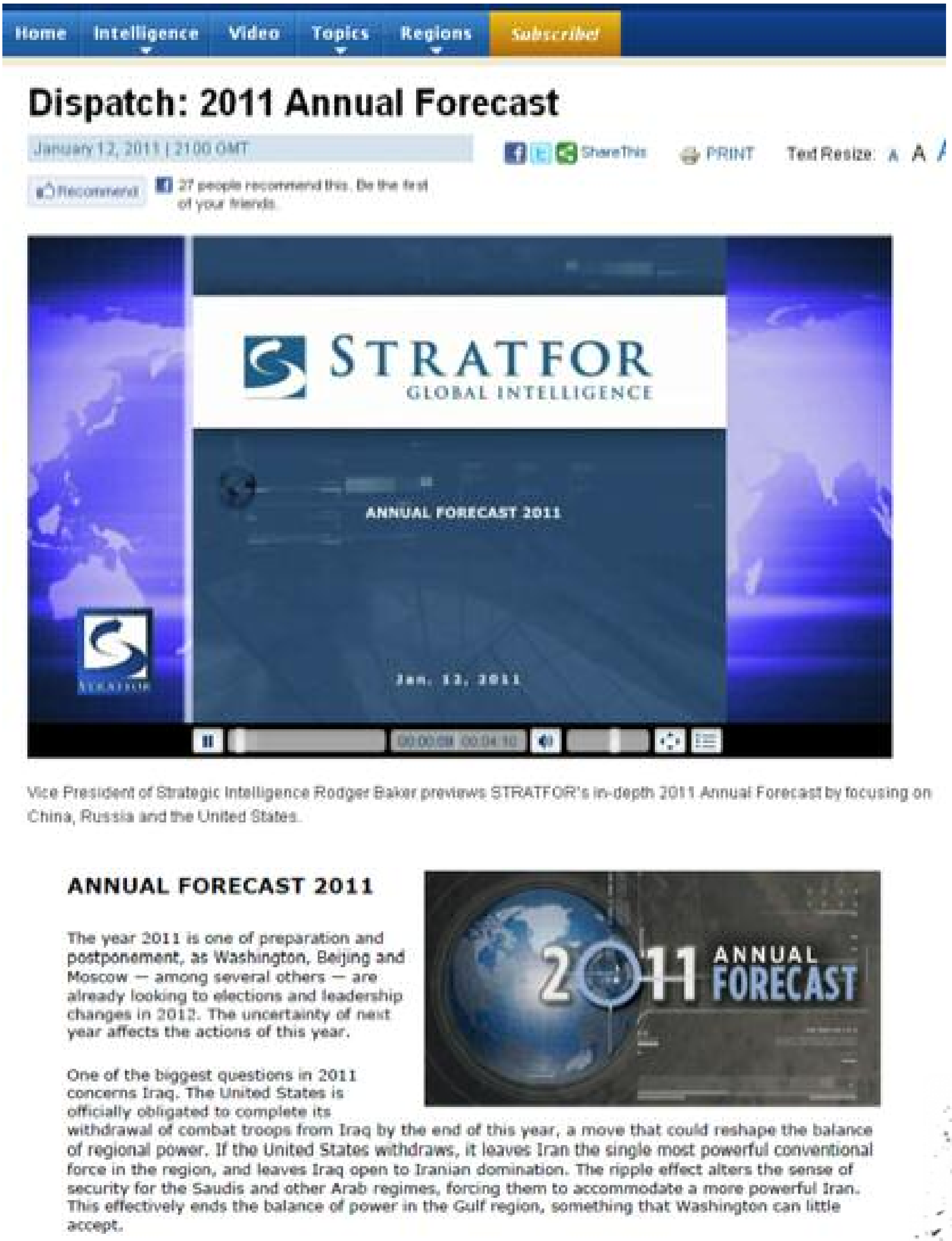
The original Ambu Bag with the unique double wall principle, designed for toxic atmospheres
The Ambu Mark III is a latex free reusable resuscitator designed for the manual ventilation of adults and children with a minimum body weight of approx. 15 kg. The Mark III has the added advantage of being constructed with an outer cover made from butyl and a gas filter, which is ideal for manual resuscitation in toxic atmospheres, e.g. fire and chemical accidents. The Ambu Mark III can be repeatedly autoclaved at 134°C (except the face mask). It comes with a built-in pressure limitation of approx. 70 cm H_2O for patient safety, face mask, cover, ext tube, carry case.

ORDERING INFORMATION	CAT.NO.
RDIC-Butyl Resuscitator, Size 5 Face Mask, Canister, Filter	233 005 000

Telephone 1-800-262-8462 Fax 1-800-262-8673

STRATFOR's 2011 Annual Forecast

Source: http://www.stratfor.com



Dispatch: 2011 Annual Forecast

January 12, 2011 | 2100 GMT

27 people recommend this. Be the first of your friends.

Vice President of Strategic Intelligence Rodger Baker previews STRATFOR's in-depth 2011 Annual Forecast by focusing on China, Russia and the United States.

ANNUAL FORECAST 2011

The year 2011 is one of preparation and postponement, as Washington, Beijing and Moscow — among several others — are already looking to elections and leadership changes in 2012. The uncertainty of next year affects the actions of this year.

One of the biggest questions in 2011 concerns Iraq. The United States is officially obligated to complete its withdrawal of combat troops from Iraq by the end of this year, a move that could reshape the balance of regional power. If the United States withdraws, it leaves Iran the single most powerful conventional force in the region, and leaves Iraq open to Iranian domination. The ripple effect alters the sense of security for the Saudis and other Arab regimes, forcing them to accommodate a more powerful Iran. This effectively ends the balance of power in the Gulf region, something that Washington can little accept.

European Master in Disaster Medicine

Source: http://www.dismedmaster.com/course/course-master-in-disaster-medicine.php

The EMDM is organised with voluntary support of the following Universities/Institutions:

- Centre for Teaching & Research in Disaster Medicine and Traumatology, Linköping, Sweden
- University of California at Irvine, Center for Disaster Medical Sciences, USA
- University of Geneva, Faculty of Medicine and University Hospital of Geneva, Switzerland
- Swiss Academy for Military and Disaster Medicine, Bern, Switzerland
- Cincinnati Children's, Hospital Medical Center, Cincinnati, USA

On June 6, 2009 a convention was signed between the Master Diploma Delivering Universities and any single listed University/Institution aimed at:

- Composing specific parts of the course core content following the guidelines proposed by the Scientific Committee
- Interacting with students on the E-Learning platform
- Preparing interactive sessions to be proposed during the residential course
- Presenting exercises and debates during the residential course
- Thesis tutoring

The EMDM is supported by international and scientific organizations with interest in disaster medicine and disaster management:

- the European Society for Emergency Medicine (EuSEM)
- the World Health Organization (WHO)
- the International Committee of the Red Cross (ICRC)

The faculty members of the EMDM are qualified professionals in disaster medicine and disaster management coming from European and extra-European countries, affiliated with academic and worldwide renowned institutions.

Course initiators:

• Prof. Michel Debacker (Free University Brussels, Belgium) • Prof. Francesco Della Corte (University "A. Avogadro" Eastern Piedmont, Novara - Italy) • Prof. Herman Delooz (Free University Brussels, Belgium)

The EMDM is a level - two Master, a 60 credit unit programme, and lasts one academic year.

The Master will be based on:

- a self-directed study based on an Internet-based e-learning platform
- a two weeks live-in course
- the writing and defence of a dissertation or a research project paper (thesis)
- a final on line examination

First National Emergency Alert System (EAS) Test Ordered

by Rick Wimberly

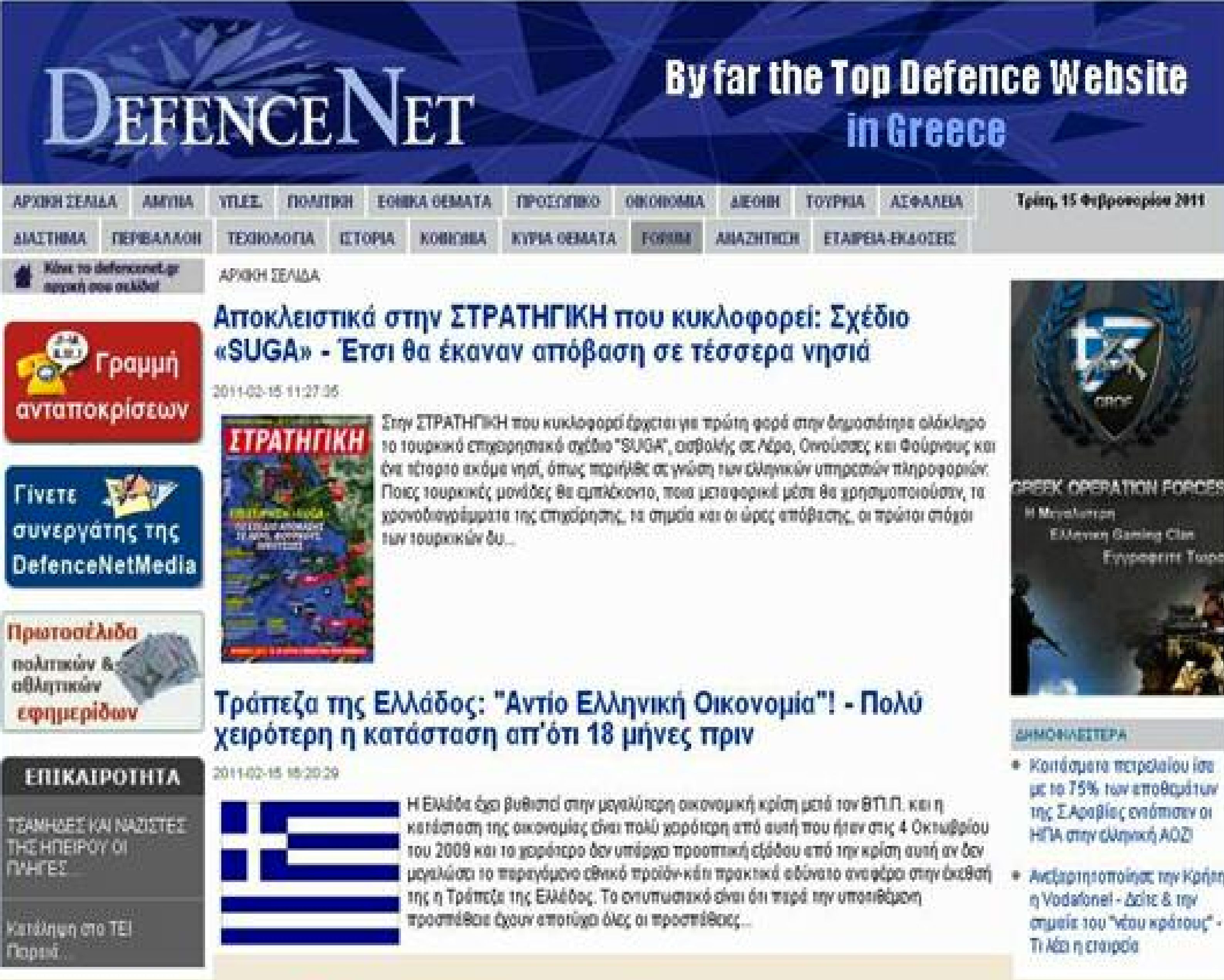
Source:http://www.emergencymgmt.com/emergency-blogs/alerts/First-National-Emergency-Alert-020411.html

The Federal Communications Commission (FCC) has made it official. It has released an order that requires participants in the Emergency Alert System (EAS), namely broadcasters, cable operators, and certain satellite providers, to participate in the first-ever national test of EAS. The test will differ starkly from the monthly EAS tests the public knows so well. In this case, the White House will actually activate the test as if the President wanted to take over the air waves to address the nation. Although EAS-type capabilities have existed since the early 50's, no President has ever used it. Now, we're going to find out how well it actually works.

The FCC order lays out how the test will be conducted. It will use what many emergency managers know as the EAN code. That's «Emergency Alert Notification», the code reserved for the President to activate EAS. The EAN code kicks in the process where video and audio content will be interrupted by EAS participants monitoring the Primary Entry Point (PEP) stations that receive the message the White House originates. Stations, cable outlets and some satellite programming providers are to interrupt their content to allow the White House to take over the air waves.

No specific date for the test was set, although as it stands, a two-month notice will be provided. The FCC gave its staff ability to extend the notice period if necessary, and to work with stakeholders to determine the right time of the day for the test. In a live web broadcast on EAS recently, senior FCC and FEMA officials indicated the test would be conducted in the latter part of 2011. (EAS is part of FEMA's Integrated Public Alert and Warning System - IPAWS.) It's an open question about the length of the test message. Recognizing the national test with a message from the White House could cause a stir among the public, the FCC said outreach will be a «major aspect of preparation» and directed its staff to work with federal partners and other stakeholders to «disseminate notice of the test as widely as possible through as many outlets as possible».

Some EAS equipment manufacturers had argued that it would be a good idea for emergency managers to receive training on EAS activation prior to the national test. The FCC said it agreed that message originators need training on properly using EAS codes, but that it has «no jurisdiction over those entities». The FCC said it «will continue to work with FEMA to establish proper guidelines for message originators». Even though emergency management training won't be necessary to activate the national code, we believe it's very important that emergency management and other public safety officials are deeply engaged and well-informed on the national test. In addition to testing a vital tool that they (and the President) can use, the national EAS test will require significant public outreach as the FCC noted. Otherwise, the public could over-react and overload 9-1-1 systems. Emergency management and other public safety officials can help make sure the local public knows what's going on. And, again, we put in a plug for emergency managers to use the national test as a reason to sit down with local broadcasters and cable operators. You can be assured they'll be paying attention, and will be encouraged to participate in outreach. It would be nice for local outreach to be a joint public safety-broadcast/cable effort. So, the national EAS test is officially coming. Stay tuned!



DEFENCENET

By far the Top Defence Website in Greece

ΑΡΧΙΚΗ ΣΕΛΙΔΑ | ΑΜΥΝΑ | ΥΠ.ΕΣ. | ΠΟΛΙΤΙΚΗ | ΕΘΝΙΚΑ ΘΕΜΑΤΑ | ΠΡΟΣΩΠΙΚΟ | ΟΙΚΟΝΟΜΙΑ | ΔΙΕΘΝΗ | ΤΟΥΡΚΙΑ | ΑΣΦΑΛΕΙΑ

ΔΙΑΣΤΗΜΑ | ΠΕΡΙΒΑΛΛΟΝ | ΤΕΧΝΟΛΟΓΙΑ | ΙΣΤΟΡΙΑ | ΚΟΙΝΩΝΙΑ | ΚΥΡΙΑ ΘΕΜΑΤΑ | FORUM | ΑΝΑΖΗΤΗΣΗ | ΕΤΑΙΡΕΙΑ-ΕΚΔΟΣΕΙΣ

Τρίτη, 15 Φεβρουαρίου 2011

Κάνε το defencenet.gr αρχική σου σελίδα!

Γραμμή ανταποκρίσεων

Γίνετε συνεργάτης της DefenceNetMedia

Πρωτοσέλιδα πολιτικών & αθλητικών εφημερίδων

ΕΠΙΚΑΙΡΟΤΗΤΑ

ΤΣΑΜΗΔΕΣ ΚΑΙ ΝΑΖΙΣΤΕΣ ΤΗΣ ΗΠΕΙΡΟΥ ΟΙ ΠΛΗΓΕΣ...

Κατάληψη στο ΤΕΙ Πειραιά...

ΑΡΧΙΚΗ ΣΕΛΙΔΑ

Αποκλειστικά στην ΣΤΡΑΤΗΓΙΚΗ που κυκλοφορεί: Σχέδιο «SUGA» - Έτσι θα έκαναν απόβαση σε τέσσερα νησιά

2011-02-15 11:27:35

Στην ΣΤΡΑΤΗΓΙΚΗ που κυκλοφορεί έρχεται για πρώτη φορά στην δημοσιότητα ολόκληρο το τουρκικό επιχειρησιακό σχέδιο "SUGA", εισβολής σε Λέρο, Οινούσσες και Φούρνους και ένα τέταρτο ακόμα νησί, όπως περιήλθε σε γνώση των ελληνικών υπηρεσιών πληροφοριών. Ποιες τουρκικές μονάδες θα εμπλέκονταν, ποια μεταφορικά μέσα θα χρησιμοποιούσαν, τα χρονοδιαγράμματα της επιχείρησης, τα σημεία και οι ώρες απόβασης, οι πρώτοι στόχοι των τουρκικών δυ...

Τράπεζα της Ελλάδος: "Αντίο Ελληνική Οικονομία"! - Πολύ χειρότερη η κατάσταση απ'ότι 18 μήνες πριν

2011-02-15 16:20:29

Η Ελλάδα έχει βυθιστεί στην μεγαλύτερη οικονομική κρίση μετά τον Β'Π.Π. και η κατάσταση της οικονομίας είναι πολύ χειρότερη από αυτή που ήταν στις 4 Οκτωβρίου του 2009 και το χειρότερο δεν υπάρχει προοπτική εξόδου από την κρίση αυτή αν δεν μεγαλώσει το παραγόμενο εθνικό προϊόν-κάτι πρακτικά αδύνατο αναφέρει στην έκθεσή της η Τράπεζα της Ελλάδος. Το εντυπωσιακό είναι ότι παρά την υποτιθέμενη προσπάθεια έχουν αποτύχει όλες οι προσπάθειες...

GREEK OPERATION FORCES

Η Μεγαλύτερη Ελληνική Gaming Clan

Εγγραφείτε Τώρα

ΔΗΜΟΦΙΛΕΣΤΕΡΑ

- Κοιτάσματα πετρελαίου ίσα με το 75% των αποθεμάτων της Σ.Αραβίας εντόπισαν οι ΗΠΑ στην ελληνική ΑΟΖ!
- Ανεξαρτητοποίησε την Κρήτη η Vodafone! - Δείτε & την σημαία του "νέου κράτους" - Τι λέει η εταιρεία

ΠΟΛΕΜΟΣ & ΙΣΤΟΡΙΑ
ΙΜΙΑ 1996
ΠΩΣ ΕΝΑΣ ΠΑΡΑΛΙΓΟ ΘΡΙΑΜΒΟΣ ΚΑΤΕΛΗΞΕ ΣΕ ΤΡΑΓΩΔΙΑ
ΣΤΡΑΤΗΓΙΚΗ
ΕΠΙΧΕΙΡΗΣΗ «SUGA»
ΤΟ ΣΧΕΔΙΟ ΑΠΟΒΑΣΗΣ ΣΕ ΛΕΡΟ, ΦΟΥΡΝΟΥΣ, ΟΙΝΟΥΣΣΕΣ
ΑΠΟΦΑΣΗ ΣΑΓΕ: ΤΑ 29 ΚΥΡΙΑ ΕΞΟΠΛΙΣΤΙΚΑ ΠΡΟΓΡΑΜΜΑΤΑ
ΑΜΥΝΤΙΚΗ ΒΙΒΛΟΣ
2010 - 2011
ΕΛΛΑΔΑ-ΤΟΥΡΚΙΑ-ΚΥΠΡΟΣ
Δυνάμεις & εξέλιξη Απειλής

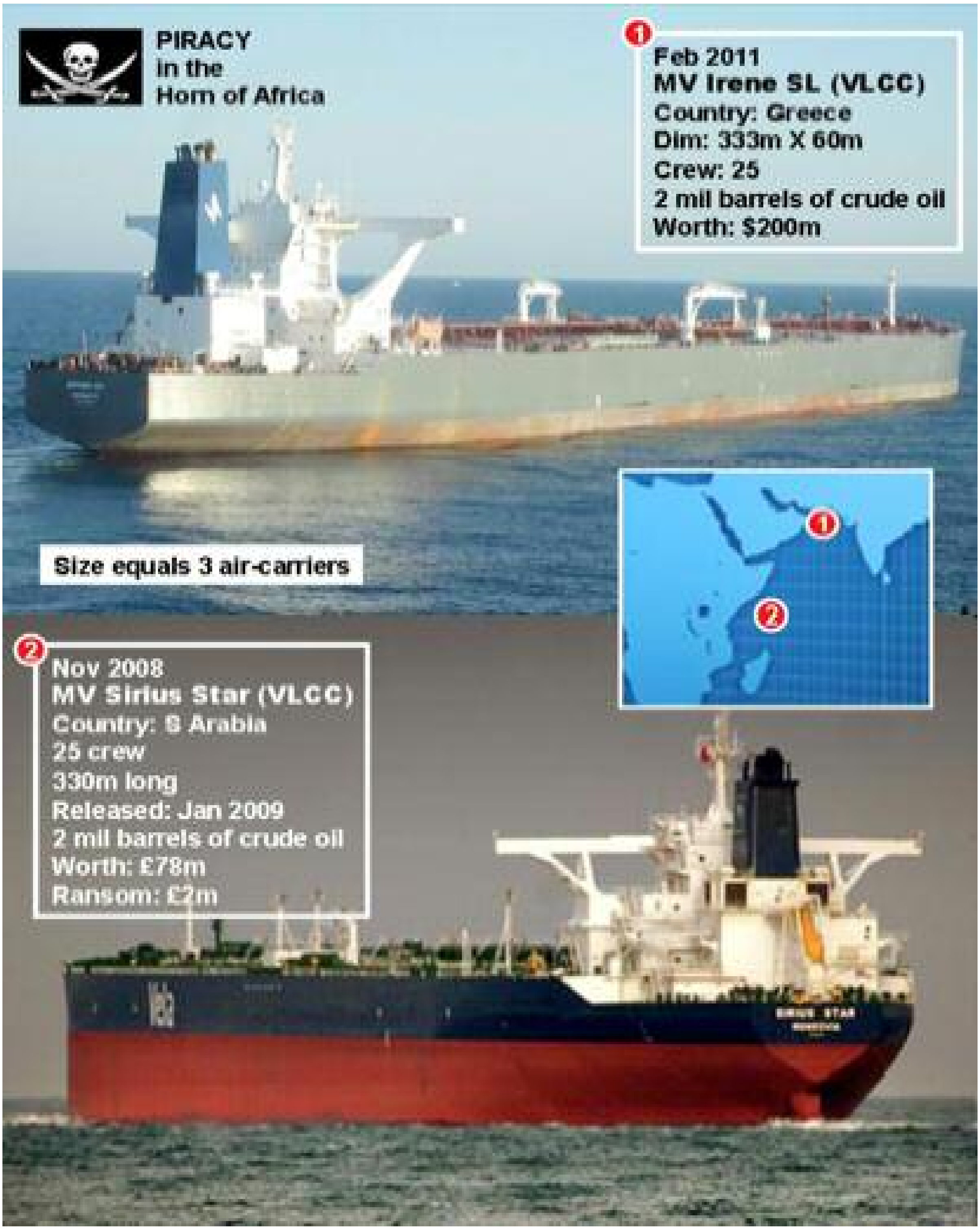
ΕΚΔΙΔΕΤΑΙ ΑΠΟ ΤΗΝ:

DEFENCE net media

www.defencenet.gr

Who will stop the pirates?

Source: The Editor



PIRACY
in the
Horn of Africa

1
Feb 2011
MV Irene SL (VLCC)
Country: Greece
Dim: 333m X 60m
Crew: 25
2 mil barrels of crude oil
Worth: $200m

Size equals 3 air-carriers

2
Nov 2008
MV Sirius Star (VLCC)
Country: S Arabia
25 crew
330m long
Released: Jan 2009
2 mil barrels of crude oil
Worth: £78m
Ransom: £2m

Interoperability Is a Cultural Problem (Opinion)

By Jim McKay

Source: http://www.emergencymgmt.com/safety/Interoperability-Cultural-Problem-Opinion.html

We've written extensively about interoperability, mostly about the nuts and bolts of a system being deployed and the grant process that allowed said deployment to happen. If there's collaboration among the agencies or jurisdictions involved, we jump all over it, because that's the name of the game these days. A common refrain years ago was that agency or jurisdiction A couldn't communicate with agency or jurisdiction B — or even within its own agency or jurisdiction. That was said to be an operability problem — not an interoperability problem. Billions of dollars have been spent on interoperability since 9/11 and genuine progress has been made, but it seems that emergency managers view interoperability as something still to be attained. For the most part, if agency A wants to talk to agency B, it can be achieved; the technology to facilitate this is available. And still interoperability is a problem. We heard so at a recent roundtable discussion involving several emergency managers. Everybody at the table agreed: It's a cultural problem. Agency A doesn't talk to agency B because the two aren't really familiar with each other — or maybe they just don't want to talk. "Everybody talks about the quantifiable parts of interoperability — the money, the hardware — but not enough about the behavior part of it," one emergency manager said. "How much effort is being put into the cultural aspect of it?" Even where there's a new, multimillion-dollar system, agency personnel revert to previous behavior. "Everything happens the way it did before, even after getting this new system," another emergency manager said. "The police guy calls the dispatcher and he calls the fire guy; they still talk in silos. Unless we address this behavior, we'll have a $100 million doorstop." There's also the issue of language. We know different jurisdictions and agencies use different codes to communicate. Coming up with a common language has to be the first part of the cultural change, said an emergency manager. And emergency managers can play key roles in this quest by hosting planning calls and conference calls — getting people to communicate regularly. "The best thing to do is have commanders sit next to each other in the operations centers." Another thing about interoperability that people stub their toes on is the notion that everyone must be able to talk to everyone, one participant said. "Everybody on the ground doesn't have to talk to each other. When you bring people from other jurisdictions, you can plug people into your system. That to me is true interoperability." I wonder if in 10 years we'll still be writing about interoperability as we do today — that it's something that's desired but still needs to be attained. Or will agencies and local governments move outside of their comfort zones and take advantage of the technology that's readily available — will they open the dialog with their neighbours, making interoperability yesterday's news?

CBRN preparedness vs. Simple Humanity

By the Editor

Source of photo: http://pressonice.blogspot.com

We spend tons of money, effort, sweat and brain power to support preparedness for our societies, our way of life and own existence. Others do the same solely with their own human resources!

Poor Indian woman breastfeeding her baby and an orphaned monkey-baby!

Original Papers

CBRN Security at London 2012

By **Andy Oppenheimer**

The London Olympics being held in July and August 2012 will require an unprecedented level of security and countermeasures against terrorist attacks. Preparations to protect the millions of visiting spectators, the Olympic Village inhabitants, officials and the travelling public during the world's most high-profile sporting event are geared towards an increasing range of possible threats.

All major sporting events and events attracting large numbers of people have been regarded as high-level terrorist targets with attendant increases in security measures and police presence. Among the panoply of threats being factored into readiness plans, a terrorist attack involving chemical, biological or radiological (CBR) improvised devices or non-explosive means of dispersal would cause longer lasting disruption than other types of attack because of contamination of people and infrastructure and subsequent spread of toxic material further afield. The threats exceed the actual Games period and the reach of the Olympic sites and venues in London, to cover the UK as a whole.

CBR threats include improvised chemical devices (ICDs), dispersal of chemical or biological agents, and radiological dispersal devices (RDDs), as well as the more prevalent means of mayhem – suicide bombers carrying explosives and vehicle-borne IEDs. While the risk of attack from conventional explosives, including novel homemade explosives, mortar attacks along with non-terrorist hazmat releases and accidents rank higher than CBR attacks, they are nevertheless regarded as substantial threats - especially as the Olympics provides resourceful terrorists with a high-profile world stage with maximum media coverage.

As threat levels change on a regular basis depending on intelligence on terrorist plots at home and abroad, it is hard to define exactly the threats facing the Olympics two years on from now, other than to assume that all of the above - with possible variations - are factored into security arrangements. And while specific attempts at a CBRN attack are low probability, the consequences of such an event are so severe that they are high on the contingency planning list of priorities for first response operations at several sites.

The shadow of previous disasters

The terrorist atrocities at the 1972 Munich Olympics, in which 11 Israeli athletes and one police officer were killed by Palestinian terrorists, formed for decades the main precedent to guide counterterrorist planning. In July 1996 in Atlanta, Georgia a pipe-bomb concealed in a rucksack was planted in the Centennial Olympic Park, which was in continuous use as a venue for live music acts. One person was killed and 100 injured.

The 7 July, 2005 bombings of the London transit system, in which 53 people died and over 700 injured in four simultaneous attacks, provided lessons for future events involving crowded situations. The worst terrorist attack on British territory (apart from the Lockerbie disaster), 7/7 occurred the day after the capital celebrated winning the 2012 bid and served most poignantly to emphasize the security challenges that lay ahead.

Incidents and plots result in enhanced readiness against possible targeting of sporting events and other crowded venues taking place simultaneously. The attempted car bomb attacks in London in June 2007 resulted in heightened security at the Wimbledon Tennis championships taking place at the time.

Non-terrorist events have provided lessons to be learned in how to manage crowd incidents, such as the April 1989 Hillsborough disaster, when 96 Liverpool Football Club supporters were suffocated to death at the Hillsborough soccer stadium. This tragic event resulted in new multimillion-pound safety measures: all-seater stadia throughout Britain and stricter controls on crowds entering the venues. But even with seated stadia, should a terrorist incident involving a toxic release take place, the stampede effect would still prove lethal.

Britain's biggest security operation

The London 2012 security operation is the largest ever in peacetime Britain. There is some dispute over how high security costs will eventually be, having been estimated to reach a staggering £1.5bn out of a projected total cost for hosting the Games of £7.52bn. In December 2010 the UK Minister for Security, Baroness Pauline Neville-Jones, told Parliament the cost to British taxpayers could be as low as £475 million, but indicated in the same speech that the final bill – factoring in a major security scare – could total £2 billion.

The Olympic Delivery Authority, the body in charge of all the infrastructure building and security, has along with civilian and military authorities planned and trained for likely scenarios, to examine how an incident would unfold. This included working through realistic casualty rates should an incident happen; how to deal with casualties; how first-responders are briefed and trained up for such events; how to manage response to a CBRNE event, including evacuation measures, decontamination of persons and locations, forensics and monitoring; the role of the media in covering an incident at such well publicised events; and how much the public should be told in advance of the event about countermeasures in place – and how they would be informed during the unfolding of an attack.

Finding a balance

Precise details on CBR surveillance at the Games are not available for the purposes of this article, but it is certain they will be based on fast detection and identification of released toxic materials. A prime challenge is achieving a balance between security concerns and ensuring spectators can enjoy a friendly and open atmosphere. Decisions on medical attendance and decontamination procedures must be made speedily to ensure casualties are treated and panic avoided. Spectators should, however, be unaware that detection equipment has been deployed so as to avoid unnecessary anxiety. Therefore, a CBRN security concept will work in the background, including perimeter watch and intruder detection. The aim is to enable visitors to enjoy the events without disturbance or alarm, in contrast to the rigid controls applied at the 2008 Beijing Olympics.

Nevertheless, an army presence will be essential: military helicopters as well as unmanned military planes used to monitor the Taliban in Afghanistan will patrol overhead and jets will be on standby to intercept any suspect private plane heading for the main Olympic stadium in Stratford, east London, where some 290,000 people are expected to be at peak times. The Army will be drafted in as civil support to assist in first response and help protect athletes and hundreds of thousands of spectators from an atrocity.

The Olympics will be a major test of information management systems for a terrorist incident, including data communications and contact with the public through the press office dealing with the media and first responders. A database of aerial photographs, maps and 3D views of all Olympic venues will incorporate technology which enables 3D images to be spun through 360 degrees - pinpointing exits, meeting points and fire hydrants, and allowing simulation of major incident scenarios. Cyberterrorism, regarded as a major threat to the Games, is being monitored and countered through advanced surveillance systems and vigilance, but this is just one wildcard in a pack of threats, many of which can not be predicted or quantified.

Internal security is paramount, as infiltration by terrorists is an ongoing threat, and involves extensive personnel screening of the many thousands of workers employed on and off site in the months leading up to, and on duty during, the Games. This will require vetting on a large scale of some 200,000 people working at venues, including 70,000 volunteers drafted in to check incoming spectators' bags and tickets, 40,000 construction workers, 30,000 security officers and 60,000 others. Biometric hand and eye scanners are in operation for onsite workers at the 2.5sq km Olympic Park, and photographic smart cards for up to 5,000 construction workers an hour at peak.

Transit security

The transport network will carry at least 240,000 passengers an hour during the Games on an already crowded Underground network. Improvements for transit communications, brought in following the London 2005 attacks, have been taken on board for readiness for the Olympics. Extra officers will be deployed on the Underground to identify suspected bombers. Problems getting enough equipment and medical supplies to several sites have been addressed by distribution of radio pagers to transit managers and the incident control room has been reconfigured to allow for multiple, simultaneous attacks - the sheer scale of which on 7/7 created confusion, stretched supplies, and put pressure on an outdated communications system. Communications protocols between police forces will enable the Police Casualty Bureau to handle more calls than were possible on 7/7.

As for CBRN attacks, lessons were learned prior to 7/7 - from the multiple sarin nerve agent attacks in Tokyo in March 1995 - the most lethal coordinated chemical attacks to occur in one day in a civilian context. As more 300 ambulance and police were injured by contact with the sarin that had been dispersed on five trains simultaneously, as well as contact with the victims, all first-responders are now equipped with personal protective equipment (PPE) and trained how to don PPE and to use rapid sampling detection systems carried by first responders.

Chemical surveillance: Learning from Germany 2006

Measures taken for enhanced security, detection and surveillance during the FIFA Soccer World Cup Finals in Germany in 2006 are regarded as an excellent milestone of organisation and anti-terrorist prevention, and as a Gold Standard for future events. Pre-emption was paramount - suspects were identified when crossing the border or even well before coming to Germany. NATO AWACS surveillance planes monitored German airspace for airborne attacks. Good communication was maintained between federal and state liaison officers, European police forces, armed forces and fire departments. The Bundeswehr was on standby for emergency situations with decontamination units.

All arenas were protected by a new multilayer concept, specifically for chemical surveillance, as a chemical attack is viewed as the highest risk within the CBRN pantheon. There was monitoring of stadia four hours prior to games, during the matches and two hours after. Reconnaissance teams, detection equipment, and surface samplers were in standby-position out of sight of the crowd, in communication with the command centre inside the stadium.

Had an emergency occurred, it is claimed that the teams would have been able to reach every position inside the stadium within minutes, with samples analysed and clearly identified within 10 to 15 minutes – as long a period as can be tolerated if the right decisions regarding decontamination procedures and medical treatment can be made. Firefighters in the command centre were able to check the located cloud position via binoculars and, of prime importance, observe the behaviour of the people inside or near a located cloud.

CW scanning installations, developed by the German blue-light services in collaboration with Bruker Daltonics, included stand-off detectors for CWA clouds (RAPID - Remote Air Pollution Infrared Detectors); hand-held ion mobility spectrometers (RAID - Rapid Alarm and Identification Devices); and mobile gas chromatograph/mass spectrometers. Together, these systems could identify any organic chemical from the soil, water, and air within 15 minutes via complementary sampling techniques and provided detailed information content as well as on-site support and scientific management. Training and operation were reduced to the lowest possible level, and detectors were installed in stand-by mode invisible to the audience, having been tested with simulation substances. There was just one alarm - for ammonia, at Leipzig Stadium. There was no impact on the crowd and it was confirmed by a visual check.

Protecting infrastructure

Barrier protection against car bombs and blast mitigation are prime measures for London 2012 to minimise the effect of bomb explosions. High-profile buildings and prime sites have been designed to incorporate blast-proof material and shatter-proof glass. Blast-resistant glazing absorbs blast energy, and the size of blast and distance of the building from the blast point are critical factors. Fixed detectors are increasingly deployed to protect infrastructure, particularly sentinel systems for chemical and biological detection. These are designed to bridge the gap between sensor data and actionable information, with automated action for evacuation and emergency response. Other countermeasures include blast mitigation tents and blastproof garbage cans which are all unobtrusive.

Decontamination

If an incident were to occur during the Games, decontamination would have to be carried out immediately to remove toxic substances from victims and to minimise the level of cross-contamination as crowds walk and drive away from the scene, touch other people and objects, and take contamination onto the transit system. This is what marks out CBR attacks from others.

Throughout England there are 73 Incident Response Units (IRUs), vehicles, each carrying two mass decontamination structures, along with 17 Detection, Identification and Monitoring (DIM) vehicles with equipment to detect and identify chemical and biological contaminants, gamma and beta radiation sources and radioactive isotopes. The IRUs carry two decontamination structures and ancillary equipment such as firefighter decontamination units which can decontaminate up to 200 people an hour. One would hope that such measures will not be necessary, but all preparations, whatever the eventual cost, will taken on board every possible risk in order to protect everyone taking part and attending the 2012 Olympic Games.

Expect the unexpected

While CBRN defence planning involves multiple and varied scenarios for training, the motto “expect the unexpected” is most appropriate. This was clearly epitomized by the totally unexpected nature of the radiological dispersal incident precipitated by the fatal poisoning of a Russian dissident, Alexander Litvinenko, in London in November 2006. The radioisotope which killed him, polonium-210, was not only relatively rare but its effects not clearly quantified. Only a minuscule amount was needed not only to fatally irradiate the victim but also spread in varying ways to as many as 20 premises in London and beyond, necessitating a contacts tracing effort and decontamination program lasting several months. The number of victims known to be directly affected by the inadvertent [or some believe, deliberate] spread of polonium contamination after the Litvinenko incident was, at 17, thankfully low. But that toll would be substantially exceeded by those suffering a chemical or radiological attack anywhere at London 2012. London’s first responders, government and agencies, and above all, hospitals would, as on 7/7, be put to the ultimate test in peacetime.

Andy Oppenheimer is Editor of Chemical & Biological Warfare Review and former Editor of Jane’s Nuclear, Biological and Chemical Defence. An independent UK-based specialist in CBRNE (chemical, biological, radiological, nuclear weapons and explosives) and author of “**IRA: The Bombs and the Bullets - A History of Deadly Ingenuity**” (Irish Academic Press), he contributes to journals and lectures at conferences worldwide.

ISDS

INTERNATIONAL SECURITY
& DEFENCE SYSTEMS

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

ISDS offices around the world

We Operate across
7 practices

Safe City
Command Control, Communication Intelligence and Information Center (C4I2)
Emergency and Recovery programs
Urban crime prevention
Coordination plans and Concept of operation

Aviation Security
air port, plane, passengers, luggage, cargo

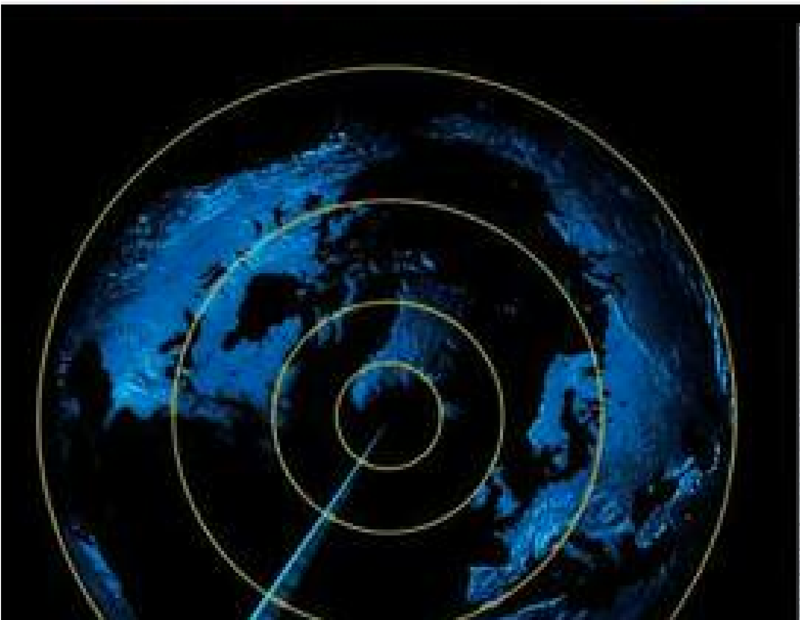
Maritime Security
Port facilities, Cargo Ships ,Cruisers, Shipping companies, Anti Piracy
A Recognized Security Organization (RSO) For the IMO's SOLAS and ISPS codes.

Infrastructure Security
Power Energy, Oil & Gas, Water Supply, Mass transportation, Communication, Mines

Defence
Special Operations, Intelligence , Search and Rescue , Air, Land and Sea Forces

HLS
Borders, Police, Intelligence agencies, Counter terror units, Emergency units, Government institutions

Security of Mega Events
Olympic Games, Conventions & Exhibitions, Sport Venues, Concerts, Delegations, and Dignitaries



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

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

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

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

Threats to Global Security

By Charalambos Varelas

Introduction

Since 9/11, the whole world is participating directly or indirectly in a "holy" war against terrorism. With the approval of the UN (UNSCR, 2001:1368,7158) in October 2001, the coalition forces are conducting war fighting by kinetic operations in the vicinity of Afghanistan in order to detain the number one wanted person in the western civilization (Bush, 2008) , Osama Bin Linden. Later on, coalition forces entered Iraq as it was suspected that it had in possession weapons of mass destruction, which were highly probable that some might fall under possession of Al Qaeda. Therefore, another war was initiated and despite the fall of Santam Housein, is still ongoing because Al Qaeda and other Non Compliant Groups are still alive and are targeting coalition and Iraqi citizens. Therefore, since the conditions for providing a safe and secure environment are not yet there, the war is still ongoing.

Billions of money spent, thousands of human lives lost, wars are ongoing, new security antiterrorist state measures have been implemented, and ten years after the world's most shocking event, the situation is still ambiguous. Are we winning against terrorism (Dylan, 2008)? Have we defeated terrorism? Is world safe today? Are individuals and societies affected by terrorism? For sure by looking at the media today we will daily see events related to terrorism, states still spend a lot for their security and counter terrorism protection, and worldwide there is still the feeling that we are all vulnerable. Therefore the least we can think of for sure is that we still feel unsafe. But are we really unsafe? Or this is just a part of an information operation campaign coming from unknown sources and interests? Through this analysis it will be proven that combating terrorism has many side-effects that certainly endanger individuals and societies directly or indirectly; side effects that drive us to the conclusion that our world is not safe at all.

In order to assess how terrorism nowadays represents a threat to global security and in what extent, a comprehensive but short analysis will be conducted based on an "effects based approach" comprising of three main principles:

- Identification of the threat and its consequences (effects on the individuals-societies-states)
- Current situation (focusing on the main incidents and public evidence)
- Assessment (on whether today's terrorism still represents a major threat)

Threats from Terrorism

Following the military standards in planning the adversary's courses of action, our approach in the holistic understanding and defining how terrorism nowadays can be a threat to modern societies, first of all we need to distinguish the threat (from terrorism) in two main categories: the direct and the indirect threat. Next in the essay we will refer and analyse in general terms the capabilities of the terrorist organizations based on motivations, available assets but most of all access to new technologies and military capabilities.

Direct Threat

The direct threat from terrorism derives from the capabilities and the motivation of the terrorist, to conduct direct actions against their targets. This category includes all actions that are initiated directly from the terrorist organizations regardless if they include military actions or psychological operations. In this category are included direct actions against people, infrastructure facilities, or both, having as a summit, the hit of the world trade centre on 9 September 2001. Additionally in this category we find information operations campaigns that terrorist groups organize and implement, in order to spread propaganda and similar psychological impact messages, to their target audience, mainly using the internet and the international media.

Military Operations

The main direct threat from terrorist organizations comes from military operations with direct attacks, creating insurgency and massive number of victims. The targets are often regular tactical army which are in war fight with the groups. One of most important courses of actions is the extensive use of suicide terrorists, against individuals and key infrastructure facilities, actions that augmented dramatically after the 2001 (Centre for American Progress, 2006, NATO Report, 2007) response of the western world against Al Qaeda and the fanatics Muslims. It is worth mentioning that terrorists have in possession high sophisticated military equipment, which is used as an example for making improvise explosive devices, No 1 after suicide attacks, causes of death in Iraq and Afghanistan.

However, the main threat derives from the possibility that terrorists have or will have in possession weapons of mass destruction, capability which is assessed unlikely but with extreme impact; the possibilities to get such weapons in possession, have augmented especially after the fall of the Soviet Union. As a similar tactic to create more effective results, terrorist groups follow the economic targeting process, which aims apart from the direct strike, to provoke economic loses to the target (Williams, 2008:177). Characteristic example of the past is the initiation of the negotiations between UK and IRA, just after IRA started the strikes in London, hampering the economic heart of Europe at that time (Williams, 2008:177).

Psychological Operations

After 9/11, we can see that the media exploitation from terrorist groups has been crucial for their propaganda and for the recruitment of new members. As it is analysed by Marc Sageman, a forensic psychiatrist, and former CIA agent, “world now faces a new terror; new generation of terrorists, who no longer answer to Al Qaeda”, but to their religion beliefs and hate for the western countries (Sageman, 2008). As an example, the Madrid’s train terrorist attack is believed to be an action of terrorists belonging to this category (NATO Report, 2007). The media have played a significant role not only in combating terrorism, but also in manipulating and disseminating particular messages to the public (Martin 2003:280). Opposed opinion to this is the Sawyer-Foster perception, that still Al Qaeda is strong and through the time will get even stronger and more dangerous (Sawer and Foster, 2008). Regardless the initiator, the analysts, keeps supporting the fact that the actions will be continued in the future.

However, the contradiction between the media professional responsibilities to make sure that people are well informed, and the attempts to direct the above mentioned effort to manipulate the global media for publishing propaganda that serve certain interests, is mainly responsible for the confusion that exists today in the world’s means of mass communication. As for terrorism, is always trying to exploit the psychological vulnerabilities to both enemy and friendly audience as the main mean for compensating various physical disadvantages. To that saying, terrorists using this kind of manipulation try to demoralise the enemy or filling them with fear (Gaynor, 2002); moreover, these actions are enhancing the motivation of terrorist allies, uniting them for the common goal (Schmid,2005:137-146).

Indirect Threat

As indirect threat, we identify the actions taken not by the Terrorist groups but due to terrorist actions, and which are having negative effects on individuals and societies. As an example we can refer to the extremely high cost that antiterrorist state measures and counter intelligence strategy (Cleeve, 2007) have, and which cost is in many cases in the detriment of social funding of entire societies, which in some -extreme- cases lead them to the lack of the absolute essential goods. Some of these effects will be reviewed later in the essay.

Effects of Terrorism

Following the second step of the process of analysing the “threat from terrorism”, we will deal with the effects of the threat of terrorism of all hierarchy social elements, such as isolated individuals-families, whole societies and entire states. In that way, we will see where we should look into later on, when we will review the current situation, trying to see the extension of the implications that terrorism has today in our world.

States

If we say that the only states that have been influenced from the global war against terror are the ones who participate in the armed conflict, we will be dramatically wrong. Apart from the military conflict, in which states pay extremely the high cost in money and in human lives, states spend extremely large amounts of money in antiterrorist equipment, regardless if they actually needed or not, just because the public opinion, or the "interests" are saying so. In many cases countries not that rich (Greece for example), spend non-impartial amount of money that they can in this direction (Greece spent 2 billion Euros for the 2004 Olympic games for security), of course again in the detriment of investing in other social aspects. Not to say that many states are now facing the edge of the economic failure due to such expenses. It is worth saying that behind the global information operation campaign of "terror is everywhere", apart from the actual terrorism, are also the private military companies, who for their interest, continue to provoke the continuality of the war.

The states also could face political instability due to the human loses that they have, especially due to the negative common opinion, which in most cases are against military campaigns thousands kilometres away for their country, serving external economic and political interests. Most recent example is the government of Netherlands, which finally decided to withdraw their forces from Afghanistan due to the will of the citizens.

Individuals-Societies

As the states facing problems, as an effect of counter terrorism, also the individuals and societies that live in, face also significant issues. As a tremendous consequence of the economical problems of a country, individual's unrest is an immediate feeling-action, as they are starting to live in a stressful and uncertain environment. The individuals, being bombarded daily with media statements that they live in an uncertain and insecure environment, decreasing simultaneously the levels of untrust from the citizens to the political status quo of their country. The criminality increases, stress and misery enters the families and as the media continue their propaganda of the societies being unprotected by terrorism, still people's mindset, is being confused and diverted from other important issues that should care about; or worse, governments, on the name of combating terrorism, are taking anti-democratical measures that transform our societies to enormous "free prisons", diminishing in that way our basic private human rights.

Current situation worldwide

So far in this essay, we (epidermatical) have touched and reviewed the current "courses of actions-threats" of the new terror and its possible affects in the whole society and state chain. To that saying, we now have identified how terrorism relates to threat, and we will continue by reviewing the today's situation, looking it from the operational level view. While we will not get into numerical details, we will see through contemporary examples that terrorism not only exists, but evolves all courses of actions mentioned above.

Direct Attacks and war fighting

Based on NATO intelligence gathering and reports, below we will review the main terrorist events-incidents that happened from 2001 and on, starting from 2002, just to depict how the global war against terrorism has affected the terrorist groups (including Al Qaeda). All information below is unclassified, retrieved from open sources, and is stated on various NATO reports [unclassified version releasable to UN and Partnership for Peace (PfP) members] on terrorism until mid 2010.

2002

- Tunisia: On April 11, a truck full of explosives is driven into a synagogue by Al-Qaeda, killing 21 and wounding more than 30.
- Pakistan: On May 8, a bus attack kills eleven Frenchmen and two Pakistanis.
- Russia: On May 9, a bomb explosion in Dagestan kills at least 42 people and injures 130
- India: On May 13, twelve people killed in a train crash when an extremist cut the trails.

- India: On September 25, two terrorists belonging to the Jaish-e-Mohammed group conducted a raid, killing 30 people.
- Indonesia: On October 12, Bali bombing kills 202 people
- Russia: On October 23, after the Moscow theatre hostage the victims were 120 Russian citizens and 40 terrorists.
- Kenya: On November 28, Kenyan hotel bombers leaves behind 15 people died
- Russia: On December 27, a truck bombing of the Chechen parliament in Grozny kills 83 people.

2003

- Philippines: 4 March, Bomb attack in airport kills 21 citizens
- Saudi Arabia: 12May, suicide (Al Qaeda) bombing kills 26 and injures 160
- Russia: On May 12, a truck bomb explodes near a government building in a Chechen town, killing 59.
- Russia: On May 12, female suicide bombers attack during a religious festival killing 13 and injuring 45.
- Morocco: On May 16, in Casablanca, 12 suicide bombers attack on Jewish targets killing 41 and injuring more than 100.
- Russia: On July 5, a bomb attack during a rock festival in Moscow kills 15.
- Russia: On August 1, a suicide bomb attack explodes in a hospital killing at least 50 and injures more than 80.
- India: On August 25, two bomb attacks in Mumbai kill 48 and injure 150.
- Turkey: On November 15 and 20, four suicide bombers attack various targets in Istanbul killing 57 and injuring 700.
- Russia: On December 5, a suicide bomber kills 46 while attacking on a train.
- Pakistan: On December 25, two suicide bombers kill 14 while exploding near the presidential convoy.

2004

- Mindanao Island: On 4 Jan a homemade explosive device kills 14 and injures 187 including the mayor who was the main target.
- Russia: On Feb 6, a bomb in the Moscow metro kills 40 and injures 147
- Quetta: On March 3, several bombs in a parade kill 47 and injure 130
- Madrid: On March 11, following the explosions of ten bombs in a train, kills 190 and injure 600.
- Islamabad: On May 7, a suicide bomber in a Mosque kills 245 and injures 125.
- Riyadh: On May 30, during a shooting rampage in an oil industry terrorist group leaves 22 dead and 25 wounded.
- Islamabad: On May 31 after a bomb exploding in a mosque leaves 21 dead and 550 injured.
- Russia: On Sep 1, terrorist seized a school in Beslan, wiring with explosives the whole territory. The seizure ended leaving behind 334 dead students, and 727 injured.
- Islamabad: On Oct 1, a bomb exploded in a mosque leaving 30 dead and 50 injured.
- Pakistan: On Oct 7, during a car bomb explosion, 38 people died and 100 were injured.
- Philippines: On Dec 13, a bomb explosion in a market leaves behind 15 dead and 58 injured.

2005

- United Kingdom: On July 7, suicide bombers attack a bus and three underground trains killing 52 people and injuring over 700.
- Egypt: On July 23, a car explosion at tourist sites killing at least 88 and wounding more than 100.
- Indonesia: On October 1, several bombs occur in resort, killing 20 people and injuring 129.
- India: On October 29, multiple bomb explosions leave at least 61 dead and more than 200 injured.

2006

- India: On March 7, several bomb explosions in a holy city, leaves 28 dead and more than 100 wounded.
- Pakistan: On April 11, a suicide bomber leaves 57 dead.
- Egypt: On April 24, bomb explosions leave 23 dead and 62 wounded.

- Sri Lanka: On June 15, terrorist attack with mines leaves 68 dead and 60 wounded.
- India: On July 11, train explosions leave 209 dead and 714 injured.
- India: On Sep 8, 2 bomb explosions leave 37 dead and 125 injured.
- Sri Lanka: On Sep 18, a bus full of explosives attacks a convoy of buses, killing 92 people including the suicide attacker.

2007

- India: On Feb 19, a train exploded leaving 68 dead and 49 injured.
- Algeria: On April 11, two suicide car bombs kill 33 people and injure 222.
- Pakistan: On April 28, a suicide bomber explodes after the minister of Interior's speech, killing 28 and injuring 35.
- Pakistan: On May 15, a bomb in a restaurant kills 24 and injures 25.
- India: On May 16, a bomb in Meccha Masjid kills 16 and injures 100.
- Turkey: On May 22 a suicide bomber kills 9 and injures 121 in Ankara.
- India: On August 25, twin bombing kills 44 and injures 54.
- Pakistan: On Sep 4, 2 bombs kill 21 and injure 74.
- Pakistan: On Oct 18, 2 suicide bombers kill 136 and injure 387.
- Algeria: On Dec 11, bomb explosions kill 37 and injure 177.
- Pakistan: On Dec 21, a suicide bomber kills 50 and injures 100.
- Pakistan: On Dec 27, suicide bombers kill 24 and injure 46.

2008

- Pakistan: On Jan 10, suicide bomber kills 23 and injures 58
- Sri Lanka: On Jan 16, a bomb in a civilian bus kills 30 and injures 65
- Sri Lanka: On Feb 2, bus explosion kills 20 and injure 50.
- Somalia: On Feb 5, 2 bombs kill 25 and injure 90.
- Pakistan: On Feb 29, suicide attack kills 27 and injures 40.
- Iran: On April 12, a bomb in a mosque kills 13 and injures 200.
- India: On May 13, various bomb blasts, kill 63 and injure 213.
- India: On July 26, 17 blasts kill 50 and injure 160.
- Lebanon: On August 13, blast kills 18 and injures 45.
- Algeria: On August 19, a suicide bomber kills 43 and injures 45.
- Pakistan: On Sep 6, 2 bomb explosions kill 50 and injure 80.
- Yemen: On Sep 17, a car bomb kills 16 and injures 16.
- Pakistan: On Sep 20, a bomb in a hotel kills 60 and injures 250.
- Pakistan: On Oct 10, a suicide bomber kills 113, and injures 100.
- India: On Oct 30 13 blasts kill 84 and injure 470.
- India: On Nov 26-29, in Mumbai, various fire attacks from terrorists kill 173 and injure 327.

2009

- Somalia: On Jan 24, a car bomb explosion kills 14 and injures 30.
- Sri Lanka: On Feb 9, a suicide bomber kills 30 and injures 90.
- Pakistan: On Feb 20, a bomb attack kills 27 and injures 65.
- Pakistan: On April 5, a suicide bomber kills 22 and injures 50.
- Pakistan: On April 18, a suicide bomber kills 27 and injures 65.
- Iran: On May 28, an explosion in a Mosque kills 19 and injures 80.
- Pakistan: On June 5, a suicide bomber kills 38 and injures 50.
- Russia: On August 17, a bomb attack kills 25 and injures 164.
- Pakistan: On Oct 9, a minibus explosion kills 41 and injures 100.
- Pakistan: On Oct 28, 2 car explosions kill 117 and injure 200.
- Russia: On Nov 27, a truck bomb attack kills 26 and injures 90.
- Pakistan: On Dec 28, a suicide bomber kills 43 and injures 60.

2010

- Pakistan: On Jan 1, a suicide bomber kills 105 and injures 100.
- India: On Feb 13, a bomb kills 33 and injures 60.
- Pakistan: On Mar 12, 2 suicide bombers kill 57 and injure 100.
- Russia: On Mar 29, 2 female suicide bombers kill 40 and injure 100.
- India: On Apr 6, a fire attack from a terrorist-militia group kills 75 people.
- Somalia: On May 1, 2 bomb blasts, kill 39 and injure 70.
- India: On May 28, an explosion in a train kills 128 and injures 145........

From the main terrorist events, on purpose we left outside incidents occurred on Israel, Afghanistan and Iraq as the incidents on these targets are almost a daily event! Just for the records, 50% of all significant incidents have been conducted by Al Qaeda.

Additionally to this list we could add also a similar list from incidents that the last minutes were prevented, mainly in the US and in Europe; as milestone events we can refer to the attack to the JFK airport of New York, the metro in London, and the more recent incident which was planned for the World Cup in South Africa; the last one was revealed by a detainee in Baghdad which among this event he revealed that Al Qaeda in Iraq has already change leadership (the previous leaders were killed in a Time Sensitive Target action), and now is ready for new strikes (Jane's, 2010). That is also the main reason that all almost NATO countries have increased their counterintelligence measures, and their threat terrorist level (NATO Counter Intelligence Summary, 2009, Cleave, 2007)

Israel is over the last years in a constant war with many Islamic militias and terrorist groups due to which, societies keep the alert status always in the highest level, as the attacks are a usual and daily phenomenon. So, even Israel which is a military giant, is still vulnerable to such attacks; such attacks which have provoked in many occasions civil unrest, tremendous casualties, and a society full of stress and fear for the unexpected. The fear is increasing, while there is the possibility that Non Compliant Groups, might get in possession, weapons of mass destruction, endanger the whole security area, by putting it in a devastating situation.

After the fall of Santam Housein, everyone believed that a new era would start for the Iraqi citizens. However, the situation after his death changed dramatically, as terrorist groups and mainly Al Qaeda started a merciless war against the allied forces operating in the area. The number of the victims is increasing day by day, as the attacks is a daily event. The unstabilised situation was the main reason that drove President Obama to order the final withdrawal from Iraq until the end of 2010 (Congress 2009:3). The main excuse was the augmented need for support in Afghanistan. Without doubt, military analysts, referring to the casualties and the actual effect, compare Iraq with Vietnam, characterising the whole operation as a "military fiasco". The cost is extremely high and the political cost from the human loses even higher. The last is the main reason that drove the US Government to "exchange" US troops with Troops from Private Military Companies, allowing them to reach so far the number of 50.000 over the last period (Glanz, 2008).

It is worth mentioning that since the "operation Iraqi freedom", the terrorist attacks have increased by 607 per cent by targeting mainly US citizens and military personnel (Centre of American Progress, 2006, CIA, 2007). For some analysts, Al Qaeda, is still persistent (Sawer and Foster, 2008), while others believe that the fear comes from a new generation of terrorists, more effective and "high tech equipped" (Sageman, 2008).

As terrorist groups still operate in Iraq, the second front of the" holy war" is also on going in the mountains of Afghanistan. Taliban warriors still are opposing coalition forces, provoking again significant casualties. Again in Afghanistan the suicide bomb attacks against military targets is a daily event, showing to the global community, that the threat has not yet being eliminated.

Indirect Involvement

The indirect involvement comprises of actions taken by the terrorist groups, which at least directly do not have immediate reaction to the audience. Having said that, the extent use of the media from the terrorists to pass their messages, to provoke fear and to publicize themselves, has tremendous consequences to the societies as the fear is constantly on our minds (Williams,2008:182-183). On the other hand, media always do not lose the opportunity to announce such incidents, since they will raise their numbers and consequently their sponsors and their income. So despite the negative impression that goes to the societies, media behaving as a business satisfy the groups becoming also part of the problem.

Apart from the non professionalism actions of the media, we must not forget that the "war industries" make a lot from the ongoing war with terrorism, having so, a strong motivation to preserve such situations. Terror is used as a psychological weapon and not just as acts of murderers. As stated previously, the entire idea of terrorism is "based on manipulation and the modification of a group's behaviour due to threats or actual harm against a minority of that group's population" (Schmid, 2005).

One of the most significant developments of the terrorist movements is the use of the media, as we saw above in the essay. The groups have "their own" TV and radio stations to promote their actions, cause and air their grievances. Satellite TV stations such as Al Jazeera, and Al Arabiya, always transform the terrorist related events, looking them from a regional perspective, rather than a western one (the opposite of what CNN has done in the past). Beyond this publicize, terrorist groups have the capability throughout this broadcast to deliver code messages, to spread propagandistic packages and religious lectures, promoting the unity of all Islamic Nations for the "Holy War" (Williams, 2008:181-182)

Overall Assessment- Conclusion

The daily event list, show us that for sure, that the main area of Terrorist Activities, is Iraq, Afghanistan, Russia and East Asia. Thousands of people have lost their lives, and will continue losing them, in the name of "justice" and "holy war". Ten years after the direct involvement of the United States in the war, the results are for sure ambiguous; it is still very immature to say who is winning or who is losing, and therefore, it will be at least surreal to state that world is safe today.

There are parts of our world that suffer a lot from terrorism, as human loses provoke pain and misery. However, the loses of lives also from the soldiers of the coalition forces that participate in the war against Terrorism, also provoke pain to the western societies, that actually are not affected so far by direct attacks. So, the western countries although they may feel safer from the others, still feel the effects from the terrorism in their daily life, either with media or with anti social measures that states take to keep up with their forces in war. The main issue in this war is that, it is not ending because strategic interests do not want it to end. And this is something that we need to take into account in our assessment. Directly or indirectly, the whole world is affected by terrorism. The possibility on strikes in western states cannot be excluded. As history has shown silence sometimes can be very bloody; the future-possible possession of weapons of mass destruction by terrorists, can lead to the end of an old era and the beginning of a new world; a new world, ruled by the economic and the strategic interest.

The world today seems that it is not safe. And regardless if it could be safe, or it is not, the issue is what it seems. This is the global picture, this is image that we get every day; this is what we need to fight: the image of the media that our world is not safe today. Why? Due to terrorism itself, or because of interest? The answer is somewhere in the middle: Terrorism gave the initiative to some audience to feel unsafe, but economic interests have taken this opportunity in order to preserve this situation and transform it to a global issue.

Concluding, regardless who is behind or who preserves such situation, the main point is that daily evidence since 2001, lead safely to that terrorism still represents a significant threat to global security, and will continue in the near future. Regardless who and why, the issue is that our world is deeply affected by terrorism, and for sure the messages are not optimistic. Analysts assess that the worst have not yet arrived. True? As an analyst myself I must base my assessment on facts than emotions. Facts show us that the world today is threatened by terrorism and it is highly probable this threat continue in the mid and long term time frame.

References

- Bush, G. (2001) CNN “break up news”, 14 Oct. Portsmouth Herald.
- Cleave Van Michelle, K. (2007), “Counter Intelligence and National Strategy”, School for National Security Executive Education National Defence University, (2007)
- Congress Report, 2009,”Measuring Stability and Security in Iraq”, In accordance with the Department of Defence Supplemental Appropriations Act, 2008, Section 9204, Public Law 110-252, March 2009.
- Dickson, P. (2008) “Star and Stripes” Associated Press 67 (193), 27 Oct: 8.
- Director of National Intelligence (2007), “ The terrorist threat to the US homeland” Washington DC: Director of National Intelligence
- Dylan, T. (2008) “Winning or Losing?” Economist [online] available from:
- <http://www.economist.com.specialprojects/displaystory.cfm?story.id=11701218>
- Gaynor, B. (2002), Terror as a strategy of psychological warfare. Retrieved from:
- <http://www.ict.org.il/articles/articledet.cfm? =articleid=443>
- Glanz, J. (2008), “Report on Iraq Security Lists 310 Contractors”, the New York Times, 29 Oct 2008.
- Hoffman, N. (2006) “Inside Terrorism”, Columbia University Press, New York: 283,285.
- Jane’s, 2010, “Jane’s defence weekly”, vol: 47, issue 21, 26 May 2010, pp18.
- NATO, Counter Intelligence Summary, (2009), [restricted], not releasable to the public.
- NATO Intelligence reports on “Annual Terrorist Activities”: 2003, 2004, 2005, 2006,2007,2008,2009 (not releasable to the public).
- NATO Report, 2007, November [Classified], “Intelligence Summary Report”
- Martin G. (2003), “Understanding Terrorism: Challenges and Issues”, Sage Publications, 2003, pp280.
- Sageman, M. (2008), “Leaderless Jihad: Terror Networks in the 21st century”. Philadelphia: University of Pennsylvania Press.
- Sawer, R. and Foster, M. (2008) “The persistent threat of Al Qaeda”, Annals, Aapss, 6(18): 99.
- United Nation Security Council Resolution, 2001, 12 Sep: 1368
- United Nation Security Council Resolution, 2001, 28 Sep: 7158
- Williams Paul, D. (2008),”Security Studies, An Introduction”, Routledge, London and New York, 2008:171-184.

Haralampos Varelas is an officer, graduate of Hellenic Military Cadet School (SSE) currently serving in Special Forces (Rangers’ Unit) specialized in counter-intelligence. He holds a Masters Degree in Terrorism, International Organized Crime and Global Security from Coventry University (UK).

SUPERGUM Civilian NBC Protective Products

Supergums personal protection products are strong and durable enough to provide effective personal safety, yet lightweight and flexible enough to allow total freedom of movement.

The line of products

*Accsessories

*Infant Shield

*Masks

*Child Shield

* Adult Hood

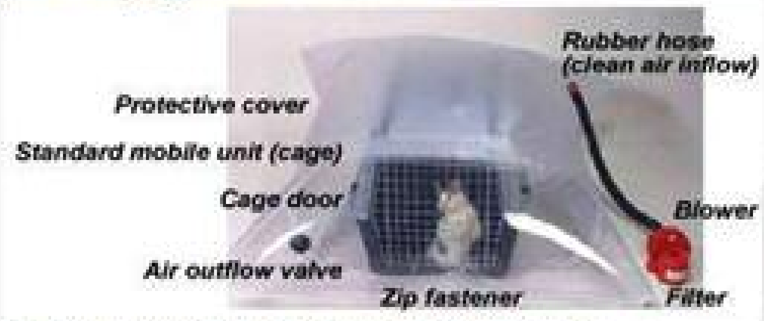
*Pet protective kit

*Body & skyn protection

* Panoramic Hood

Animal Protective Kit

Pet Protective Kit. The kit is used for protecting pets (dogs, cats and pet birds) against NBC hazards.



The Pet Protective Kit comes in three sizes:

- For pets weighing up to 25 kilograms (such as cats or Poodles). Suitable for a cage of 50 □ 69 □ 48 cm. Contains one filter-blower unit.
- For pets weighing from 25 to 45 kilograms (such as Pointers). Suitable for a cage up to 102 □ 69 □ 76 cm. Contains one filter-blower unit.
- For pets weighing more than 45 kilograms (such as Dobermans or German Shepherds). Suitable for a cage up to up to 102 □ 69 □ 76 cm. Contains two filter-blower units.

Web: www.supergum.com
E-mail: info@supergum.com
Tel: +972 3 9365692
Fax: +972 2 9367742

Chemical and Biological Weapons Preparedness

By Leah Roberts

The United States has extensively studied chemical weapons since WWI, when the German army used chlorine gas against U.S. troops near Ypres (Tucker, 2006). Formal research on biological weapons followed in 1943 after WWI, and the debriefing of Japanese military scientists that conducted unethical research on humans in their Unit 731 (Harris & Paxman, 2002). Since the initiation of these warfare programs, the U.S. along with numerous other countries, have ran the Arms Race against one another, both covertly and overtly (Alibek, 1999; Tucker, 2006; Mangold & Goldberg, 1999). The number of chemical warfare agents has risen from the original few rudimentary choking and blister agents to over 30 agents that include nerve gases, toxins, and incapacitating agents. Similarly, biological warfare agents considered for weaponization have grown from those easily biomined from environments, to more than 30 known disease causing agents, as well as potential agents never seen which are genetically engineered in laboratories (Zajtchuck, 1997; Tucker, 2006). The U.S. military, civilian federal employees, and emergency responders are not adequately prepared for a confrontation with most of these combined, more than 60 agents of warfare. Even in the early 1980s, U.S. and NATO troops were ill equipped to deal with a chemical or biological attack (Seagrave, 1981, pg. 200-202). The likely opponents in a war involving chemical or biological agents, which were Russia and Middle Eastern terrorist groups either trained their fighters to function in bulky, somewhat disabling protective gear for extended periods of time, or were trained to be accepting of any personal injury and death which would arise from such an attack, respectively (Seagrave, 1981; Tucker, 2006).

A small survey regarding knowledge and training for chemical and biological warfare was conducted through the website, Surveymonkey.com. The survey asked participants to answer 5 detailed questions to the best of their ability, without disclosing any classified information, and gained valuable insight into the preparedness of our military, civilian federal employees, and emergency responders. The survey began on May 15, 2010 and results were collected on October 7, 2010, but the survey remains active. There were 25 respondents, of which, 16 had a military background, seven were civilian federal employees (CFE) with no military background, one was a contractor for military-style operations, and one was an emergency medical responder (ER) with no military background.

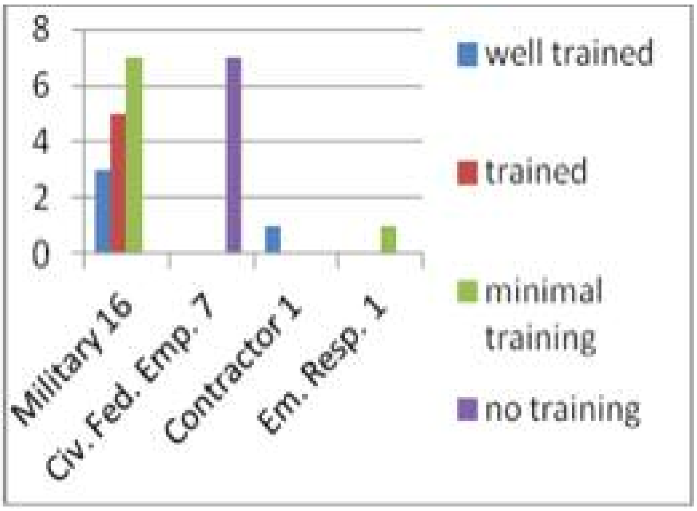


Figure 1. Training

Respondents were asked to state their background (military, CFE, or ER) and estimate the time spent in training and protective measures for aerosolized warfare confrontations. Figure 1 shows the training as described by respondents, where well trained corresponds to extensive training with regular refreshers; trained corresponds to initial extensive training with either yearly or no refreshers; and minimal training as the one day spent on proper use of a mask done in basic training.

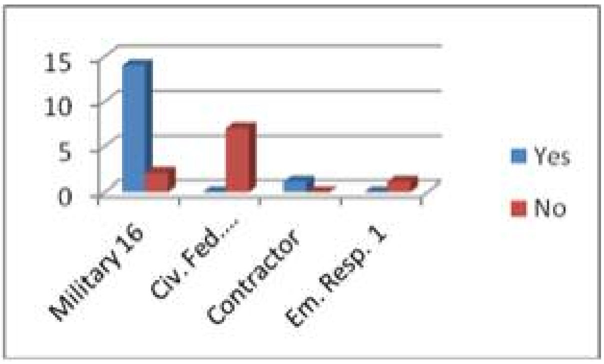


Figure 2

The respondents were then asked if they were taught anything about which chemical or biological agents might be used against them. Figure 2 below shows a graph of the responses. The majority of military respondents answered, "yes" with a short explanation, mostly describing a category the particular agents would be classified into (choking agents, blood agents, etc.). None of the civilian federal employees were either trained for confrontations with chemical or biological weapons, or taught which of them might be used against them in the field. This is an important issue since as a civilian federal employ, they are expected to deploy to hostile areas if required by their agencies. Most of these areas, such as Afghanistan, Iraq, and Korea are areas where there has been noted to be either government operated chemical or biological warfare facilities, terrorist groups operating in the vicinity that expressed interest in these/ noted that they had them, or historic record of the use of certain warfare agents (Tucker, 2006; Seagrave, 1981; Mangold & Goldberg, 1999).

The third question asked if respondents were taught anything about training of any prospective enemy's strategies, preparation, and protective gear. This is an important concept that follows the logic of knowing your enemy. The responses were interesting as several of the "yes" responses were followed by an explanation that depicted training about contaminated battlefields, how long certain chemical or biological agents would persist in various environments, and the gear given to the respective respondent's own group, rather than information pertaining to a prospective enemy. Only those who noted "yes" with no explanation and those with an explanation noting opponents specifically were counted as a "yes" and the rest were counted as "no". Figure 3 displays these results. Interestingly, most of those who answered "yes" with detailed answers described being taught about the former Soviet Union's and Iraq's capabilities, equipment, and possible strategies.

The next question asked respondents what tools they were given, if any, to protect themselves such as protective suits, gas masks, detection kits, prophylactic medicines, etc. The answers for most of the military respondents included masks, over-garment suits, gloves, detection kits, decontamination kits, antidote kits and prophylactic medications. Four military respondents answered "none". Out of the seven CFE respondents, three had some basic personal protective equipment training and one had training with chemical detection kits and aerosol alarms. Both the contractor and the emergency responder answered with extensive training with elaborate protective gear and equipment.

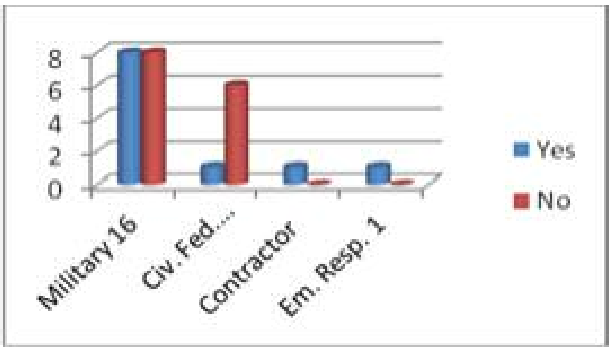


Figure 3

The final question simply asked respondents to list chemical and biological warfare agents they are aware of without looking these up from any resource. The idea for this question was to gain awareness of the extent of knowledge each responder had. Figure 4 below illustrates the results relating to chemical warfare agents and Figure 5 corresponds to results for biological warfare agents. Each chart lists a variety of known agents, respectively from the literature and historic records.

The answers given in this survey outline the training and knowledge deficits of a portion of military members and nearly all of the civilian military employees with regards to

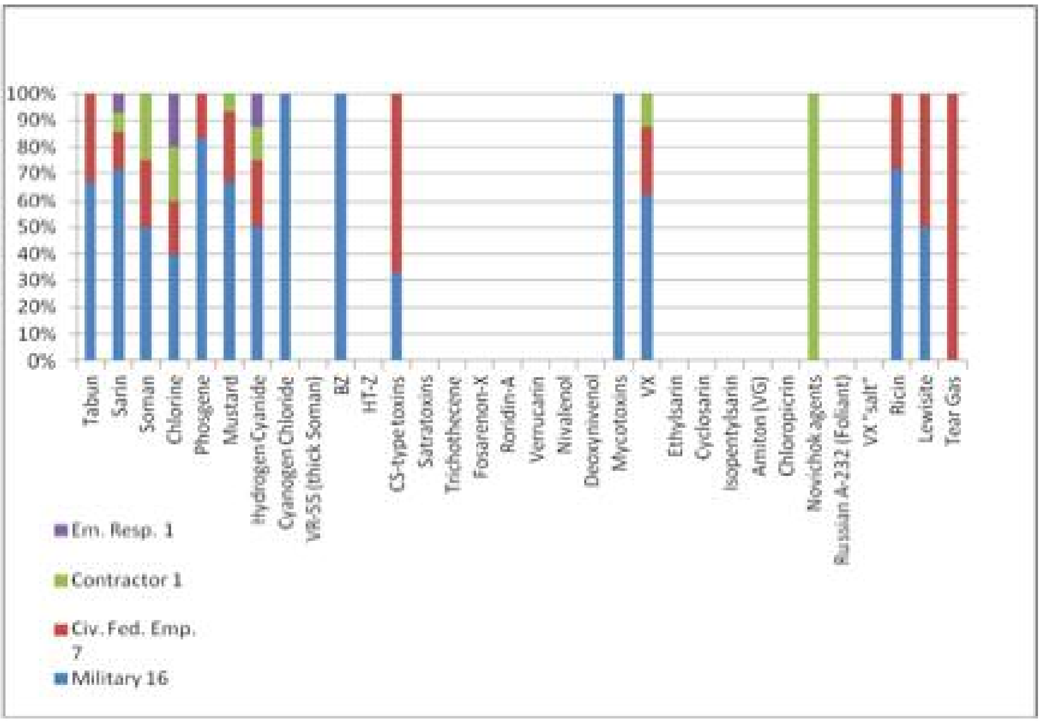


Figure 4 – Chemical agents

chemical and biological warfare threats. There is a certain need for better training of military members and civilian federal employees who are expected to deploy to hostile countries. Because there was only one respondent, who is an emergency responder, the data obtained cannot be adequately distributed across the entire quantity of emergency responders and more information will be needed to assess needs for training in this group.

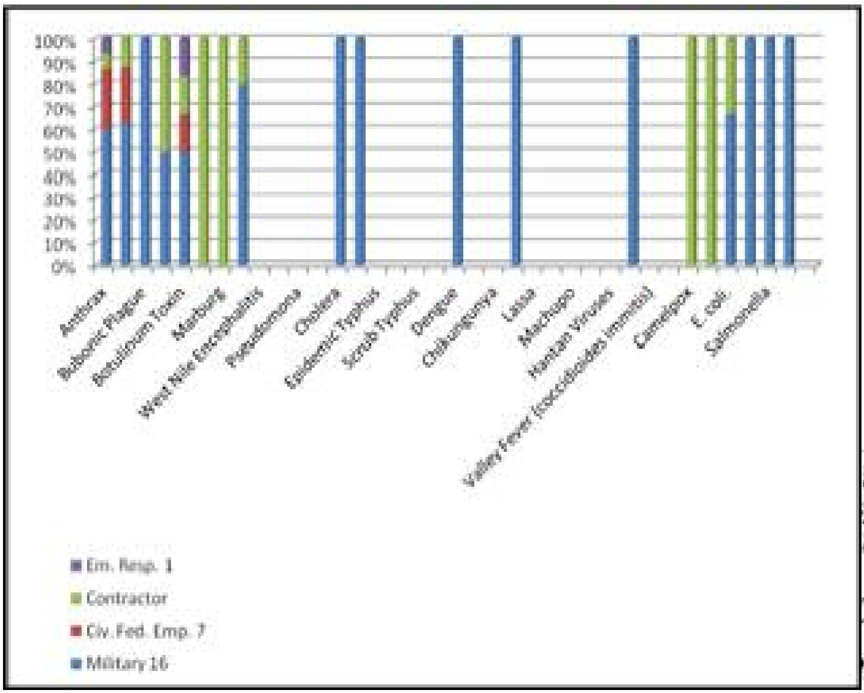


Figure 5 Biological agents

Bibliography

- Alibek, K. (1999). Biohazard. New York: Random House, Inc.
- Burgess, S. F. (2007, August). South Africa from the perspective of WMD supply networks: Indications and warning implications. Strategic Insights, 6(5).
- Carroll, M. C. (2004). Lab 257. New York: Harper Collins.
- Dando, M. (2006). Bioterror and biowarfare a beginner's guide. England: Oneworld Publications.
- Harris, R., & Paxman, J. (2002). A higher form of killing. New York: Random House, Inc.
- Ketchum, J. (2006). Chemical warfare secrets almost forgotten. California: Chem-

books Inc.

- Lederberg, J. (2001). Biological weapons limiting the threat. Massachessetts: The MIT Press.
- Mangold, T., & Goldberg, J. (1999). Plague wars. New York: St. Martin's Press.
- Nahmias, R. (2009, September 3). Traces of chemical weapons found in Hezbollah warehouse. Retrieved 14 October, 2010, from http://www.ynetnews.com/articles/0,7340,L-3771736,00.html
- Regis, E. (1999). The biology of doom. New York: Henry Holt and Company, LLC.
- Romano, J. A., Jr., Lukey, B. J., & Salem, H. (2008). Chemical warfare agents; chemistry, pharmacology, toxicology, and therapeutics, second edition. Boca Raton, FL: CRC Press.
- Seagrave, S. (1981). Yellow rain. New York: M. Evans and Company, Inc.
- Silverberg, M. (2008, July 17). America's bioterrorism nightmare. Retrieved 13 October, 2010, from http://www.familysecuritymatters.org/publications/id.633/pub_detail.asp
- The Trumpet. (2009, September 8). Hezbollah found to have chemical weapons. Retrieved 13 October, 2010, from http://www.thetrumpet.com/?q=6510.5003.0.0
- Tucker, J. B. (2006). War of nerves: Chemical warfare from WWI to al-Qaeda. New York: Pantheon Books.
- Wessely, S. (2001, October 20). Psychological implications of chemical and biological weapons. British Medical Journal, 323(7318), 878-879. Retrieved from: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1121425/
- Zajtchuck, R., & Bellamy, R. F. (1997). Medical aspects of chemical and biological warfare. Washington D.C.: Office of the Surgeon General Department of the Army United States of America.

Leah Roberts graduated from Saint Louis University's Master's program in Bio-security, (GPA 3.95/4.0). She also earned a Bachelor's degree in Public Health. Leah is an independent researcher concentrating on chemical and biological weapons threats and writes geopolitical and threat assessment profiles of foreign countries. She is an accomplished editor in a variety of written works and is sought after for her skilful experience. In addition, Leah is a teaching assistant for the Saint Louis University Institute for Bio-security.

Interview with Ralph Langner: Stuxnet, the new face of cyber warfare

By Ioannis Michaletos

Stuxnet is a Windows-specific computer worm first discovered in July 2010 by VirusBlokAda, a security firm based in Belarus. While it is not the first time that hackers have targeted industrial systems, it is the first discovered worm that spies on and reprograms industrial systems, and the first to include a programmable logic controller (PLC) rootkit. It was specifically written to attack Supervisory Control And Data Acquisition (SCADA) systems used to control and monitor industrial processes. Stuxnet includes the capability to reprogram the PLCs and hide its changes.

Ralph Langner is a German cyber-security expert and an international leading researcher in SCADA security. He is the President of the Langner Communications GmbH based in Hamburg. Over the past few months, he unravelled the importance and the technical capabilities of the Stuxnet malware that inflicted mostly the Iranian nuclear program and has spread in several industrial locations across the world. According to Langner's findings, a new era in cyber warfare emerges, that should be taken into account by security and military specialists across the world.

Ioannis Michaletos: How do you view the future of cyber warfare after the emergence of the Stuxnet?

Ralph Langner: Stuxnet marks the starting point for a new era of real cyber warfare, meaning physical destruction. Follow-on attacks are possible and first of all the militaries across the world should learn from this experience and built up their security systems. It is a whole new era and the emergence of a cybewarfare weapon that can inflict great physical damage to industrial systems. All should learn from this experience and analyze what happen in order to prepare for the future which is going to be formed by these kinds of technological advances. In contrast to the past, the Stuxnet destroys the physical infrastructure and can paralyze the capabilities of an industry and even a state.

Ioannis Michaletos: So that means that warfare changes face, a kind of «military revolution»?

Ralph Langner: I don't know if we can talk about a «revolution», but certainly this is a new type of weapon and a new type of an attack. It is indeed an asymmetrical attack. For example I estimate that the cost for developing Stuxnet, does not exceed 10 million Dollars, but it is capable of destroying equipment costing 100 times more. Therefore it is a low cost and high affectivity weapon. In simple terms, it is a fantastic weapon. Moreover, there are no casualties in human lives involved and this is also a factor to be taken into consideration. In a nutshell the Stuxnet does exactly what a sophisticated weapon like a missile does -destroying military or civil infrastructure- but without harming human lives, and quite possible in an even more accurate fashion that conventional weapons. It's a dream come true for the future of warfare.

Ioannis Michaletos: Is it likely to assume that more cyber attacks will occur in the future?

Ralph Langner: Yes, absolutely sure. I have to say that many people and journalists especially that I have discussed about seem frightened of the possibilities of this type of cyber warfare. First of all, because of the high level of success of this malware, there are going to be similar operations in the future and lets not forget that this type of «cyber-battlefield» seems to be more effective and of course no lethal for civilians and military alike. It's surely better that a full blown war and I assume that similar attacks will happen in the future. Actually I presume that a second version, a «Stuxnet 2.0» is underway; this is what logic dictates and the pace of technological advancement, plus the advantages I mentioned earlier.

Ioannis Michaletos: How well prepared is the private sector Worldwide, against such type of an attack?

Ralph Langner: In Northern Europe and USA, there is vulnerability against such type of an attack, due to the dependency of these states in automation and computer systems. There is a real danger in most respects against such type of an attack because services and industries depend on a critical level and would be subject to great difficulty when being attacked in such a manner. In less technologically developed countries, the issue is significantly less, because their systems operate in a different mode, with less dependency on technology and electronic systems. I have to say, that preparation for such a peril is extremely important nowadays and I have to emphasize that many private corporations in Europe-USA, they have no idea how vulnerable they are against such a cyber threat. The world is not prepared to deal with such cyber attacks. Industrialized nations, especially in Northern Europe, are most prone to a system failure because of the aforementioned.

Ioannis Michaletos: As far as the Iranian nuclear project is concerned, do you believe that Stuxnet really inflicted considerable damage?

Ralph Langner: Absolutely yes. A key factor on that is the following: Iran's Bushehr Nuclear Power Plant was about to begin full operation in early August 2010, but still has not due to the damage caused to its centrifuges. The operator of the system, stop the processes as soon as possible in order to avoid further damage to the equipment, thus the aim of the attack seemed exactly to be the overall delay of the nuclear program. The cleaning process from the Stuxnet, in the Iranian nuclear project systems could take more than a year and will require a lot of effort. Thus the whole of the Iranian nuclear program has been postponed. For the time being, the only option for the Iranians is to concentrate into getting rid Stuxnet from their operating system and delay other projects at hand.

Ioannis Michaletos: Several analysts have asked the question, why has not Stuxnet attacked the North Korean nuclear project as well? Is it because of the different mode of operations between the Iranians and the Koreans?

Ralph Langner: First of all this question should be asked to the developer of the Stuxnet and what was his specific intention. From my point of view, I can say that it is quite possible that the North Koreans have different automation programs, and they may have better security procedures that may halt the intrusion of such a malware. The Iranians seemed to have less security controls that they should have.

Ioannis Michaletos: Who do you assess was behind this cyber war attack

Ralph Langner: It is crystal clear that nation states were behind this attack and not private companies or individuals or academic research teams. I would say that the two nations heavily involved were USA and Israel along with the critical assistance of a third force, quite possibly either Germany or Russia. All of those, through their collaboration are capable for this kind of a malware development in our age.

Ioannis Michaletos: How do you view the evolution of Stuxnet? Should the people be afraid that future malware may interrupt with airport control systems or other transportation means?

Ralph Langner: As I mentioned earlier, a first evolution stage would be the creation of a «Stuxnet 2», aiming the same targets in Iran and with the same purpose. In general evolutions of this type of malware in the military theatre should be expected across the world. For the general public there is concern, since it is likely this malware can be copied and then be sent to infiltrate civilian infrastructure as the one you referred to. I would state as an example the interference through malware of the traffic lights system in a city that can cause transportation chaos or the production processes of a food plant or a chemical industry with dire consequences. Lastly, we have to prepare ourselves for these types of unfortunate scenarios. Organized crime groups and terrorists would not miss the opportunity of staging similar attacks, once they acquire such technology, and make use of the advances in cyber warfare in the future.

Ioannis Michaletos (Editor South East Europe, Coordinator of South-eastern European Office World Security Network Foundation), has been educated in the UK in the fields of Political Science (BA) and HRM (MSc). He is occupied as an independent journalist-security analyst for Greek & international organizations and media, including Jane's information Group, European Oil & Gas Monitor and European Energy Review. He is a correspondent analyst for ISRIA a security assessment agency.

ST53

AVON

www.avon-protection.com
protection@avon-rubber.com

The Multi-Role Respiratory Protection System Providing Operational Flexibility

Avon's revolutionary ST53™ multi-role Respiratory Protective Equipment (RPE) System has been developed specifically for specialist applications where the user needs to respond to changing operational conditions.

For the first time, the operational flexibility required by specialist users from their respiratory protection system is being offered in a purpose designed product. Depending on the threat or operational circumstances at the scene of an incident, ST53™ can be configured to provide the ideal protection mode.

The ST53™ combines Avon Protection Systems' FM53™ mask with new and innovative modular breathing apparatus technology to provide positive pressure SCBA and/or PAPR capability. The ST53™ system provides the operator with total flexibility to select the necessary level of protection quickly and efficiently whilst continuing to operate effectively at an incident.

Available in two versions: The standard ST53™ with full back frame offers 4.7 litre, 6.8 litre and 9 litre lightweight carbon cylinder options, a short duration variant; ST53 SD™, provides a belt or harness carry option with 1 and 2 litre cylinder options meeting the needs of law enforcement and special forces for short-term tactical operations.

AVON

Trusted in Hazardous Environments

Why al Qaeda is different from other terrorist groups of the past?

By Charalambos Varelas

Introduction

Since September 11, 2001 our perception of the world has changed more significantly than the world itself. The threat had been known before, nevertheless, the act of war disguised as a terrorist attack made the entire world aware of the new dimensions of a global vulnerability. The new type of terrorism, unlike all its previous forms, did not express any territorial or political demands and allowed the United States, regarded as its main enemy, to draw the final conclusions on the causes of the attack. The message declared the destruction of that world system whose most important pillar after the Cold War became the United States, left without a super power partner (Delpech 2001). The unanimous decision of the United Nations Security Resolution on September 12, 2001 interpreted the New York attacks as a threat to peace and was completed on the 28th with an action plan aimed at fighting terrorism (UNSCR 2001).

Since then, after spending billions of dollars and thousands of human lives (Dickson 2008), after eight years of a global war against international terrorism worldwide, the results are, unfortunately for the western policy, ambiguous. Al Qaeda is still the main target of the coalition forces, and Osama Bin Landen is still number one wanted person all over the world (NATO Intelligence report for terrorism, 2008). For sure, the coalition forces have managed many decisive victories, not only by capturing or neutralizing significant number of AQ's leaders but also by destroying strategic key infrastructure facilities (Heyden 2007). However, despite these successes, the world has not yet calmed from the fear of terrorism. Since the initiation of the "Operation Iraqi Freedom", terrorist attacks have increased by 607 per cent (Center for American progress 2006). Most of the foreign military and policy experts admit that the primary targets are the United States and American civilians (Director of National Intelligence 2007), without however being conducted in US territory since 2001 (Dylan 2008).

It is undeniable that the declaration of the global war against Terrorism by the president of the United States (Bush, 2008) seems mainly against Al Qaeda, though there are numerous terrorist organizations which hamper everyday the safety and security of the world. So, is this global war just a world war against one enemy? And if so, why are the results not more decisive? Why can not wait The United States and its Allies have a clear victory after 8 years? What are the reasons behind this insufficiency? Is it because the coalition forces are doing something wrong or because Al Qaeda is so strong? The answer, though not easy, is somewhere in between.

According to statistics, ninety per cent of terrorist organizations throughout history fail within a year while fifty per cent of those that last longer fail within ten years (Rapoport 1992:1067). That makes Al Qaeda the exception of the rule. The organization concentrates the majority of the strategic characteristics a terrorist organization must have to rule, terror and survive. These characteristics, such as beliefs, sustainment, training and decisiveness alone, are not enough to afford the publicity and the appreciation Al Qaeda enjoys. Additionally, no terrorist group so far had such a strong enemy for such a long time as the United States has. Paradoxically, instead of losing, Al Qaeda's leaders claim that "it is stronger and more capable now than it was on 9/11" (Hoffman 2006: 283). Al Qaeda is certainly very different from other terrorist groups in the past, and although it has many common characteristics with others, it gathers all those elements that are needed for forming the "ultimate terrorist group".

The main objective of this essay is to study and analyze the reasons why Al Qaeda is different from other terrorist groups in the past. In order to achieve this aim, we will follow the evolution of terrorism over the last years, as well as changes in the ideology, methods and tactics the terrorist groups used in the past. Simultaneously, we will examine and designate the fields in which Al Qaeda differs significantly compared to other terrorist groups in history. Then, through a simple and clear comparison, we will understand how Al Qaeda manages to embody the most important of the strategic characteristics a group needs in order to survive and profess the ultimate terror in the entire world.

Classification of Terrorism

Terrorism and terrorist organizations groups and persons can be classified on the basis of various aspects. Throughout this classification it will be easier to understand the true motivations and ideology in which the terrorist organizations base their cause. Then it will be easier for us to compare the characteristics of past terrorist groups.

First, we can group the terrorism on the basis of the theatre of activity and the effective range of the terrorist acts in the following arenas: Local (within a country or region), Sub regional (affecting the security of two or more countries), Regional (certain regions such as South Africa, Middle East), International (affecting two or more regions) and Global (threat to global security). On the basis of the persons, groups, organizations, or countries providing support to terrorist acts, terrorism can fall into the following categories: Individual, Group, State and International terrorism. Depending on the motivation, terrorism can be classified in Religious groups, groups championing racial superiority, ideological/political groups and Nationalist-separatist terrorist groups.

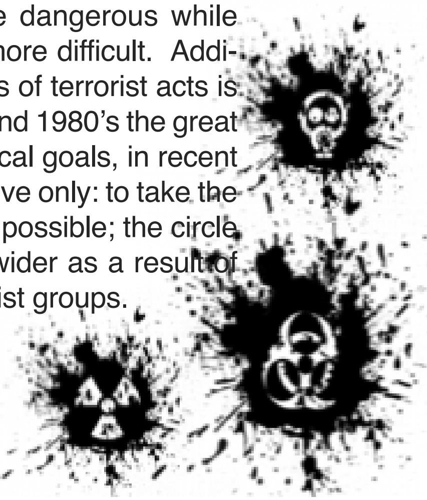
Additionally, on the basis of level of determination, terrorism can be classified as: Emotional terrorism without a final political goal, terrorism with well defined and rational strategic objective and finally terrorism with exaggerated strategic goals. The last classification is based on the response of the opposing party; we have terrorist groups “mapping the limit of the state tolerance” without risking the total elimination of the group, and we have groups which seek to provoke responses that will radicalize a particular ethnic group or minority. The last classification is the most serious: in this case the group may provoke the reaction of a whole region. Al Qaeda and the 9/11 strikes had similar goals; to provoke American (NATO or western) responses and counter-strikes that could lead to the “unification” of the Islamic World and result in the radicalization of the Arab states.

It is obvious from the classification that Al Qaeda’s characteristics show us that it is a global organization with a complete ideology, international connections, and global area of operations. Moreover, Al Qaeda, though not the only identified terrorist group by UN and other Non Government Organizations, still has the “privilege” of having as a major enemy the most powerful state (United States). It used to be that the United States participated partially in the hunting of terrorist groups, but for the first time in history, it participates in a long and expensive global war against multiple terrorist “enemies”. From this we can understand the seriousness of the situation Al Qaeda has provoked.

Characteristics and evolution of Terrorism

One of the most comprehensive summaries of the features and characteristics of new international terrorism was compiled by National Commission on Terrorism established in the United States in 1999. According to that survey, the Commission established a series of characteristics that the new face of terrorist organizations like Al Qaeda has, compared to others in the past.

During the past decades the character and objective of international terrorism has significantly changed. The international community, for example, devoted 12 conventions to the investigation of terrorist activities. Although the number of countries opposing terrorism is growing, a few states continue to provide support to terrorism; in certain cases terrorism is a factor of state policy. The features of a terrorist threat have changed and today both terrorist groups and acts are more dangerous while countering them is much more difficult. Additionally, the fatality numbers of terrorist acts is rising. While in the 1970’s and 1980’s the great majority had clear-cut political goals, in recent years they have one objective only: to take the lives of as many people as possible; the circle of motivations has grown wider as a result of structural changes in terrorist groups.



Among the differences that the old fashioned terrorist groups had with the new: the groups have a cross-border financial and logistic support system, they are increasingly independent from the support of a state which makes fighting them with economic sanctions increasingly difficult, the terrorist groups widely use the most up-to-date encoded communication technologies, and finally, achieving their goals takes an increasing number of lives.

Al Qaeda has been transformed into an International terrorist organization which is still surviving despite the war against it and it continues to play a significant role in the decision make process of many states and ideologies.

Global Terrorism: The ultimate Evolution

Nowadays globalization is one of the most determining and at the same time the most discussed processes. The concept in itself has no consensus-based definition. Some experts say globalization is a permanent phenomenon in the history of mankind, others link it to capitalization, and there are many who regard it as a typical feature of a post-modern era.

Looking to the past we see that almost all Terrorist groups have limited area of operations with the exception of PLO, which was the first to carry out airplane hijackings, expanding in that way its borders worldwide. PLO was the first known terrorist group that even in a limited way posed a threat to global security. After PLO, the most chronically active "global capable" terrorist group is Al Qaeda which, as mentioned before, remains the number one global threat. From the strikes in United States embassies all over the world, to the strikes in 9/11 and in Middle East and Europe, Al Qaeda has even expanded its operations from the known world to the cyber one!

To that end, we must take into account that the global capabilities of Al Qaeda flow from their global "f*atwas*", ideologies, funds, tactics and outside state-supporters.

Ideology and Motivations

Analyzing the motivations, it can be stated that the "sound ideological foundation" of extreme right and extreme left (Euro-terrorism, for example) was increasingly replaced by ethnic nationalism and religious extremism. In most cases these two motivations "co-exist" as illustrated by the Sikh militants fighting for the establishment of the state of Khalistan, or the fundamentalist Egyptian Islamic Jihad (EIJ) with the goal of establishing an Islamic state in Egypt. These motivations fall into four categories: religious extremism, nationalism, ideology and psychology.

Religious extremism makes up the basis of religious terrorism and Islam is its most dangerous form. A practical manifestation of this trend was the bombing of the New York Trade Centre (1994) carried out by a Sunnite terrorist. The 9/11 strike was also an action from followers of extremist Islamic movements. Some extremist militant elements of other religions also carry out violent terrorist acts such as the Christian group of Aryan Nations that is the most active in North America, and the Jewish Defence League which acts by nationalism and religious intolerance are executed in Israel.

One of the most striking features of the nationalistic motivation factors is ethnic nationalism. Typically it is a long-term motivation factor. Examples include the terrorist organizations in Yugoslavia, Northern Ireland, or the Basque regions, as well as Palestinian and Kurd terrorist groups. Nationalism is often blended with separatism and irredentism, especially in the post soviet regions. The terrorist acts indicate that groups with nationalist-separatist objectives are the most active.

Comparison of existing terrorist groups with Al Qaeda

After analyzing the categories of the terrorist groups, it comes very easy to our mind to put every known terrorist group in the appropriate classification. Having already enough evidence to argue that Al Qaeda is a unique terrorist group, we dare to say that she is perhaps something different than a simple terrorist group, something which history will show in future. However, for those that believe that only the circumstances have driven Al Qaeda to the publicity it now has, or now it is helpless and weak, and only lonely jihadists take actions on behalf of it (Sageman 2008), the comparison that follows is the practical evidence for the opposite.

Beliefs and Supporters

All terrorist organizations actions are based—of course–on their beliefs, motivations and ideology. The ideology is the beginning, the present and the future of these groups. This means that the better the foundation the more possibilities the group has to survive in time. So, we see the left based terrorist groups, whose aims were mainly the independence of a specific region, to have a limited area of operations. We see the Red Brigades in Italy, the ETA in Spain, the PKK in Turkey and many others whose actions were based in left ideology and claimed an independent state within their state. It is natural that their supporters are mainly idealist's supporters of ideology; communists, believers of the old Soviet Union, dreamed of a new communism-based society. In that case firstly the audience is very limited, and secondly, after the fall of the Soviet Union, these groups quickly realized that they lacked a strong foundational ideology. Therefore, they, soon or later realized that it was the beginning of the end.

On the other hand, the groups that either based their ideology on nationalism or manage to transform leftist ideas into ethno-nationalist beliefs have more possibilities of surviving and being more effective. Groups as PLO and LTTE two of the most important terrorist groups ever, based their motivation in an ethicist ideology, which even today ensures a large network of new believers-fighters and a future. The religious-based terrorist groups on the other hand, have an even larger audience, augmented decisiveness toward their primarily targets, and easier ways of recruiting new members. Particularly, when they combine nationalism with unfulfilled prejudices and conjunctive religious beliefs, the foundations are so strong that they easily override state borders, giving an international perspective and creating a global capable actor. The one and only group that has managed to achieve this goal is without doubt Al Qaeda, which has created the conditions to maintain itself as well as develop its future.

Tactics-Structure-Funds

Another strategic advantage that Al Qaeda has over other groups is the structure of the organization and the nature of the tactics it uses. Although most terrorist groups use the "hierarchical pyramidal structure", Al Qaeda leaders preferred to keep it in the "main flatter, more linear and more organizationally networked" (Hoffman 2006: 285). "A tight fixed complete organization with a strong foundation- a whole network and a subculture of rebellion at the same time" (Dylan 2008). Their leaders, especially Osama Bin Laden, wanted to create a complete and organized community in which everyone has rights, privileges, considers himself important and necessary to the organization, and in which the common objective is the realization of the "f*atwas*" and ideologies whatever the cost may be (Esposito 2002).

While other groups have limited audience and space, their primary objective is to hide from the central state and to announce their demands, without risking arrest. Their actions and tactics are based mainly in Improvised Explosive Devices and assassinations (like LTTE killed Indian president Rajiv Ghandi), whether the targets are of high importance or not. For sure, their restricted capabilities are reflected in their results, just as their ideology reflects their limited motivation and future. Additionally, their income comes mainly from robberies as well as human and drug trafficking, a fact that shows the uncertainty of their entire existence (as it concerns safety and jeopardize). These "light" groups usually lack training and their (left or extreme right) ideology is the significant issue that either divides them, or destroys them.

However, many terrorist groups are operating against entire nations, as they have the support of a large audience, belonging mainly to national-religious ideology terrorist groups, such as IRA, LTTE, PLO, PKK which are opposed to an entire country, with significant or not results, but at least in a way that the whole world recognizes them as very important groups. These groups are the first to initiate an open war against their host-nation whether they have the support of the common opinion or not. They have a strictly hierarchical pyramidal structure, a strong leader, very good training, significant income coming from various sources (human, drug, weapon trafficking), an outside state supporter and, finally, a developed network of recruitment that preserves the future which is “The first strategic objective” of every group.

Al Qaeda on the other hand, by being “not only an organization but also an idea” (Economist 2008a), has all the previously mentioned characteristics in an order of magnitude that no other has achieved so far. The first generation of terrorists trained in camps in Afghanistan with the assistance of the United States, which was engaged in a larger Cold War campaign against the Soviets. It has now turned against its former benefactor and enjoys the bequeathed tactical knowledge. The fact that the coalition forces are still in war with Al Qaeda has not impacted their levels of training. On the contrary, after the invasion in Iraq, incidents of attacks have increased by 607 per cent (NATO report 2007). The safe and secure environment that the mountains of Pakistan provide continues to play a significant role to the effectiveness of the group. Moreover, the income from Osama Bin Laden himself, the drug trafficking, and the cover support from Islamic states classify Al Qaeda in the first position in the bases of wealth among all terrorist groups.

When it comes to “tactics”, guerrilla and urban warfare were the most common and usual reactions of the most sophisticated terrorist groups. The groups already mentioned, who opposed to an entire state, often, apart from isolated strikes, provoke the state in an open style war, to show off for commercial reasons too. However, the first time that a new word appeared to the world scene in the base of a new tactic of war, after the 9/11 strikes, was the phrase “asymmetric threat”. Actually, it was the first time that an organized and international schedule was developed for combating the so-called “asymmetric threat”.

Martyrdom- Asymmetric Threat

Without doubt, Al Qaeda is not the first to use suicide terrorist actions in the history of terrorism. The background of suicide terrorism is very rich. The PKK, LTTE, and PLO are some of the most classic examples of groups that used suicide attacks for achieving their goals. The psychological impact of suicide terrorism on a victim community is enormous. The implication is that the organization using suicide terrorism is willing to sacrifice its members and is able to recruit people who are willing to die for the cause, i.e. they must be a determined, long lasting threat. That is of course the main reason for having so few groups using the tactic. As a result, the use of Suicide Bombers (SB) brings an enormous tactical advantage to an organization.

So far it seems that Al Qaeda has imitated these groups and created its own suicide bombers. But, if just Al Qaeda did exactly the same as its processors, why did the term “international defence against asymmetric threat” appear only after 9/11? The answer appears to imply that the way that Al Qaeda used the suicide attacks points to something deeper. Indeed, looking back to past events we see that all the other suicide attacks consisted mainly of women or men carrying bombs or explosive devices, targeting civilian or military personnel—sometimes key infrastructure facilities—without any serious need of planning or scheduling. On the other hand, Al Qaeda has amazed the world by the genius and precise planning of 9/11 and other previous strikes.

After the accidental failure of the operation “Bojinka”, which was a schedule of simultaneous destruction of twelve US airplanes in the air, Al Qaeda on the 2nd of August in 1998 attacked in the US embassies in Nairobi, Kenya and Tanzania killing 250 people. It was a well organized plan which was executed by suicide bombers. The fact that it had been planned for years shows exactly the professionalism which Al Qaeda dealed this issue with. Moreover, seeing the budget as though the intelligence gathering of their members, we come to the conclusion that the act of 9/11 was similar to a military action, based on accurate intelligence, followed by a detailed decision making process plan and finally executed with pure professionalism. Additionally, the strikes in Madrid and London, although the originator is not confirmed yet, they do not seem to be a job from a group of the past, leaving clues for deeper interference of Al Qaeda. To that, the investigation that conducted after these strikes proved that the bombers were inspired and guided by Al Qaeda.

Al Qaeda has managed to transform the global war of terrorism into a complex war of actions and mainly ideas, finding that way recruits in every part of the world. As Muslims which are the main audience-target, are everywhere, the "jihad" is easier; the union of all Islamic countries against the United States and their allies seems easier than ever since the ideas are much more difficult to deal with, and need more time to fade away. Muslim Kids brought up from New York to Pakistan instead of love and grammar, they are taught how and why they must become suicide bombers for Allah (Phares 2007: 245).

It can be easily assessed that this war of ideas, if not confronted in a clever manner with decisiveness it will have major impact in the entire world, as the Jihad will be extended to the next generation of fanatic Muslims and the war of ideas will continue hampering the global security. This achievement is without doubt part of Al Qaeda's strategic goals and objectives, fact that drives us to the apprehension of how well organized and scheduled their leader's plans are. This long term planning and acting capability has not been met anywhere before, from any other terrorist organization. The war of ideas that Al Qaeda professes, is an endless source of fanatic new believers who create the foundation and the base of its future.

Relation to Media-Publishing capability

In the era of satellites and endless internet, Al Qaeda had the privilege of being in the spotlight for a long time. Since the idea and the scenes of a ruthless terrorist group overcome in ratings many other significant events, it seemed to the media that Al Qaeda is an open and profitable issue. Additionally, after the invasion in Iraq and the important loses that it caused, internet was the ultimate and safest mean to reorganize, recruit and continue their fight. Since the beginning of their existence, the strikes in New York and until today, Al Qaeda had the covert support of many Islamic television channels and radio stations, through which it had a certain seat and a safe way to publish their ideas, to unify the Islamic people against the common enemy; the United States and the western policy.

The fact that Al Qaeda got that publicity is of course because of their opponent. In the past, the world knew about terrorist groups only from certain television channels which were not that independent and therefore not objective. They covered only the major events such as the Munich Incident (due to the Olympics), and some activities of IRA (due to the power Great Britain). The fact that other terrorist groups lived in anonymity because of the non objective and sometimes guided media, in case of Al Qaeda the media worked quite differently. Actually, nowadays the flow of information through the media, although still not objective it includes all aspects of an issue, fact that enable us to see all the views and make out our own point of view.

Conclusions

If instead of the numerous glorious and undefeatable Persian army, the three hundred Spartans had in front of them just a numerous and anonymous army, perhaps history would not care about them. The significance of the enemy is augmented by the power of the opponent. In our case Al Qaeda has taken enormous publicity not only because of its characteristics and capabilities, but also because it turned against the most powerful state in the universe. Throughout this essay, we saw the evolution of the "terrorism", we classified it in a way, and we identified through comparison, why indeed Al Qaeda is different from other terrorist groups in the past. Although the present and future capabilities are a matter of strong contradiction, the fact remains that the world war against terrorism is still on-going. "No one seems to win, but no one seems to lose either" (Economist 2008a).

Of course the circumstances helped the evolution of Al Qaeda a lot, and along with the evolution of the media and modern technology, this organization managed to take advantage of every little or important situation and seized the opportunity for the benefit of its own objective. The capability that has to renew its supporters and fighters is unique and based on the ideology and motivations their "fatwa's" professes (Esposito 2002). The fact that has complete and safe training facilities, in conjunction with the wealth that it owns, establishes the bases in which it will build their future. So far the results of its strikes are the most lethal having also the unique privilege and capability in having as area of operations the whole world.

Whether we like it or not, we conclude from the above that the "threat from Al Qaeda is likely to last for decades" (Economist 2008b). For sure, as we saw "there are essential elements contributing to Al Qaeda's survival and ultimate resurgence" (Sawyer and Foster 2008). However, the time is enough for the experts to reconsider the circumstances that brought this group in the zenith of its glory and the rest of the world to an endless fear and terror, to find the way to eliminate the threat and provide a safe and secure environment to the citizens of the world.

References

- Bush, G. (2001) CNN "break up news", 14 Oct. Portsmouth Herald.
- Dickson, P. (2008) "Star and Stripes" Associated Press 67 (193)] 27 Oct: 8.
- Delpech, Th. (2001) Die Liebe zum Tod.Uber den Umgang mit dem Terrorismus In: Internationale Politic, November: 54-56.
- Director of National Intelligence (2007) "The terrorist threat to the US homeland" Washington DC: Director of National Intelligence.
- Dylan, T. (2008) "Winning or losing?'' Economist [online] available from
- <http://www.economist.com.specialprojects/displaystory.cfm?story.id=11701218 > [3 November 2008].
- Economist (2008a) [online] available from <http://www.economist.com.specialprojects/displaystory.cfm?story.id=11701267 > [3 November 2008].
- Economist (2008b) [online], available from <http://www.economist.com.specialprojects/ displaystory.cfm?story.id=11750386> [3 November 2008].
- Esposito, J. (2002).Unholy War: Terror in the name of Islam. New York: Oxford University Press.
- Heyden, N. (2007) "The complexity of terrorism". In Ranstorp, M. (ed) Mapping terrorism research: State of the art gaps and future direction, London: Routledge: 219-352.
- Hoffman,B. (2006) "Inside Terrorism", Columbia University Press, New York: 283
- Hoffman,B. (2006) "Inside Terrorism", Columbia University Press, New York: 285
- Interactive Map (2006): Al Qaeda Attacks Around the World. Center for American Progress. Retrieved on September, 06.
- NATO (2008) Intelligence Summary Report: Restricted.
- NATO (2007) Intelligence Summary Report for Iraq: Restricted
- Rapoport, D. (1992) "Terrorism", In Hawkesworth, M. and Kogan, M. (eds) Routledge encyclopedia of government and politics''. London: Routledge: 1062.
- Sageman, M. (2008) Leaderless Jihad: Terror Networks in the 21st century. Philadelphia: University of Pennsylvania Press.
- Sawyer, R. and Foster, M. (2008) ''The resurgent and persistence threat of Al Qaeda'' Annals, Aapss, 6(18):99.
- United Nation Security Council Resolution (2001), (UNSCR), 12 Sep: 1368.
- United Nation Security Council Resolution (2001), (UNSCR), 28 Sep: 7158.

Haralampos Varelas is an officer, graduate of Hellenic Military Cadet School (SSE) currently serving in Special Forces (Rangers' Unit) specialized in counter-intelligence. He holds a Masters Degree in Terrorism, International Organized Crime and Global Security from Coventry University (UK).

Hummingbird Syndrome: Why Disasters Occur

By Luiz Hargreaves

Once there was a wildfire in a forest, the animals were in panic… they saw a hummingbird going towards the river, picking up some water in order to try to extinguish the fire. He repeated this gesture frequently and thoroughly.

When the other animals saw the gesture of the kiss-flower, the Lion asked him, "Hummingbird, what are you trying to do? The Hummingbird replied, "I am fighting the flames." To which the Lion responded, "Do you realize you cannot put out the fire out with just your effort?" The Hummingbird said, "But, at least, I'm doing my best."

This story has been told by many as an example to be followed, with the idea being that we should always do our best, regardless of what the others may do. From the standpoint of managing emergencies and disasters, the actions of the hummingbird often cause disasters. However, several lessons can be learned from this small story.

The hummingbird did not follow a previously defined Disaster Plan, which should have been constantly checked and all the animals should have trained according to the Disaster Plan. The animals did not work as a team.

The hummingbird ignored the actions taken by other animals, which could result in duplication of efforts. He worked alone, without following any protocol or command set.

Therefore, he has used ineffective measures (he failed to extinguish the fire) and probably watched the forest burn down in flames, perhaps causing the deaths of many animals, and possibly himself. Using this story we can draw a parallel with real life disaster preparedness and emergency response.

What has just been described is called "the Hummingbird Syndrome." The Hummingbird Syndrome describes a crisis situation with no previous plans for preparedness, mitigation or prevention. In these situations, many people flee and some act as the "Hummingbird," acting on their own instincts, based only on their beliefs. In most cases, they believe they are being useful and effective in their methods. The result will probably be disastrous.

Many disasters can be avoided. By definition, disasters are critical situations where the response capability is lower than the magnitude of the main event. A small fire managed without the good practices can lead to a major disaster.

We can classify crises and disasters, didactically, in four phases:

- Pre-impact,
- Impact,
- Post-impact, and
- Recovery

We live permanently in the Pre-impact phase, waiting for the next crisis or disaster. The question is not if they will occur but, where, when and why. We often believe in a Post-disaster phase, the worst has gone, forgetting that this phase coincides with the Pre-impact of the next event.

Some of the activities that precede the Impact phase are, prevention, preparedness, assessment of vulnerabilities, threats and risks assessments, monitoring of critical situations, mitigation preparation, preparation of business continuation plans, and disaster and/or contingency training. In other words, what we should be doing now in order to avoid the next disaster.

Applied to any crisis, vulnerabilities that are superficially analyzed, threats that are unrecognized or underestimated, in environments where there is no culture of preparedness and prevention for critical situations, invariably result in serious crises and disasters. When this occurs, the Hummingbird will probably be remembered as a hero, but will be victim of the inefficiency of the system which has failed to prevent disaster. It will be too late. It is up to friends of the Hummingbird to tell of his courage, but, however, he will have died in vain…

Qylur
Security Systems, Inc.

The First Fully Integrated Security Checkpoint Solution for Large-Scale Public Venues

We are committed to enabling mass public venues to achieve an ideal balance between the highest security level available and a business model that provides the highest standards of service to their customers by enabling: Ultra -High People Flow, Multi-Threat Detections Capabilities, High Detections Rates with Minimal False Alarms, Lower Cost of Ownership and Operations, Deployment Agility, and Operational Threat Mitigation. These features are the backbone of solutions designed specifically for large scale public venues and their guests who deserve the best security, the best business fit, and the best personal experience.

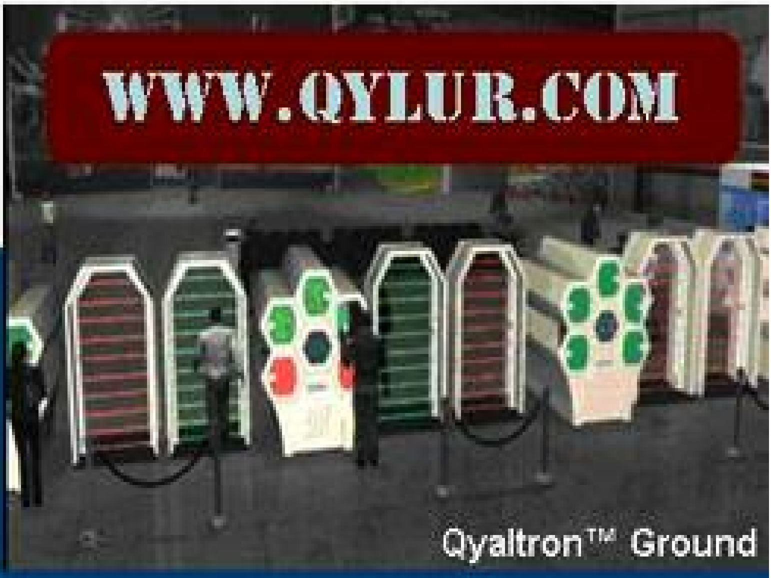
Qylatron™ the first fully integrated security checkpoint system for large public venues is designed to provide both an optimal security screening solution to security managers, and an entirely new experience to visitors, by maintaining the natural flow, and respecting their right to privacy.

The Qylatron™ family of checkpoints include:

- **Qylatron™ Rail**
- **Qylatron™ Ground**
- **Qyltaron™ Air**

Qylur Security Systems Inc.
1015 East Meadow Circle
Palo Alto, CA 94303

Tel: (650) 845-2000
Fax: (650) 845-2004



Qyaltron™ Ground

Vulnerabilities and Threats: A Relationship Not Always Understood

By Luiz Hargreaves

In recent years, organizations have increasingly been incorporating strategic planning into management. All organizations, including State(s), have missions, values and visions. In other words, it is necessary for everyone in these organizations to understand what it means to work for this corporation or what it means to be a government employee. The understanding of strategic planning is essential for the commitment of employees and the success of the organization.

The first step in this process is analyzing internal and external environments.

In an internal environment, we find strengths and weaknesses that are linked with the opportunities and threats (external environment). These are the concepts of the "SWOT matrix", used extensively in strategic planning in organizations, but not always when we are talking about State or government strategies.

The internal analyses of the organizations' forces are of great importance in determining conditions for searching opportunities. It makes no sense to talk about opportunities that are not linked with the forces of the organization. What can be understood as an opportunity for one corporation may not be for another.

Conversely, the weaknesses of the organization and/or State(s) are generating elements of vulnerabilities that can be linked with threats that lead to disasters. The inventory of risks must be constructed over that knowledge. Only after evaluating the vulnerabilities, threats and risks, is it possible to begin preparedness, prevention and mitigation of crises or disasters.

Frequently, we find some risk analyses based essentially on threat assessments. In such cases, the risk can be falsely low. There are threats that are known because of their intensity and frequency of occurrence. This is the case of "Hurricane Season" in the Caribbean, Tornado seasons in the Midwest United States, and summer flooding in several Brazilian cities. There are, however, some "invisible" threats which, for several reasons (i.e. political issues or because people believe they will never occur), are not considered. This is the case, for example, of Terrorism.

There are several countries where the terrorist threat is seen as unlikely or even impossible to occur according to many. In these places, one common analysis is developed upon the statistics of attacks in prior years. The problem is statistics have little value because we cannot predict future events based on the absence of such events in the past. As a result, there are neither terrorism laws nor a culture for preparation, prevention and response. Because of this superficial or even weak analysis, organizations as well as the State(s), become vulnerable to terrorist attacks, resulting from the perception of low risk.

The condition which permits a threat to exist is a vulnerable system. A tornado in an open field, without threatening property or persons, is just a natural phenomenon and not a threat. However, in other places where houses are vulnerable to strong winds, it becomes a credible threat. This analysis seems quite simple however, it is not always realized.

Vulnerabilities are directly linked to weaknesses. It is the weaknesses of the organization or the State that lead to vulnerability. States that believe they are completely immune against terrorist threats are more vulnerable to attack than those with a culture of protection, even if those with a culture of protection have been victims of terrorist attacks more often. It is a paradox. Countries that have suffered recent attacks and have changed their prevention and response procedures in order to face new challenges and are therefore far less vulnerable to a new attack (even if the threats are serious) than countries believing they are safe because they have never suffered an attack before. Vulnerabilities imply more chances for the loss of lives and property.

In an analogy to biological systems, we would say that those immunologically stronger (low vulnerability) are more protected against specific virus transmission than those who have little or no immune protection (high vulnerability).

The early warning for crisis situations, including terrorism and natural disasters, should come from committed and trained communities, in order to respond to situations that can potentially lead to critical events.

The adoption of a pro-active approach to reduce weaknesses and vulnerabilities (controllable events) should be the role of the organization, as the reduction of threats (non-controllable events) is much more difficult, if not impossible.

Investing in prevention and preparedness is an essential path to decrease risks and lower vulnerability resulting from weaknesses. It is a way of reducing or eliminating threats, indirectly.

The search for mitigation and direct elimination of threats is, however, often shameful and difficult to implement because they are non-controllable variables. This does not mean mitigation and elimination of threats should not be attempted until removing a threat and allowing the system to remain vulnerable will protect the State and Organizations?

The answer for these issues could be to work on weaknesses, reducing the vulnerable systems, while the threats are monitored and response systems prepared. This is valid for States and organizations.

Luiz Hargreaves, AAS, MD, MSc, is a qualified Expert in Crisis Management, Disaster Planning and Response, Health Care Management and Travel Medicine. He is a Medical Doctor, Political Scientist (MSc), and Crisis Manager, with 25 years of experience in Disaster and Emergency Planning for Corporations, Public Events, Public Safety and Counterterrorism.

Islamic Terrorism in Mexico

By Leah Roberts

Executive Summary: Islamic terrorism is an ominous growing problem at our borders, particularly our southern border with Mexico. Over the last decade or so, numerous persons with known connections to Islamic terrorist organizations were reported to be in Mexico. Among these groups are Hezbollah, Hamas, and al Qaeda, Islamaya Al Gamat and members / supporters from African Islamic terrorist organizations like Al Shabaab. The most important of these appears to be Hezbollah because of their ties to Venezuela, and Iran; also because of their global presence of sleeper cells and relationships with anti-American countries.

Hezbollah is a known terrorist group that poses a threat to the U.S. at home and abroad. Recent arrests in the U.S. and Mexico of Hezbollah members, and the trends in tactics used in attacks by Mexican cartels being trained by Hezbollah members, reveal the ominous presence of this group at our borders. Hezbollah has several large communities of sympathizers in Mexico as well as in the Tri-borders region of Argentina, Paraguay, and Brazil. The Tri-borders region has long been known to be a hot-spot for anti-American activities, money laundering, drug and weapons trafficking and falsification of travel and identity documents. Hezbollah members use the Lebanese communities as well as their connections with the drug cartels of Mexico to fund terrorism, launder money, to get their members into the U.S., and to sell drugs to Americans as a way of killing infidels.

To aid in this mission, Hezbollah members have opted to train Mexican drug cartels to use more advanced weaponry, to make bombs, and to use fear tactics such as beheadings to influence communities, political leaders, military, local police, and anyone they need to manipulate in order to achieve their objective. They have set up cells in small sympathizer communities across the globe, most importantly, in Canada and Mexico, but also in many regions in South America and West Africa.

There are numerous routes taken by these people to do their trafficking, make connections, earn money, acquire weapons, and recruit new members. Tunnels are becoming more elaborate and advanced in their engineering due to the experience of the Hezbollah members who are notorious for building sophisticated tunnels under the Lebanon border with Israel.

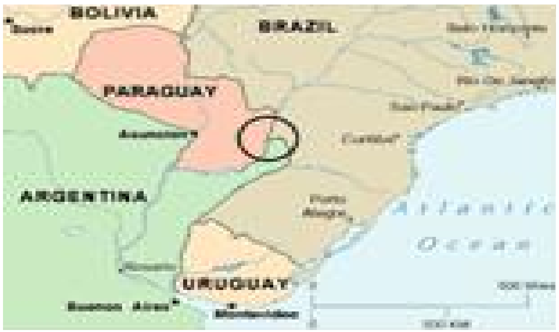
Unfortunately, there is money to be made for helping these terrorists in achieving their goals. In addition to those drug gangs who agreed to share their turf and work along with Hezbollah members on common ground, there are random American citizens aiding in this operation for money whether they realize the scope of it or not. Even large banking companies have been found to launder money for Hezbollah-backed Mexican drug cartels.

There are numerous recommendations that may aid in the curbing of these acts. Some research and education in the identification of key points for identifying Hezbollah activities and influence will go a long way in this conflict. Policy changes need to be enacted and enforced so that Other Than Mexican illegal aliens are not released on their own recognizance after they are detained at the border. Prison officials and police need to be trained to identify potential Hezbollah members by their language, identifying tattoos, symbols, and confiscated paraphernalia

Area at risk: All of Mexico, but specifically those towns bordering the U.S.; All Mexican border areas within the U.S.; All of the United States; Canada

Statement of Information: Hezbollah, the bastard child of Iranian Revolutionary Guard Corps (IRGC) and a lower class Lebanese Shi'ite minority group has cells in many countries of the world. Although Lebanon has a mere 4.2 million people, over 10 million Lebanese live in other countries. Lebanese were one of the first Middle Eastern immigrants to enter Latin America, and did so as early as the 1870s. (Thompson, 2010) Focus on those Lebanese in Latin America recently has been on their influence on drug cartels, money laundering, and trafficking of drugs, weapons, and humans between the U.S. and Mexico. Further concentration on the Lebanese communities spread out throughout the globe reveal hubs for the activities conducted by Hezbollah and all of the anti-American groups which give them any sort of aid, including but not limited to concealment, uninterrupted travel through regions to home bases in Lebanon, laundering of money, smuggling operations, trafficking of drugs and weapons, and numerous avenues of illegal activity to fund not only their operations, but also the building of infrastructure in the sympathizer communities to promote cooperation. Lebanese communities in Latin America also provide a rich source for new recruits (Webster, 2010; Vernaschi, 2010).

Lebanese communities in Latin America supported terrorist attacks by Hezbollah as early as 1992 when the Argentinean Israeli Embassy was bombed. The Tri-borders region of Argentina, Paraguay, and Brazil is a known area for Hezbollah operatives to carry out all sorts of illegal activities including but not limited to drug smuggling, falsifying documents (so Hezbollah personnel can pretend to be Mexican in attempts to sneak across the U.S. borders with other Mexicans, often using aid from drug cartels), money laundering, music piracy and other intellectual copyright infringement, and weapons smuggling (Rollins & Wyler, 2010; Thompson, 2010; Barrett, 2010; Ynet News, 2009;). The former FBI Director, Robert Mueller, was quoted confirming the fact that Middle Eastern persons were learning a bit of English, assuming Hispanic-sounding names, and attempting to cross the U.S. border as Mexicans or other South American residents. The Venezuelan government issued thousands, likely more, “cedulas” which are that country’s version of Social Security cards to people from anti-American and terrorist-supporting / sympathizing countries such as Cuba, Columbia, Iran and other Middle Eastern countries (McCaul, 2006).



Money from drug cartels in Mexico even made its way into the U.S. where it was laundered through Wachovia banks. Money laundered through Wachovia banks paid for an unknown number of airplanes used for smuggling and traffic activities, which span the globe. Among planes bought by this laundered money, was the DC-9 seized in Guinea Bissau, where the pilot, Carmelo Vasquez Guerra, escaped and was later taken into custody in Mexico, only to be released in less than two years (Smith, 2010; Evil Grin, 2010). During their hearings, Wachovia officials admitted that the amount of money was so great that it was too difficult to pass up despite U.S. banking laws (Webster, 2010; Hudson, 2003; Nelson, 2010).

These cells of Lebanese groups near the border of the U.S. have plain-looking shops, warehouses, and other buildings where tunnels are concealed, similar to those constructed in the region between Lebanon and Israel. News articles dating back to even early 2002 reveal tunnels like this found on the U.S.-Mexican border. Some of the tunnels found are almost a mile long, many have ventilation, air conditioning, drainage systems, and railways with

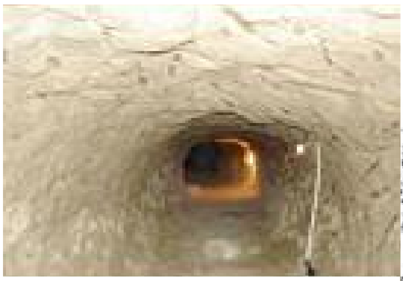


Photo retrieved from: http://www.usnews.com/usnews/news/badguys/070108/elmo_puppy_dogs_and_other_drug.htm on 24 Sept. 2010

Photo retrieved from: http://www.signonsandiego.com/news/2010/nov/03/drug-tunnel-discovered-marijuana/
Inside of the warehouse in Otay Mesa is the tunnel entrance hidden in a filing cabinet.

rail cars to transport people, weapons, and drugs underground into and out of the U.S. One tunnel that was most recently discovered stretched from Tijuana, Mexico to the Otay Mesa industrial area of San Diego, and had some 30 tons of marijuana in it (Dibble, 2010). Similar tunnels were discovered on the U.S./ Canadian border, revealing the possibility that weapons, humans and a variety of paraphernalia are being smuggled through Canada into the US. Montreal, Canada has one of the largest Lebanese communities in that country. In 2009, a Canadian government representative announced availability of direct flights from Montreal to Beirut, Lebanon; this was made possible to cater to Montreal's largely Lebanese population (The Lebanese Inner Circle, 2009). A tunnel found in 2007 at the U.S./Mexico border, was dramatically engineered and 80 feet below ground level. An associate of Mahmoud Youssef Kourani, a Hezbollah arrested in the U.S. for material support of the group, smuggled some 20 to 30 Hezbollah members across the Canada/ U.S. border in recent years. Officials are working with border patrol and the military to fill these tunnels with concrete. The estimate given to fill the 2007 tunnel was 3 days and $2.7 million (in taxpayer's money); so not only do these tunnels provide an entry to the U.S. but they also aid the crippling of the U.S. economy by necessitating the job of filling them in. In the past four years, at least 75 tunnels have been discovered that penetrate our border with Mexico. More than 125 have been found since the early 1990s when border officials began counting (Associated Press, 2005; Terrorist Planet, 2010; Carter, 2009; Dibble, 2010).

A little more than a year ago, Canadian intelligence identified Hezbollah "sleeper cells" in Canada. They reportedly did surveillance of intended Israeli targets in Canada such as synagogues. These individuals made another ominous move; they sent their established families living in Canada, back to Lebanon, possibly a move to prevent information about their proposed operations from being revealed, to prevent family members from being indicted as accessories to crimes they were planning, or simply protection since they were likely planning a big enough operation that backlash would become a problem for these family members (Carter, 2009).

Little known Lebanese communities across Mexico make up a population of 439,000 or more according to the Joshua Project. Mexican census reports appear to be incorrect and due to the corruption and violent conflict between government, military, and the drug cartel groups, it is difficult for an accurate census to be taken in traditional ways. Although many of these Lebanese consider themselves Christian or Catholic, they have a tendency to sympathize with Hezbollah as do those living in Lebanon due to the infrastructure that Hezbollah maintains to keep them cooperative. Those cells of Lebanese that are indeed supporting Hezbollah would be expected to report being Christian or Catholic in order to avoid the attention that would come from being classified as Islamic. In addition, there are a variety of Muslim centers in Mexico that can cater to Hezbollah sympathizers. Searching through www.islamicfinder.com using the names of cities in Mexico reveals at least 27 Islamic Centers and Masjids across Mexico, which would provide sanctuary to Hezbollah members. The most notable Islamic Centers are: Muslim Center de Mexico (MCM), in Mexico City; smaller Islamic centers inspired by the MCM are in Torreon, Coahuila, Guadalajara, Jalisco, and San Cristobal de las Casa, Chiapas, and up to 20 major cities in Mexico. It is difficult to understand why there would be so many Islamic Centers and worshiping locations in a country where the reported number of people worshiping this religion is merely

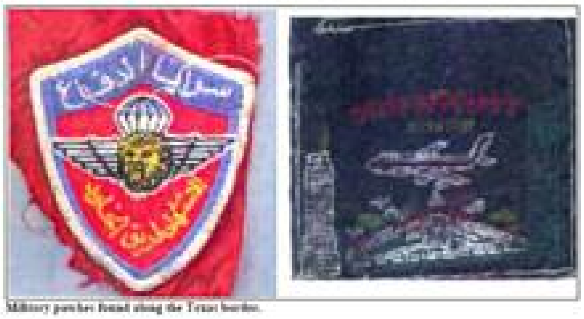
2000 as a report published in the year 2000 had noted.

The Muslim Center de Mexico said in their article on Islam in Mexico, that they are interested in appealing to the numerous indigenous groups in Mexico for conversion to Islam. It was noted that these indigenous people appear to be receptive to the teachings of Islam. They are reaching these people and appealing to them by holding periodic dinners where they invite the people from surrounding villages to eat meals (likely without charge) while they talk about and glorify Islam to the attendees (Muslim Center de Mexico, no date).

A man arrested in December 2002, Salim Boughader Mucharafille, admitted to smuggling more than 200 Lebanese aliens into the U.S. during the three years leading up to his arrest. He kept a notebook of the information about each person he smuggled in the café he ran which doubled as a cover for his smuggling operations. In his mind, he was helping "Brother Lebanese" people, even though he admitted to knowing many of them were part of the group, Hezbollah. Mucharafille told of smuggling these people in a variety of ways, including in the trunk of his car, by leading a team of illegals on 4-hour treks with a lead man to keep look out and a trailing man to sweep away their footprints (Associated Press, 2005; Terrorist Planet, 2010).

Another disturbing note is that a group belonging to Hezbollah smuggled cigarettes across border into Michigan where there is a large Muslim community (more than 300,000). These cigarettes were sold on the black market and in addition to swindling the Michigan government of more than $40 million in tax revenue over the period of the operation, and robbing the economy of more than $750 million in sales, which could have been made by legitimate businesses. It funded terrorism as the Hezbollah members running the operation sent the money (laundered) to Lebanon to fund the terrorist activities of the group which involve a complex mesh of: diamond smuggling through West Africa; cocaine smuggling from Latin America, particularly Venezuela, to Guinea Bissau, en route to Europe; Money laundering through S. America and W. Africa to Hezbollah-affiliated banks in Lebanon; Weapons acquisitions via Iran from Russia – which were shipped to S. America to use in training of Mexican drug cartels, and cartel violence, traded for drugs with the intention to sell these drugs to Americans as another means of "killing infidels", and sold in the Tri-border region between Argentina, Paraguay, and Brazil to send funds back to Lebanon for Hezbollah funding. An important consideration about the Hezbollah operations that are funded by this money obtained through the mentioned means is that Hezbollah operations include killing 241 U.S. Marines in the bombing of their barracks in Beirut in 1983, attacks on U.S. Embassy

Photo retrieved from: http://lapolaka.com/2010/07/23/terroristas-de-hizbulla-en-carrobomba-de-juarez/ on 24 Sept. 2010



Military patches found along the Texas border.

Photo retrieved 5 Oct. 2010 from http://www.freerepublic.com/focus/f-news/2572787/posts

buildings, and attacks on U.S. allies that continue today. Before 9-11-2001, Hezbollah was responsible for more American deaths than any other terrorist group (Associated Press, 2005; Mexican Train, 2009; Nelson, 2010; Barrett, 2010; Benhorin, 2006; Hays, 2007; Associated Press, 2005; Webster, 2010).

Ties between Hugo Chavez in Venezuela and Mahmoud Ahmadinejad in Iran have created an area in South America where allies of Iran can easily enter into the western hemisphere. In 2007, a new route to enter appeared as the Iran Air 744, a huge airbus that travels from Tehran, Iran to Caracus, Venezuela, making stops in Damascus and in Beirut. This allows any of Iran's allies including the IRGC and Hezbollah to fly comfortably into South America, often without a Visa, where they can conduct trafficking operations into the U.S. through the porous Mexico/ U.S. border. One must have connections and know the right people and what to say to get a ticket on this flight. The flights will appear to be booked solid until the passenger calls and speaks to certain personnel, and then they may get the ticket. Numerous YouTube.com videos of the Iran Air 744 flights show dozens of empty seats (Homeland Security News, 2010).

In the last 4 or 5 years, reports of Mexican drug cartel actions and operations have morphed ominously into those resembling terrorist operations seen in Iraq, Iran, Afghanistan, and attacks against Israel. Before about 2006, things like beheadings, car bombs, and IEDs were not reported in Mexico. Hezbollah is notorious for using civilians as human shields and is now teaching the Mexican drug cartels to also use this tactic making civilian life in border towns much more dangerous. Now, what is reported as drug cartel violence appears as shoot-outs using AK-47 rifles, car bombs, and more recently, IEDs. Anonymous Mexican military officials are making disturbing reports to small newspaper outlets and an assortment of blogs; members of the drug cartels who are disturbed with acts they are told to participate in; by U.S. Border Patrol employees; and others involved in the drug wars at the border. These reports include: the "Other Than Mexican" illegals captured at the border often do not run and cooperate with officials because they have heard through smuggling channels that the U.S. only deports Mexican citizens and those from other countries are released into the U.S. on the good faith that they will appear for a court hearing; recruitment for the cartels is taking place in public using banners as well as on Craig's List and other avenues using the internet; there are military-style training camps on and near the U.S. Mexico border utilizing instructors from Afghanistan and other Middle Eastern countries who teach the fighting skills used against U.S. troops oversea by these groups. Evidence of the Hezbollah presence near the U.S./ Mexico border such as prayer rugs and anti-American cloth patches have been found by land owners and border patrol. There are Mexican officials who admitted to knowing about such special training camps in Tamaulipas and in Michoacán where they say new "Zetas" members are intensively trained for at least 6 weeks in the skills of weapons, tactics

Retrieved 24 Sept. 2010 from http://www.bloomberg.com/news/2010-07-07/wachovia-s-drug-habit.html

and intelligence (La Polaka, 2010; Mexican Train, 2009).

It has been known, since at least 2001, that Hezbollah and other Islamic Terrorist Organizations were entering Mexico. Adolfo Aguilar Zinser, the former Mexican national security advisor noted that Islamic terrorist groups as well as those from Spain were using Mexico as a refuge. In 2002, a National Migration Institute official, Felipe Urbiola Ledezma said he knew about people being in Mexico who were linked to terrorism and that his organization was constantly observing unusual immigration flows, noting those with connections to ETA, Hezbollah, and Usama Bin Laden. He finished his statement noting that there were six or seven known organizations, but that the connected people living in Mexico were not involved directly with any terrorist activities (Curtis & Miro, 2003).

Hamas is another Islamic militant group, which was recently found collaborating with Hezbollah. Hezbollah was found funding Hamas through several covert means, including bank transfers, and couriers. Hezbollah has also offered their training camps to Hamas in Iran and Southern Lebanon (Anti-Defamation League, 2010; McCaul, 2006).

Photo retrieved from: http://www.globalnewscast.com/ on 24 Sept. 2010

There are reports that Hezbollah members have worked to create their presence in the U.S. using Mexico as their entry point for several reasons. First, they are taking advantage of the money to be made trafficking weapons, drugs, and humans. They are laundering money through a variety of ways through the two countries into interim countries before the money reaches Hezbollah owned banks in Lebanon. They are setting up Hezbollah fighters who are instructed to wait quietly and inconspicuously in case the leader of Iran says the words to attack if he is compromised on his nuclear weapons program or other agendas. Adel Assadinia, Iran's Consul General in Dubai from 2000 and 2003, confirms this operation for setting up sleeper cells of militants in Western Countries. He continues to say that these cells are operating in Nigeria as well as several other West African countries where they recruit Africans to form Islamic radical groups and participate in laundering money and trafficking operations. Assadinia says that if Iran's nuclear progress is tampered with by the West; suicide bomber attacks in the West will dwarf the tragedy of 9-11(Gertz, 2010; Brett, 2009; McCaul, 2006).

In addition to the aid Hezbollah is receiving from the drug gangs, they are getting help from random individuals who are able to be bought for a sum of money. Recently, a worker in Washington State, Melanie Yoder, was arrested for selling driver's licenses to a Rodrigo Moura for $500, which he then sold to some illegal immigrants claiming to be from a country in the Tri-borders region for $3000. Anonymous former border patrol officers told small news agencies about illegal immigrants from Iraq and other Middle Eastern countries paying as much as $25,000 to guides or others who were adept at human trafficking across the U.S./Mexican border (Farmer, 2009). Fourteen people on a single bus headed for Mexico were arrested after X-rays of their bags showed what turned out to be packages of money. All of the individuals were approached by people who promised to pay large sums of money for carrying these suitcases across the borders (Schiller, 2010). This sort of trafficking method has been used in recent years, in some countries in Africa, particularly Uganda, where the prospective "mule" is found in bars or tourist areas and profiled for characteristics such as lack of wealth and being adventurous. These mules are then paid money as well as extravagant living conditions and travel expenses for smuggling bags of cocaine across borders.

There are specific drug smuggling routes through Texas and other southeastern states where the Mexican cartels have relationships with trucking companies and others who aid in their distribution of drugs (and possibly humans, including those OTM aliens from special interest countries). The trafficking of humans pays handsomely and carries less risk if caught by officials than drug smuggling. NATO has helped these practices somewhat by allowing Mexican trucks to cross the border and drive 20 miles before being required to unload and use American trucking or other transport means. Only about one in five trucks gets a thorough inspection at the border and it seems that the cartels and those people acting as “coyotes” to smuggle aliens into the country are aware of this fact and are willing to take the risk (McCaul, 2006).

Mexican cartels, Mexican Mafia, and gangs operating in the U.S. have been reportedly working together in their efforts to sell drugs for profit in the U.S. One group of note is Mara Salvatrucha (also known as MS-13) which conducts cross-border drug smuggling operations, and is known by U.S. law enforcement officials for their record of violent crime including robbery, assault, rape, and murder. Having these gangs working with those in Mexico, who are being trained by Hezbollah, is ominous and may result in these gangs accepting the same training and alliances with Hezbollah, making safety in the U.S. mirror that of Mexico in the coming years if not corrected now. There is already evidence of some U.S. gangs collaborating with the Mexican gangs particularly in border towns, and DEA officials who told journalists about their knowledge of this wanted to remain anonymous for unknown reasons. An entire 3500 acres of Arizona desert, which had been open to the public, has been closed due to the cartel and gang violence as well as kidnapping. Americans have recently been reported as kidnapped and then shot execution-style by cartels (Webster, 2010; McCaul, 2006).

In addition to the violence and brutal killings, cartels are attempting recruiting efforts by both opening drug treatment centers, and by placing members in established centers where they can tell patients of the centers a number of benefits to becoming part of the cartel. Some centers are simply small homes of former addicts who are trying to help others with addictions while making some money. These centers are unlicensed and more difficult to track by officials but are somehow discovered easily by cartel members. They tell prospective recruits about an endless supply of money, not having to struggle to support their families, and other schemes to make joining sound attractive. If glorifying the cartel life is not successful, they may threaten those persons with death. Shootings at these clinics over the last year have killed hundreds of people. Cartels say killings are to scare others into joining, and also punishment for those not paying drug dealers (Associated Press, 2010).

The drug cartels in Mexico also have been tapping into the oil pipelines using heavy duty drilling equipment and specialized taps with valves to eliminate detection for pressure differences, to collect the oil. Pemex representatives said these cartels have stolen over 8,000 gallons each day in 2009. In addition to the theft, when they have filled their tankers and leave, they allow the oil to spill out on the ground, creating an environmental hazard. Farmers with land close to these illegal taps have complained that the oil soaked into the ground water and their wells used for irrigation are contaminated with oil and the smell of hot tar from the spills are unnerving. The cartels sell the oil for profit and have even sold this stolen oil to several US companies, five of which were charged and plead guilty to buying the stolen oil. Many cartels have acquired gas stations and can use these for laundering money as well as for selling gas they get from trading and selling the stolen oil (Jacksonville Observer, 2010). These exact tactics have been used in Nigeria on the oil pipelines by thieves who tap the pipes and sell to tanker ships waiting offshore. There are groups modeling themselves after Hezbollah in Nigeria and there are Hezbollah cells conducting smuggling, trafficking, and money laundering operations through this and other West African countries (Brett, 2009; Mbachu, 2010; Vernaschi, 2010).

In addition to the threat of Hezbollah militants operating in Mexico, there are members of the Iranian Revolutionary Guard Corp (often called Pasdaran), utilizing allied connections with Venezuela and Paraguay to enter South America where they then move through Mexico to get into the United States. In 2004, U.S. intelligence sources said a group of 25 Chechen rebels crossed the U.S. border with backpacks. Chechen Rebels, an Islamic militant group from Russia, have conducted numerous tragic and bloody attacks in Russia over the years. A particularly memorable attack is that which was carried out on an elementary school on the first day of classes in Beslan, 2004. Russian mafia groups, including Poldolskaya, Mazukinskaya, Tambovskaya, and Izamailovskaya have been reported to be operating in Mexico along with a Moscow-based gang and mafia-gangs from Chechnya, Georgia, Armenia, Lithuania, Poland, Croatia, Serbia, Hungary, Albania, and Romania. The same source notes the presence of al Qaeda and Hamas members in the groups who did gain access to the U.S. through this southern border (The Washington Times, 2004; Webster, 2008).

Crimes committed on the U.S. side of the border may not be reported through federal channels and may not be categorized as terrorist activity. The Los Angeles Police Department noted in December, 2006 that foreign terror activities to include funding, trafficking of a variety of goods and money, along with other crimes often get 'lost' in local law enforcement records and may not be found by those searching for data on terrorism through the federal channels (Los Angeles Police Department, 2006).

Several important Hezbollah arrests have been made in recent years. These include:

Jameel Nasr, a Hezbollah leader, living in Tijuana, Mexico until his arrest who frequently traveled back and forth to Lebanon and Venezuela to communicate with other leaders of Hezbollah.

Jamal Yousef (Talal Hassan Ghantou), former member of the Syrian military, who negotiated weapons trafficking deals with supposed FARC members who were actually DEA members. He wanted to bargain weapons for cocaine and told his potential customers that he thought drugs were another good way to kill Americans.

Mahmoud Youssef Kourani, Hezbollah fighter who gained entry into the U.S. in 2001 after bribing the Mexican consul in Lebanon. He maintained a clean-shaven appearance while living in Michigan and did not attend mosques to avoid suspicion but was arrested in 2003 for charges about his raising money to support Hezbollah. Kourani admitted to bribing a Mexican consular official in Beirut for a Visa to access Mexico, and then paid coyotes to get him and his partners into the U.s> via our porous Southern border.

Karim Hassan Nasser, a naturalized U.S. citizen; along with Theodore Schenk (from Miami Beach, FL), Imad Hamadeh, Elias Mohamad Akhdar, and Hassan M.Makki (all from Dearborn Heights, MI) were arrested and pled guilty, to racketeering and other charges associated with the Dearborn, MI bust which involved trafficking of cigarettes, Viagra, cigarette papers, and unlikely items like baby formula and toilet paper.

Ali Boumelhem (Dearborn, MI) was convicted of attempting to send weapons and ammunition to Hezbollah in 2002.

Salim Boughader Mucharrafille was arrested in 2002 for smuggling more than 200 people, including Hezbollah supporters, across the U.S. border. He used his Lebanese café for a base and displayed the Lebanese flag as a beacon to alert his 'customers'.

Mohamad Hammoud and his brother Chawki Hammoud were convicted for material support in 2002 when they were found procuring numerous items including laser range finders, GPS devices and others as well as smuggling cigarettes and sending money to Hezbollah.

Statement of risk: There are many layers of risk involved in this threat to our national security. The obvious risk is in allowing Hezbollah members and members of other terrorist groups and terrorist sympathizers into the U.S. where they will conduct criminal and terrorist operations.

There is the risk of allowing these groups to fund their home bases in other countries that conduct attacks against our troops, and the troops and civilians of our allies.

Risks of deadly attacks by Mexican drug cartels are increasing due to the training in formal military tactics of the groups by hardened terrorists. These attacks target civilians, government officials, and especially any journalists who attempt to report on the incidents.

Spillover into our border towns will become increasingly violent and may begin to include car bombings, beheadings, and shoot-outs involving automatic weapons. Recent news from Arizona reported the discovery of a beheaded man in an Arizona apartment. The victim and suspected murders were all illegal immigrants (Associated Press, 2010).

There are additional risks that follow the introduction of the drugs imported to be sold on U.S. streets. U.S. gangs getting involved with the Mexican gangs and copying their terror-tactics in the U.S is possible. There is also the obvious problem associated with the increase in crime and violence that accompanies drug addiction, drug dealing and drug dependency.

The tunnels built by these groups will be used to smuggle humans and paraphernalia under the border with the cover of private homes or businesses on either side, making them difficult to discover. These tunnels have also proven to be an economic problem because they cost millions of dollars in taxpayer's money to fill, only to have new ones built soon after.

Actions recommended: This is a dire situation, which needs attention now, or rather, yesterday. U.S. officials have reported this problem in part, since over a decade ago. There are at least ten distinguished officials belonging to the DEA, FBI, Homeland Security, U.S. Military, Mexican Military, Mexican political figures and more who remain anonymous who have said that they knew Hezbollah was operating below our southern border, that they knew money laundering and weapons, drug and human trafficking was taking place across our borders, and that they discovered elaborate tunnels with signature clues of Hezbollah in them as well as the new tactics and munitions used by drug cartels over the past several years. So why have we not acted on these warnings even now?

Border Patrol for both the U.S. and Mexico must work together to identify important clues which reveal Hezbollah presence. These clues include, but are in no way limited to:

Identify rifles and other weapons used traditionally by Hezbollah in the Middle East countries. Due to the weapons trafficking to put these weapons in the hands of new “allies”, the Mexican drug cartels, weapons used by Hezbollah in Lebanon which are often supplied by their other ally, Iran, are appearing at shoot-outs and being found in bust-operations by Mexican Military. Some of the weapons will no doubt have the serial numbers ground off, but the style, make, and origin of the weapons can still be estimated by weapon characteristics. (See photos 1, 2 below) Still more weapons have been found during investigations and indictments of known Hezbollah members that were stolen from Iraq. Weapons found in Mexico should be compared to this model of a weapons cache for identification. The brass and any live ammunition found can also be analyzed for origin and compared with that ammunition traditionally found in the Middle East in skirmishes with Hezbollah.

Track the Iran Air 744 flights and see if suspected or known operations coincide with the flight patterns. Iran Air 744 could easily be smuggling weapons, drugs, ammunition, militants, money, and other things necessary to carry out their operations in South America and North America. It could also be carrying back supplies to aid in Iran's nuclear development without any prying eyes from the U.S. or U.S. allies.

Illegal immigrants that are found to be “Other Than Mexican” should not be released into the U.S. on the good faith that they will appear at a court hearing.

Border Patrol, Mexican police, police agencies from U.S. border towns, FBI, and any other organizations involved in the drug war and national security on this border should be looking for Islamic influence in the people they catch on the border. Things like tattoos in Farsi, patches or other clothing or articles displaying a cedar tree (symbol of Lebanon), poor Spanish abilities, speaking languages other than Spanish when claiming to be from Mexico, especially if holding a (likely falsified) Venezuelan passport of other identification.

All raids conducted near the border on houses or any other structures should include thorough searching for tunnels.

Observations of how these anti-American and terrorist groups operate in other countries should serve as templates for profiling here in the U.S. and in Mexico for purposes of intelligence gathering and border protection.

Be watchful for so-called "charity" groups that send money and freight or other packages routinely to Islamic countries that support terrorism.

Weapons confiscated by Israeli military troops, (retrieved 24 Sept. 2010)

Weapons confiscated by Israeli military troops, (retrieved 24 Sept. 2010)
Weapons confiscated in Mexico, (Photograph by ATF, retrieved 24 Sept. 2010)

Tattoo shops should be visited and artists questioned about requests for tattoos in Farsi.

Drug rehabilitation clinics, occupational rehabilitation, and physical rehabilitation clinic staff should be instructed on recognizing signs of drug cartel members and prevent them from infiltrating the practice for purposes of gaining recruits. Rehab centers that are run by such cartel members can be located by conducting routine surveillance.

Social networking sites on the internet should be scoured for names of known terrorist group members. Surprisingly, some of those mentioned in this report have pages on Facebook.com.

Prisons in border areas should be watchful for persons who appear of Middle Eastern decent that claim to be Mexican and take note of behaviors like Islamic prayer traditions, speaking languages other than Spanish, and tattoos in Arabic languages or Farsi.

Bibliography

- Anti-Defamation League. (2010, June 9). Hezbollah. In *Terrorism*. Retrieved 6 October, 2010, from http://www.adl.org/NR/exeres/B90EABC8-DA1E-4F81-A4BE-713D3C205DF3,DB7611A2-02CD-43AF-8147-649E26813571,frameless.htm

Weapons confiscated in Mexico, (Photograph by ATF, retrieved 24 Sept. 2010)

- Associated Press. (2005, June 15). *Charging Hizbullah*. Retrieved 18 September, 2010, from http://www.ynetnews.com/articles/0,7340,L-3099235,00.html
- Associated Press. (2005, July 3). *Terror-linked migrants channeled into U.S.* [Tijuana, Mexico]. Retrieved 22 September, 2010, from http://www.foxnews.com/printer_friendly_story/0,3566,16,473,00.html
- Associated Press. (2010, October 29). Arizona beheading raises fears of drug violence. In *Crime & Courts*. Retrieved 29 October, 2010, from Fox News: http://www.foxnews.com/us/2010/10/29/arizona-beheading-raises-fears-drug-violence/
- Associated Press. (2010, February 4). *Drug cartels co-opt rehab for recruits in Mexico*. Retrieved 24 September, 2010, from

http://www.mysanantonio.com/news/Drug_cartels_co-opt_rehab_for_recruits.html

- Barrett, B. (2010, September 9). *Myrick wants task force to study Hezbollah ties on border*. Retrieved 16 September, 2010, from http://www.charlotteobserver.com/2010/09/09/1677268/myrick-wants-task-force-to-study.html
- Benhorin, Y. (2006, April 1). *U.S.: Hizbullah selling fake Viagra*. Retrieved 18 September, 2010, from http://www.ynetnews.com/articles/0,7340,L-3234805,00.html
- Brett, D. (2009, January 25). *Profile of an African hezbollah*. Retrieved 1 October, 2010, from http://www.mesi.org.uk/ViewBlog.aspx?ArticleId=49
- Carter, C. (2009, September 30). *Hezbollah prepared to hold the U.S. hostage*. Retrieved 22 September, 2009, from http://www.familysecuritymatters.org/publications/id.4401/pub_detail.asp
- Ceren, O. (2007, November 2). Former CIA head: Hamas and Hezbollah cells active in Mexico, exploiting open border to get into the US. In *Mere rhetoric*. Retrieved 18 September, 2010, from http://www.mererhetoric.com/2007/11/02/former-cia-head-hamas-and-hezbollah-cells-active-in-mexico-exploiting-open-border-to-get-into-the-us/
- Conery, B. (2009, March 27). *Exclusive: Hezbollah uses Mexican drug routes into U.S.* Retrieved 15 September, 2010, from http://www.washingtontimes.com/news/2009/mar/27/hezbollah-uses-mexican-drug-routes-into-us/
- Curtis, G. E., & Miro, R. J. (Project manager; researcher). (2003, February 23). *Organized crime and terrorist activity in Mexico, 1999-2002* (Federal Research Division, Library of Congress).
- Defense Tech. (2006, July 19). *Hezbollah's surprise weapons*. Retrieved 18 September, 2010, from http://defensetech.org/2006/07/19/hezbollahs-surprise-weapons/
- Dibble, S. (2010, November 3). Drug smugglers' tunnel linked Tijuana, San Diego. In *Border and immigration*. Retrieved 3 November, 2010, from http://www.signonsandiego.com/news/2010/nov/03/drug-tunnel-discovered-marijuana/
- Ensinger, D. (2010, November 10). *NAFTA fueling drug trade*. Retrieved 10 November, 2010, from Economy in Crisis: http://economyincrisis.net/content/nafta-fueling-drug-trade
- Evil Grin. (2010, July 19). *Pilot in DC9 5.5 ton cocaine bust «escaped» custody in three separate countries*. Retrieved 5 October, 2010, from http://qwstnevrythg.com/2010/07/pilot-in-dc9-5-5-ton-cocaine/
- Farmer, J., & Gambill, T. (Reporter; Posted by). (2010, May 12). *TERRORISTs crossing Mexican-U.S. border*. Retrieved from http://www.nwofighters.org/terrorists-crossing-mexican-u-s-border/
- Ferriss, S. (2002, August 12). *Spanish Muslim mission grows in Mexico*. Retrieved 19 September, 2010, from http://www.islamawareness.net/LatinAmerica/mexico2.html
- Gaffney, F. (2010, July 9). *Hezbollah in Mexico: Two inconvenient men*. Retrieved 15 September, 2010, from http://www.maricopagop.org/2010/07/09/hezbollah-in-mexico-two-inconvenient-men/
- Galland, J. D. *News border patrol Mexico*. Retrieved 18 September, 2010, from http://www.warriorsfortruth.com/news-border-patrol-mexico.html
- Gato, P., & Windrem, R. (2007, May 9). *Hezbollah builds a western base* [Video of Hezbollah member]. Retrieved 19 September, 2010, from http://www.msnbc.msn.com/id/17874369/
- Gertz, B. (2010, June 10). *Hizbullah building terror infrastructure in U.S., infiltrating from Mexico*. Retrieved 23 September, 2010, from http://www.worldtribune.com/worldtribune/WTARC/2010/ss_terror0516_06_11.asp
- Gilman, N. (2009, July 17). *The Lebanese connection: Middle Eastern cuisine in Mexico City*. Retrieved 19 Sep-

tember, 2010, from http://goodfoodmexicocity.blogspot.com/2009/07/lebanese-connection-middle-eastern.html

- Haaretz Service. (2009, March 9). *Report: Chemical weapons in Hezbollah arms cache blast*. Retrieved 17 September, 2010, from http://www.haaretz.com/news/report-chemical-weapons-in-hezbollah-arms-cache-blast-1.8552
- Halili, Y. (2007, May 10). *Hizbullah training for attacks on US - telemundo*. Retrieved 18 September, 2010, from http://www.ynetnews.com/articles/0,7340,L-3398088,00.html
- Homeland Security News. (2010, September 23). Feds arrest Arizona buyers of guns for drug cartels. In *Mexico: descent into chaos*. Retrieved 23 September, 2010, from http://homelandsecuritynewswire.com/feds-arrest-arizona-buyers-guns-drug-cartels
- Homeland Security News. (2010, July 11). *Hezbollah terrorists plotting on the U.S. border*. Retrieved 15 September, 2010, from http://www.nationalterroralert.com/updates/tag/hezbollah-mexico/
- Homeland Security News. (2010, August 19). *Iran gearing up for a post-attack retaliatory campaign in western hemisphere*. Retrieved 1 October, 2010, from http://homelandsecuritynewswire.com/iran-gearing-post-attack-retaliatory-campaign-western-hemisphere
- Homeland Security News. (2010, September 13). *U.S.: Mexico's drug war posing growing threat to U.S. national security* [Mexico: descent into chaos]. Retrieved 18 September, 2010, from http://homelandsecuritynewswire.com/us-mexicos-drug-war-posing-growing-threat-us-national-security
- Hudson, R. (2003, July 11). *TERRORIST and organized crime groups in the tri-border area (TBA) of South America* [A report prepared by the Federal Research Division, Library of Congress under an Interagency Agreement with the United States Government]. Retrieved 20 September, 2010, from http://www.loc.gov/rr/frd/pdf-files/TerrOrgCrime_TBA.pdf
- Islamic Finder. (2010, September 19). *Mexico prayer times*. Retrieved 19 September, 2010, from http://www.islamicfinder.org/cityPrayerNew.php?country=mexico
- Jacksonville Observer (Guest Columnist). (2010, June 7). *Cartels tap into Mexico's oil lines*. Retrieved 1 October, 2010, from http://www.jaxobserver.com/2010/06/07/cartels-tap-into-mexicos-oil-lines/
- Johnson, T. (2010, April 1). Why are beheadings so popular with Mexico's drug gangs? In *McLatchy newspapers*. Retrieved 18 September, 2010, from http://www.mcclatchydc.com/2010/04/01/91481/beheadings-become-signature-of.html
- Joshua Project. (2010, July 26). *Mexico*. Retrieved September 19, 2010, from http://www.joshuaproject.net/countries.php?rog3=MX
- Korte, T. (2010, September 20). *NM physicist, alleged spy sent to halfway house* [Tried to give nuclear weapon info to under cover FBI agent posing as Venezuelan rep.]. Retrieved 23 September, 2010, from http://www.washingtonpost.com/wp-dyn/content/article/2010/09/20/AR2010092003752.html
- Kouri, J. (2010, November 13). *Al Shabaab: Several men charged in terrorism conspiracy*. Retrieved 13 November, 2010, from Examiner: http://www.examiner.com/law-enforcement-in-national/al-shabaab-several-men-charged-terrorism-conspiracy
- La Polaka. (2010, July 19). *The general irresponsibility R. Zarate Ruiz*. Retrieved 17 September, 2010, from http://lapolaka.com/?s=r.+zarate+ruiz
- La Polaka. (2010, July 23). *TERRORISTAS DE HEZBOLLÁH EN CARROBOMBA DE JUÁREZ <http://lapolaka.com/2010/07/23/terroristas-de-hizbulla-en-carrobomba-de-juarez/>*. Retrieved 17 September, 2010, from http://lapolaka.com/2010/07/23/terroristas-de-hizbulla-en-carrobomba-de-juarez/

- Lalani, R., & Lalani, R. (2008, May 29). *Tehran to North Vancouver*. Retrieved 28 September, 2010, from http://www.canadianimmigrant.ca/ArticlePrint/493
- Latin American Herald Tribune. (2010, November 10). *Cuba and Venezuela strengthen ties*. Retrieved 10 November, 2010, from Latin American Herald Tribune: http://www.laht.com/article.asp?ArticleId=376532&CategoryId=10718
- Long, C. (2010, November 13). *Gunmen in Mexico's drug war getting younger*. Retrieved 14 November, 2010, from http://www.metronews.ca/ottawa/world/article/690653—mexico-prison-population-surges-amid-drug-war—page0
- Los Angeles Police Department. (2006, December 29). *An L.A. police bust*. Retrieved 12 November, 2010, from L.A.P.D.: http://lapdblog.typepad.com/lapd_blog/2006/12/an_la_police_bu.html
- Luna, D. M. (2008, October 8). *Narcotrafficking: What is the nexus with the war on terror?* Retrieved 15 September, 2010, from http://merln.ndu.edu/archivepdf/terrorism/state/110828.pdf
- MacDonald, B. (2010, September 9). *America: Terrorists on the doorstep*. Retrieved 15 September, 2010, from http://www.thetrumpet.com/?q=7466.6044.0.0
- Mbachu, D. (2010, August 30). *Shell says $1.1 billion Nigerian crude-oil pipeline is nearing completion*. Retrieved 1 October, 2010, from http://www.bloomberg.com/news/2010-08-30/shell-says-it-s-close-to-completing-1-1-billion-crude-oil-line-in-nigeria.html
- McCaul, M. (Chairman). (2006, October 18). *A line in the sand: Confronting the threat at the southwest border* (Majority Staff of the House Committee on Homeland Security Subcommittee on Investigations).
- Merco Press. (2010, November 9). *Narco-violence and political repression threaten Latin American press*. Retrieved 10 November, 2010, from South Atlantic News Agency: http://en.mercopress.com/2010/11/09/narco-violence-and-political-repression-threaten-latin-american-press
- Mexican Train. (2009, December 8). *Mexican drug cartels and terrorist are recruiting for more fighters to train as soldiers*. Retrieved 22 September, 2010, from http://edumexico.org/mexican-drug-cartels-and-terrorist-are-recruiting-for-more-fighters-to-train-as-soldiers
- Miller, A. (2009, April 8). *Hezbollah agents flood into America*. Retrieved 17 September, 2010, from http://www.thetrumpet.com/print.php?q=6093.4481.0.0
- Muslim Center de Mexico. *Islam in Mexico a struggle to remain giving Dawa according to Quran and Sunnah*. Retrieved 9 November, 2010, from Al-Islaah Publications: http://maseeh1.tripod.com/advices7/id196.htm
- Nahmias, R. (2007, November 2). *Expert: Hamas, Hizbullah cells may be active in Mexico*. Retrieved 17 September, 2010, from http://www.ynetnews.com/articles/0,7340,L-3466854,00.html
- National Drug Intelligence Center. (2010). *National methamphetamine threat assessment*. Retrieved 26 September, 2010, from http://s3.amazonaws.com/nytdocs/docs/374/374.pdf
- Nelson, E. (2010, July 12). *Hezbollah terrorist operatives in Mexico*. Retrieved 16 September, 2010, from http://borderalert.usbc.org/open-borders/hezbollah-terrorist-operatives-in-mexico
- Nunez-Neto, B., Siskin, A., & Vina, S. (2005, September 22). *Border security: Apprehensions of «other than Mexican» aliens*. Retrieved 18 September, 2010, from http://trac.syr.edu/immigration/library/P1.pdf
- Rollins, J., & Wyler, L. S. (2010, March 18). *International terrorism and transnational crime: Security threats, U.S. Policy, and Considerations for congress*. Retrieved 15 September, 2010, from http://www.fas.org/sgp/crs/terror/R41004.pdf
- Russia Today. (2009, February 23). *Russian arms to win Arab markets*. Retrieved

20 September, 2010, from http://rt.com/Top_News/2009-02-23/Russian_arms_to_win_Arab_markets.html

- Schiller, D. (2010, September 29). *Arrests shed light on drug money pipeline into Mexico*. Retrieved 1 October, 2010, from http://www.chron.com/disp/story.mpl/metropolitan/7224333.html
- Scott, J. (2006, July 16). *Katusha & Qassam rockets*. Retrieved 17 September, 2010, from http://www.aerospaceweb.org/question/weapons/q0279.shtml
- Sherwell, P. (2009, March 27). *US marshall executed in lawless Mexican town of Juarez*. Retrieved 23 September, 2010, from http://www.telegraph.co.uk/news/worldnews/centralamericaandthecaribbean/mexico/5057965/US-marshall-executed-in-lawless-Mexican-town-of-Juarez.html
- Smith, M. (2010, July 7). *Wachovia's drug habit*. Retrieved 5 October, 2010, from http://www.bloomberg.com/news/2010-07-07/wachovia-s-drug-habit.html
- Terrorist Planet. (2010). *Mexican and Canadian drug tunnels*. Retrieved 22 September, 2010, from http://www.terroristplanet.com/2010/02/mexican-and-canadian-drug-tunnels
- The Lebanese Inner Circle. (2009, October 26). *YUL - BEY: Direct flights Beirut/Montreal*. Retrieved 24 September, 2010, from http://theinnercircle.wordpress.com/2009/10/26/yul-bey-direct-flights-beirut-montreal/
- The Washington Times. (2004, October 13). *Chechen terrorists probed*. Retrieved 1 October, 2010, from http://www.washingtontimes.com/news/2004/oct/13/20041013-121643-5028r/
- Thompson, J. (2010, August 1). The new world expansion of Hezbollah. In *Mackenzie briefing notes*. Retrieved 17 September, 2010, from http://www.mackenzieinstitute.com/2010/hezbollah081810.htm
- Thug Life DFW. (2010, July 17). Showing newest posts with label Mexican drug war. In *DFW Gangs*. Retrieved 23 September, 2010, from http://dfwgangs.blogspot.com/search/label/Mexican%20Drug%20War
- Tobacco News. (2010). *Articles:Listing Hezbollah*. Retrieved 22 September, 2010, from http://www.tobacco.org/articles/org/hezbollah/
- Tornabene, R. (2009, October 8). Mexican drug cartels series part 2-enforcer gangs. *Gateway Gazette, X ed.,* sec. 4, pp. 2-4.
- Vernaschi, M. (2010, Winter). The cocaine coast. *The Virginia Quarterly Review.* Retrieved 24 September, 2010, from http://www.vqronline.org/articles/2010/winter/vernaschi-cocaine-coast/
- Webster, M. (2008, April 16). *Mexican drug cartels and terrorists are recruiting for more fighters to train as soldiers*. Retrieved 15 September, 2010, from http://www.americanchronicle.com/articles/view/58757
- Webster, M. (2008, October 27). *Hezbollah operating in Mexico and U.S.* Retrieved 15 September, 2010, from http://atlanta10.cityspur.com/2009/12/07/hezbollah-operating-in-mexico-and-u-s/
- Webster, M. (2010, August 8). *Alarming sensitive U.S. Government Rdeport*. Retrieved 23 September, 2010, from http://edumexico.org/alarming-sensitive-u-s-government-rdeport/1794/
- Webster, M. (2010, August 29). *Big and Dangerous U.S. gangs making alliances in other states and countries*. Retrieved 21 September, 2010, from http://edumexico.org/big-and-dangerous-u-s-gangs-making-alliances-in-other-states-and-countries/1939/
- Webster, M. (2010, June 3). *Hezbollah and Maxica drug cartels operating in Mexico and U.S.* Retrieved 21 September, 2010, from http://docstalk.blogspot.com/2010/06/hezbollah-and-mexica-drug-cartels.html
- Webster, M. (2010, May 25). *Mexican drug cartel's cash is king!* Retrieved 24 September, 2010, from http://www.usborderfirereport.com/mexican_drug_cartel.htm
- Webster, M. (2010, August 11). *More El Paso gang members arrested for violent*

crimes. Retrieved 23 September, 2010, from http://edumexico.org/more-el-paso-gang-members-arrested-for-violent-crimes/1817/

- Webster, M. (2010, June 14). *The U.S. gov: Giving parts of Arizona back to Mexico*. Retrieved 23 September, 2010, from http://www.usborderfirereport.com/new_page_19.htm
- Wyler, L. S., & Cook, N. (2009, September 30). *Illegal Drug Trade in Africa: Trends and U.S. Policy*. Retrieved 15 September, 2010, from http://www.fas.org/sgp/crs/row/R40838.pdf
- Ynet. (2009, March 27). *Report: Hizbullah, Mexican drug cartels working together*. Retrieved 18 September, 2010, from http://www.ynetnews.com/articles/0,7340,L-3693129,00.html
- Zidane, Z. (2008, Summer). *So Far from Allah, So Close to Mexico: Middle Eastern Immigrants in Modern Mexico/Another Arabesque: Syrian-Lebanese Ethnicity in Neoliberal Brazil*. Retrieved 19 September, 2010, from Bnet: http://findarticles.com/p/articles/mi_qa4000/is_200807/ai_n27899404/?tag=content;col1

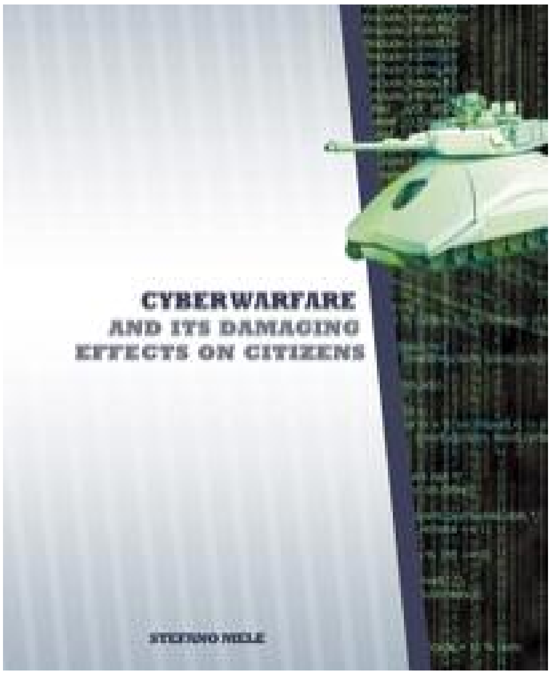
Cyberwarfare and its damaging effects on citizens

by Stefano Mele

Introduction

In order to analyze the real damage that a hypothetical *cyber-war* or individual act of *cyberwarfare* could do to the citizens of any nation coming under attack, it is fundamental to begin with some reflections which will help us reach a full understanding of the phenomenon, and its related practical implications.

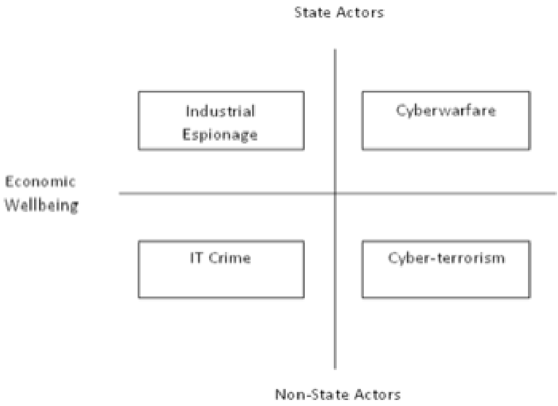
The first of these is surely linked to the difficulty faced in defining the difference (which in the realm of cyber-space can be very subtle) between common criminals committing IT crime and so-called '*cyber warriors*', by which I mean those individuals with a high level of technical skill who are paid by a State to commit acts of cyberwarfare. This is because, on a fundamental level, acts of cyberwarfare are often completely identical – technically speaking – to those acts which common criminals might commit over the internet: only the aims of these acts change (although sometimes even the targets are the same) along with those who conduct them, or order them to be carried out.



The classic quadri-partition of illegal acts within the realm of IT, as shown below, is therefore actually merely theoretical.

In addition, as is already known, it is not unusual for Governments to 'dip a toe' into the world of IT crime – organized or not – in order to carry out an individual cyberwarfare operation, or to reinforce their range of attacking options. This is especially true in cases in which the subject to be hired is capable not just of using those instruments or tools which can be found on the internet, but who is above all capable of creating such tools on an *ad hoc* basis for each specific act of penetration or manipulation of the target security system, and who is able to identify new bugs (the so-called 'zero day'[1] attacks) in the software used by Governments and individuals, so that defence systems do not already have the attack signatures of these bugs on their databases, thereby making such actions difficult to uncover.

Furthermore, we must consider that some types of illicit actions, although perhaps only those which are not considered by Governments to be too 'delicate', can be directly outsourced to specific private companies or criminal groups, which may also be foreign and without any geopolitical connections to events which could lead to cyber-war, and which would require, as an extra layer of security, the use of intermediaries both in initially obtaining the services of the company or the criminal group and in dealing with them, in such a way as to make more simple and immediate any public denial should an electronic attack come to be identified (a practice which is already common and widespread).



It follows on from these initial reflections, then, that beyond the commonly understood ease with which it is possible to remain completely anonymous in a conflict which, in its nature, is sometimes fought in a temporal arc of just tens of minutes, the problem of attributing responsibility for the attack does not just stem from the technical-structural elements of the web, and the material impossibility of putting a 'face' on its author, but also from the impossibility of pinpointing the precise geographical location of the attacker.

It is also useful to point out, even as a brief mention, that in the overwhelming majority of cases of penetration and, even more so, manipulation of critical electronic national security systems, these are carried out (and will always be carried out) under the utmost secrecy. Even if it was possible to do so, the target State would only be able to find out if the attacking operation or the manipulation of electronic systems was successful or not if a real cyber-war was to break out, or only at the moment in which an act of cyberwarfare was carried out, and, therefore, those cyberweapons which had been previously set up against an adversary would have to be used.

An additional mention in this analysis must be given to the consideration that the weakest link in electronic security systems has always been – and will be for a long time to come – man himself. And this is true both in terms of purely malicious, or intentional acts, and also in terms of unintentional failures.

In fact, as far any system can really be said to be 'fully protected' from external attack, it is certainly possible – if not highly likely – that disloyal employees may manipulate the network and its security systems from within, installing malware and/or modifying its security settings, thereby facilitating outside access. At its heart the history of espionage is full of traitors and double agents. It is not correct, therefore, to assume beforehand that such agents could not exist within the world of information security[2].

Different, but just as dangerous, is the purely random possibility that a lack of attention on the part of internal personnel, or an inadequate culture of security, or the fallacious assumption that a network, thought of as being inviolable from outside, can therefore be configured from within to be as useful and 'elastic' as possible, can lead to security systems being totally compromised. This, for example, occurred in 2008, when a file infected with malware originating from the non-secure network (NIPRNET) of the American Department of Defence was copied onto a USB pen-drive, and was then uploaded onto a computer connected to the secure network (SIPRNET). The file was opened, and the malicious software then spread uncontrollably, within hours infecting hundreds of terminals in Afghanistan, Iraq, Qatar, and, obviously, at American Central Command[3].

A recent study from the DHS[4], in fact, highlighted how the IT systems of US-CERT (*United States Computer Emergency Readiness Team*), which are used by the NCSD (*National Cyber Security Division*) in its mission to be the focal point in terms of cyber-security, both at the public and private level, suffer from numerous, and dangerous, vulnerabilities linked above all to the problem of a poor IT security culture amongst its employees. US-CERT, in fact, amongst other things, monitors the alert signals that 'Einstein', the intrusion detection system (IDS) which is tasked with monitoring the non-military networks of the US Government (the so-called '.gov' systems), sends out in the event of any unauthorized attempted intrusions. This IDS system is also set up to send out, over the entire network it is in control of, notifications concerning software updates to be installed on the various computers which make up its 'domain', so that all users of the internal network are immediately warned of any eventual problems with security (bugs) found on the system, and so that patches for these bugs can be swiftly installed. This method, however, has been shown to be completely ineffective. Leaving the task of updating his or her machine to the end user, in fact, meant that, after a scan was carried out using the *Nessus* vulnerability scanner, 1,085 instances of 202 bugs pegged as 'maximum risk' - which could easily have been exploited for malicious purposes - were reported.

Finally, space must be left for a few brief reflections on the genuine probability of the break-out of cyber-war.

Even on the sole basis of the arguments analyzed thus far, it is logical to deduce that cyber-war is much more likely, and perhaps more convenient, than is currently predicted. A cyber-war, in fact, would even allow smaller States, which are normally incapable of competing either militarily or economically with larger international powers, to attack the critical systems of other State targets thanks to its excellent 'cost-benefit' ratio. In fact, by exploiting technical skills and know-how which in 90% of cases are available for no cost directly on the internet, and by exploiting the actually poor level of defence capabilities seen on this 'battleground' in all those nations (above all America) which are excessively dependent on technological systems, it is possible to bring this war to any part of the world, at low cost, and with a very high probability of obtaining a successful outcome.

It should also be highlighted that nations with a low level of IT development, for this very reason, retain at the same time a relative strength, and an insuperable defence strategy, with regards to any possible technological counter-attack which might be carried out by 'highly digitalized' nations, meaning they possess a kind of 'general deterrent' should acts of cyberwarfare be used, or should a real cyber-war break out.

Virtual conflict, real damage

What has been said thus far should lead to serious (and urgent) consideration being given not just to the general aspects of cyber-war and its related strategies of attack, defence and the mitigation of damage, but above all to the precise identification of what the primary targets within our national territory which can be attacked via the internet[5] might be, even in the case of individual acts of cyberwarfare.

If we wish to refer only to targets where an attack could lead to the loss of human lives, we must highlight:

- *electronic airport, civil and military air traffic and airspace control systems*: although under current security procedures it does not seem possible that these could be used to cause mid-air collisions or other problems for aircraft coming in to land[6], it is however highly plausible that these airspace control systems[7] could be remotely disabled, allowing, for example, carpet bombing of the territory by hostile aircraft without any early-warning alarms being set off[8].
- *electronic control systems on civil and military aircraft*: these systems becoming compromised can cause problems for aircraft during take-off and landing[9], in addition to, as was sadly demonstrated by Air France flight 447 in June 2009[10], aircraft falling out of the sky in mid-flight.
  Despite this, at least as far as is known, not being the result of an actual malicious attack, this tragic event has demonstrated how current aeronautic (fly-by-wire) technology, in the event of any problems with the on-board computer, can irredeemably compromise the safety of the flight and of the passengers on that flight, giving the pilot very little chance to regain control of the aircraft.
- *the electronic systems of companies which design and develop the hardware and software used in airports, in air traffic control and in the construction of aircraft, both civil and military*: here, the objective is that of manipulating, in the design phase, software or hardware which will eventually come to be used in critical environments[11].
  The events linked to the theft of designs relating to the American F-35 project[12] are an example of this kind of act.

It is also possible (although this would be difficult) that a hostile Government would not limit itself to simply copying confidential information, or carrying out acts of simple electronic espionage, but would aim to gain access to the plans, have them analyzed by its specialists, and introduce into the millions of lines of code which form the basis of the flight control software of an aircraft a small 'backdoor' – which would be hard to single out amongst the sea of information present – which would allow it to gain complete remote control of the aircraft. This manipulated code would then be reinserted into these previously violated systems. Once these are put into large-scale production, this 'backdoor' could then be used to make the aircraft fall out of the sky, or, in the case of military aircraft, to make it launch, for example, a missile with different target coordinates than had previously been set.

- *electronic national defence systems*, via which a 'non-willed' attack could be launched (even a simple long-range missile) towards the territory of a specific nation.
- *fully-automated subway control systems*: these do not require conductors or drivers to be present on trains, but feature, and are driven automatically, by 'VAL' systems. Compromising the security of these could lead to two trains colliding, or could cause individual trains to derail or travel beyond the end of the line, with a probable consequent loss of human lives.
- *water supply and control systems*, which, if compromised, might not just leave large areas without water (and for long periods), but most importantly may not reveal, or cover up for, the presence of impurities or of substances which are highly toxic and damaging to the health of citizens.
- *hospital electronic systems*: the electronic systems for managing patient's clinical records could be compromised and/or, even worse, manipulated.
- *electronic emergency management systems (such as the Italian 118 services and the fire brigade)*: this could cause a late response, or even the total lack of a response, to emergencies, with the result that the health and/or lives of one or more citizens would be put at risk.
- *electricity grid management systems*: the manipulation of these could represent the greatest threat thus far analyzed and, therefore, must be thought of as the absolute priority issue in terms of defending our nation.

It is enough to remind ourselves that without electricity, nothing would work: computers, trains, aircraft, hospitals, telecommunications services, supply systems, etc. This would most likely cause a popular civil revolt, resulting in unmanageable damage to the Government's image, and causing people to lose faith in it.

Also, in the event of a serious, targeted attack, and not a simple, temporary malfunction, there is little that the systems which control energy continuity could do to compensate for the system being compromised and for damage which could not be repaired within 24 hours, which would have the domino-effect of causing further blackouts as attempts were made to make up for the deficit in the supply of electricity.

In order to provide a complete overview, two further cases must be highlighted, in which at first glance it would seem possible that human lives could be put directly in danger. However, for two different reasons, this could not in fact occur. These two cases are:

- *railway electronic systems*, which, despite 'taking on' the locomotive as soon as the train arrives at the barrier at stations such as Rome or Milan and electronically managing its speed, time of arrival, and scheduling its route with respect to other trains on the same line and any stops to be made, are always subject to a procedure which means that overall control is never completely taken out of the hands of the driver of the train or the operator working within the train station control centre. These two operatives in fact, in a reciprocal, duplicate manner, control the operations undertaken electronically by the two computers (on the train and at the control centre), and are always, at any moment, able to manually intervene and override this automated process.
- *financial and banking systems*, which, in the same way as was explained with regards to the manipulation of the national electricity grid, despite not being able to cause the direct loss of human lives, control an asset so critical to the State that, at all times, they must be taken into direct consideration. The economic or financial collapse of an entire nation, in fact, could easily bring about public uprisings which would have a high risk of causing human lives to be lost.

In this particular case, however, most foreign countries would be reluctant to commit such a devastating act of cyberwarfare, given the fact that the financial collapse of one nation often has repercussions for many others. For this reason, nations which are normally considered to be 'threats' in terms of cyberwarfare - above all China and Russia - would not actually see any benefit from carrying out a massive electronic attack on these kind of systems, as they are already tightly 'interconnected', both economically and financially, to the Western world.

A different logic applies, however, to those economies which are particularly independent and shut off from the rest of the world, for example North Korea, which, conversely, might find an attack on Western financial systems to be highly convenient, given that, amongst other things, it would be immune from any possible counter-attack aimed at causing similar economic or financial damage. Seen this way, however, the strong influence that China currently exerts on that part of the world can be said to have a pacifying influence with regards to this particular threat – so much so, in fact, that we can say that such an event would be very unlikely to occur.

Data and statistical elements related to the threat

Currently, tracking down reliable data and statistics with which to support the theses so far put forward is a difficult, complicated activity.

This is true for two reasons: the first is linked to the – at least public - scarcity of data relating to acts of cyberwarfare and/or of a true, proper cyber-war; the second, on the other hand, is closely linked to what was previously mentioned in the introduction to this project with regards to the simplicity with which it is possible to cover up the true origin of any act/attack carried out using IT equipment, which is aimed at the computer systems of another State.

In any case, a good starting point can be tracked down in the document "*Significant Cyber Incidents Since 2006*"[13], edited and updated by the *Center for Strategic and International Studies*, which collects and lists attacks which have been carried out on IT systems and the networks of Governments, defence departments and the largest high-tech companies, in addition to financial crimes which have caused losses of over one million dollars. Even a brief analysis of the contents of the list can shed light on how, in the short space of three years (2006-2009), there have been at least 44 attacks of this type, 30% of which occurred in 2009 alone[14].

Further reflections can be made on data supplied by *U.S. Strategic Command* which, via the *U.S.-China Economic and Security Review Commission*, has highlighted how over the course of 2008 the computer systems of the American Department of Defense registered 54,640 attacks on its computer systems. Furthermore, during the first six months of 2009, 43,785 were recorded. Should the rate of these attacks remain constant, by the end of the year this would result in the annual number of attacks showing an increase of 60% with respect to 2008. A level of growth which was confirmed by the few statistical hints presented in the most recent *Quadrennial Defense Review*[15], in which it was acknowledged that in the last two years computer attacks on the military sector have averaged over 5,000 per day, and also by the words of General Keith Alexander – currently commander of U.S. *Cyber Command* – who, during the Senate hearing to confirm his nomination in April 2010, confirmed that the integrity of the computer systems of the Department of Defense are tested by those with malicious intentions "hundreds of thousands of times a day[16]". Surely the words of General Alexander refer to the so-called probing activities which are carried out on computer systems, and not to actual attacks, but this fact, should it come to be confirmed and supported by solid data, would certainly be revealing.

The American data, which is certainly substantial, seems however to lose a little of its consistency when compared to the recent declarations made by a representative of Azerbaijan's *State Protection Special Service*, who, during an international workshop on the theme of "A *Comprehensive Approach to Cyber Security*", revealed that the IT systems of critical Azerbaijani infrastructure are the targets of around 3,500 attacks every day, almost all of which come from Chinese and American systems, with around 15% also coming from Armenian systems[17]. Certainly just as relevant is the fact that 3,060 computers are compromised daily on Australian soil[18], as is the fact that 6,039 cyber-incidents were recorded and confirmed by CERT-India in 2009[19], or the 1,942 intrusions observed up to August 2009 by the Malaysian Government[20].

Conclusions

Before we are able to discuss any conflict conducted on that new battleground represented by the internet, and which is already dominated by the ‘fifth element”[21] (after sea, land, air and space), we find ourselves today also having to fight a war of words over the meaning of the term ‘cyber-war’.

But what is a cyber-war? At what point can we say that we find ourselves facing an electronic war? What are its rules of engagement, and what methods are there for verifying that our responses are commensurate with any attacks suffered? Where can we lay the blame for any attack, and with what degree of certainty? When faced with the dangers that derive from a threat which, as much as it has been analyzed so far, certainly cannot be said to have been overestimated, these cannot and must not be thought of as simply academic questions.

Providing a convincing answer to these questions is not one of the objectives of this study, which is aimed more at providing evidence for, and developing, a debate on the real danger to human lives which even a single, isolated act of cyberwarfare, if well planned out, and/or a hypothetical cyber-war, could have. They are questions which, despite being posed at the very dawn of the creation of a specific Cyber Command[22] by the American Department of Defense, have still not been answered definitively. They are also questions which are constantly being bandied about as part of this war of words between those who are convinced that the Western world – *in primis* America – has for some time been in the middle of a real cyber-war, and that it is losing it, and those who, despite the continuing and growing amount of criminal activity perpetrated over the internet, argue that the label ‘cyber-war’ was created for merely economic reasons by those hundreds of satellite companies which orbit the world of American Defense, and who are ready to try and ferment a fear of this new world (which is difficult for those who are not specialists in the subject to understand) in order to receive a share of the billions of dollars in consultancy fees set aside to help protect against this new threat.

Above all, the element which this debate (which already seems to be without end) seems to be missing is a solid understanding of the true nature of the threats originating from the internet. The term cyber-war is surely legitimate, but only when used to define those attacks carried out by military personnel using as their instruments computers or comparable electronic systems, and which have as their targets the comparable computers, computer networks or electronic systems of their adversaries, with the intent of causing real-world damage.

This last point is the essential issue here: in order for us to be able to talk about cyber-war, it is necessary for those acts carried out using IT equipment to have had damaging consequences in the real, ‘offline’ world too. And this is the reason for which, for the majority of cases which until now have made it into the news, it is certainly more opportune to talk about acts of cyberwarfare, or acts which have as their objective the non-authorized violation of a computer in another country on its network or of any other activity which is part of an IT system by, or against, or supported by, a Government, which has the aim of adding, modifying or falsifying data, or to interrupt or damage, even temporarily, one or more networked devices, or any other device which is controlled by an IT system[23].

And so, if what has been discussed above is correct, at this point it would be particularly difficult to describe this type of threat as having been ‘overestimated’, given the possibility (if not the probability) that the damage that might arise from this threat is not just verifiable, but that it could also put the lives of citizens in serious danger, as this study has shown.

Bibliography

[1] It must be noted, however, that in a recent study on the phenomenon of the so-called zeroday attacks and the relevance they actually have to the computer crime ecosystem, only a minimal and almost irrelevant percentage of attacks were carried out through the exploitation of errors of this kind, and that, instead, the majority of IT system violations are actually carried

out via the exploitation of well-known bugs which have not been fixed with their relevant patches.
For more information, see Dancho Danchev, "*Seven myths about zero day vulnerabilities debunked*", at http://www.zdnet.com/blog/security/seven-myths-about-zero-day-vulnerabilities-debunked/7026?tag=mantle_skin%3Bcontent

[2] General Michael Hayden, former director of the NSA, during a speech at the *Black Hat* conference, stated that a solution to the problem of attributing responsibility was currently being discussed and evaluated by the American Government, founded on avoiding searching for a precise 'face' (whether State or non-State) to be linked to one or more IT attacks carried out against America, but instead considering nations to be directly responsible for any damaging activities that originate in their 'cyber-space'.

[3] The Wall Street Journal, however, in April 2009, revealed that Chinese and Russian spies have long been violating the electronic systems of United States National electricity grids, installing within them programs which can be activated over the internet, and which are capable of deactivating and/or destroying them within a matter of minutes.
The article can be found here: http://online.wsj.com/article/SB123914805204099085.html

[4] As an example of this, it is enough to remember that FBI agent Philip Hanssen, over 22 years of betrayal (from 1979 to 2001) and espionage carried out for the Russian Government, managed to photocopy and sell just a few hundred pages of classified documents, putting himself directly at risk. Hanssen is currently serving out a life prison term, including 23 hours per day of solitary confinement.
Because of the internet and the digitalization of documents, however, the risk of being personally discovered during criminal acts has not only declined, but it is above all now possible to obtain many thousands of pages of confidential documents in an instant, and with extreme ease. Emblematic of this, recently, was the *Wikileaks* scandal over Afghanistan, which saw over 92,000 confidential documents made public, and the case of the young American intelligence analyst Bradley Manning, who is accused of making public, again via the *Wikileaks* portal, a video which documents military action carried out by the USA and of handing it over to a non-Governmental third party.

[5] The events highlighted in the previous note have forced DARPA (the Defense Advanced Research Projects Agency) to develop, over the course of one month, a program known as CINDER (Cyber Inside Threat), through which it aims to try and stem the loss of confidential information from within the American defence sector by constantly monitoring the research, indexation and electronic copying of data.
Further information on this highly interesting project can be found at: https://www.fbo.gov/index?s=opportunity&mode=form&id=cf11e81b7b06330fd249804f4c247606&tab=core&tabmode=list&

[6] An event which was only recently acknowledged by US Defense vice president William Lynn III, following the publication in *Foreign Affairs* of an essay entitled "*Defending a New Domain: The Pentagon's Cyberstrategy*", available at http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain

[7] See Department of Homeland Security (DHS) – Office of Inspector General, "*DHS Needs to Improve the Security Posture of Its Cybersecurity Program Systems*", available at http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_10-111_Aug10.pdf

[8] For a general overview of vulnerabilities relating to the management and control systems of critical infrastructure, see Idaho National Laboratory, "*NSTB Assessments Summary Report: Common Industrial Control System Cyber Security Weaknesses*", at http://www.fas.org/sgp/eprint/nstb.pdf,

May 2010, and Jason Stamp, John Dillinger, William Young and Jennifer DePoy, "*Common vulnerabilities in critical infrastructure control systems*", at http://www.sandia.gov/ccss/documents/031172C.pdf, November 2003.

[9] The collision between two aircraft during landing is highly improbable, at least following an act of cyberwarfare by a foreign State, as cross-checks are carried out between the pilot of the aircraft and the control tower which, until it has the aircraft in sight, communicates with the pilot using radar data (position, speed etc.). The control tower 'directs' the aircraft from the moment its presence is detected in its airspace until it lands, giving it information on speed, when to change direction, and the height it must descend or ascend to, etc. Each command given to the pilot is immediately confirmed. This means that, even if some radar signals were to be falsified, which is certainly plausible, the pilot could always disregard those commands he receives in favour of what he himself sees from the cockpit during the landing phase, and his own instrumentation. Furthermore, a large number of sensors exist along runways which indicate the presence and position of other aircraft.

[10] For a greater understanding of the American situation, an analysis of the U.S. Department of Transportation document entitled "*Review of web applications security and intrusion detection in air traffic control systems*" makes for interesting reading, available at http://www.oig.dot.gov/ sites/dot/files/pdf-docs/ATC_Web_Report.pdf. This document sets out five security recommendations for the *Federal Aviation Administration* to apply to its air traffic control and management systems, with the aim of avoiding the possibility that these systems continue to be vulnerable to *cyber-attacks*. Actually, as can also be seen in this official document, (http://www.oig.dot.gov/sites/ dot/files/Response%20Letter%20to%20Reps%20Mica%20Petri%20ATC%20Web%20Secuirty%20Follow-up%2008-05-10.pdf), of the five recommendations, only four have currently been put into practice, with the recommendation relating to the adoption of intrusion detection systems remaining 'open' and incomplete.

[11] This is what happened to the computers of the Syrian air defence systems when, in September 2007, they inexplicably did not signal the entrance into the National territory of Israeli Eagle and Falcon aircraft (which are not 'stealth' aircraft), which were capable of bombing a nuclear site.

[12] Around the end of August, the Spanish newspaper *El Pais* carried the news that the authorities investigating the Madrid air disaster of 2008 had discovered that one of the computer systems which monitored technical issues on the aircraft was found to be infected with malware. It is supposed, therefore, that one possible cause of this tragedy, in which 154 people died, was in fact the lack of an alarm warning of a technical malfunction, due to an infection within the control server. According to *El Pais*, an internal compiled by the airline company revealed that that computer, which is situated at the Palma di Majorca headquarters of the airline, should have recognized at least three technical problems with the aircraft which, had they been correctly diagnosed by the server, would not have been allowed to take off. The Trojan virus, therefore, despite not having directly caused the incident, could have contributed to allowing an aircraft which should never have left the ground to do so. The final report on this event, however – which goes into greater detail – will only be made public in December. For now, for further details, see: http://www.elpais.com/articulo/espana/ordenador/Spanair/anotaba/fallos/aviones/tenia/virus/elpepiesp/20100820elpepinac_11/Tes

[13] Detailed information on this event, above all focusing on what happened on board the aircraft before it crashed, can be found at: http://wikileaks.org/wiki/Category:Air_France

[14] In fact, most electronic components currently used in all computers and mobile

phones today are made in China, which is held, along with Russia, to be the most dangerous nation in the world in terms of the risks associated with cyberwarfare. Not by chance, some months ago, India decided to ban, for security reasons, the use of electronic components sourced from China, in particular those produced by the two largest companies present in the territory, Huawei Technologies and ZTE. http://india.foreignpolicyblogs.com/2010/05/18/india-restricts-chinese-telecom-firms-citing-security-concerns/

[15] For further details on this event, see "*Computer Spies Breach Fighter-Jet Project*" at: http://online.wsj.com/article/NA_WSJ_PUB:SB124027491029837401.html

[16] This document, which was unfortunately only last updated on January 29 2010, can be found at the following address: http://csis.org/files/publication/100120_CyberEventsSince2006.pdf

[17] For further details, see also my own analysis, "*Le esigenze americane in materia di cyber-terrorismo e cyber-warfare. Analisi strategica delle contromisure*" ("American needs in terms of cyber-terrorism and cyber warfare. A strategic analysis of counter-measures"), March 2010, available at: http://www.intuslegere.it/doc/cyber_warfare_s_mele.pdf

[18] U.S.-China Economic and Security Review Commission, "*2009 Report To Congress of the U.S.-China Economic And Security Review Commission*", November 2009.

[19] In 2000, however, the number of IT incidents highlighted stood at just 1,415. It must be remembered, however, that this disconcerting increase is also in part due to the increased ability of the American Government to recognize these so-called cyber threats, and the growing attention world public opinion is giving to the subject.

[20] Available in full at: http://www.defense.gov/qdr/images/QDR_as_of_12Feb10_1000.pdf

[21] For the entire text of the Senate hearing, see U.S. Senate - Committee On Armed Services, "*Nominations Of Vadm James A. Winnefeld, Jr., USN, To Be Admiral And Commander, U.S. Northern Command/Commander, North American Aerospace Defense Command; And Ltg Keith B. Alexander, USA, To Be General And Director, National Security Agency/Chief, Central Security Service/Commander, U.S. Cyber Command*", available at: http://armed-services.senate.gov/Transcripts/2010/04%20April/10-32%20-%204-15-10.pdf

[22] According to the article "*3,500 external penetrations fixed in state segment of Azerbaijani internet per day*", available at: http://abc.az/eng/news/47804.html

[23] *Cfr.* Duncan Anderson, "*Cyber Security and Critical Infrastructure Protection: An Australian Perspective*", International Telecommunication Union Regional Cybersecurity Forum for Asia-Pacific, September 2009, available at http://www.itu.int/ITU-D/cyb/events/2009/hyderabad/docs/anderson-cybersecurity-australia-sept-09.pdf

[24] *Cfr.* Gulshan Rai, "*Cyber Security & Role of CERT-In*", International Telecommunication Union Regional Cybersecurity Forum for Asia-Pacific, September 2009, available at: http://www.itu.int/ITU-D/cyb/events/2009/hyderabad/docs/rai-role-of-cert-in-sept-09.pdf

[25] *Cfr.* Mohd Shamir Hashim, "*Malaysia's National Cyber Security Policy. Towards an Integrated Approach for Cyber Security and Critical Information Infrastructure Protection (CIIP)*", International Telecommunication Union Regional Cybersecurity Forum for Asia-Pacific, September 2009, available at: http://www.itu.int/ITU-D/cyb/events/2009/hyderabad/docs/hashim-national-policy-malaysia-sept-09.pdf

[26] For a more in-depth analysis, see RAND Corporation, "*Cyberdeterrence and Cyberwar*", at http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf, 2009.

[27] The "*U.S. Cyber Command Fact Sheet*" is available here: http://www.defense.gov/home/features/20

10/0410_cybersec/docs/CYberFact-Sheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf

[28] This definition does not contain within itself the concept of "electronic espionage", which, in many ways, is a completely different activity, at least on the theoretical, objective level, from that defined as cyberwarfare.

Stefano Mele is a lawyer specializing in IT, privacy, security and intelligence law. He holds a PhD from the University of Foggia. Stefano lives and works in Milan where he carries out consultancy work for large, often multinational, companies, on the subject of legal problems inherent within the issue of privacy and the protection of personal data, the internet and computer crime. He has prepared numerous publications and studies for books, reviews and specialist websites on these subjects. He is also an expert in security, cyber-terrorism and cyberwarfare. He is a senior researcher at the Department of Strategic Intelligence and Security studies at the Link Campus University of Rome, and teaches the cyber-terrorism and cyberwarfare modules of its "Masters Degree in Intelligence Studies and National Security". He is a founding partner and vice president of the Centro Studi Informatica Giuridica di Foggia (CSIG-Foggia – 'Foggia Centre for the Study of the Legal Aspects of Computing') and is Sector Director 'Intelligence and Electronic Espionage' of the Italian Institute for Privacy. The author thanks Davide Cardilli [http://www.theogre.org] for the cover design and layout of this document.

The Complexities of the Drug-Conflict Nexus

By Vanda Felbab-Brown

The tiles from the roof slid as soon as I landed on it and noisily crashed down to the picturesque street of Ayacucho, Peru, alerting the Senderista and *cocalero* guards who patrolled the area near the *zócalo*. The shots they fired into the air were probably not meant to hit me, but the residents whose roof I destroyed in my ill-fated attempt at escape and who rushed to the roof of the adjacent house in fury looked scary enough.

This was six years ago. I had come to Ayacucho, the former hotbed of the Shining Path, to investigate what happened with the remnants of the guerilla movement and interview the former insurgents and current *cocaleros*. And I was lucky on that first of my many fieldwork trips to research from the ground up the relationship between military conflict and illicit economies: The *cocaleros* – maybe five thousand of them – in an impressive display of power seized the area of the main city square while I was there, set up barricades, and held it under siege for a few days, demanding an end to forced eradication of their coca fields. As a result, I got great access and could interview some key actors otherwise hard to track down. But I also had arranged for another trip into one of Peru's areas of illegal coca cultivation. This involved crossing the Andes in a small plane, meeting up with my contact, hiring a motor boat and later a motorized canoe, and hiking deep into the forest to access the coca fields and the *cocaleros*. But there I was stuck in Ayacucho without any means to communicate with my contact who was waiting at the edge of the jungle. Hence, my first escape attempt. My second attempt worked out, however; and the fieldwork in the coca fields proved equally valuable.

Subsequent trips took me to some of the world's most marginalized areas of violence, criminality, and poverty: the coca fields of Colombia, where local *cocaleros,* alienated from the government by aerial spraying, still swear allegiance to the FARC; the poppy areas of Burma where former insurgents and drug dealers who had become officials of their autonomous zones gave me lengthy lectures on their eradication efforts even while their labs produced *meth* right under my nose; to Afghanistan where poppy flowers liven up an otherwise bleak landscape, and produce more opium than any other country in the past fifty years; and to India, Mexico, and Morocco. Each of the trips was not only full of adventure, even fun, but also provided a wealth of data, based on interviews with multinational organizations and government officials, military, police, and intelligence officers, farmers of illicit crops and producers of illegal goods, traffickers, crime bosses, and insurgents.

What emerges from the fieldwork and analysis is sobering: Much of U.S. anti-narcotics policy abroad has been based on the premise that suppression of drug production will promote both anti-drug and counterterrorist goals. My work challenges this premise. I show that, far from being complementary, U.S. anti-narcotics and counterinsurgency policies are frequently at odds. Crop eradication—the linchpin of U.S. anti-narcotics strategy— fails to significantly diminish the physical capabilities of the belligerents.

In fact over the past fifty years eradication has not yet bankrupted one single belligerent group to the point of substantially weakening it – not in Colombia, Afghanistan, Peru, Thailand or Burma. In Colombia, for example, the prototypical showcase for those who argue that suppressing an illicit economy will destroy the belligerents (as the government of President Alvaro Uribe frequently did), both the leftist guerrillas, such as the FARC, and the rightist paramilitaries and their descendents, the so-called *bandas criminales*, adapted by switching to kidnappings, the extortion of other economies, such as gold mining, and following the coca farmers to new areas where they replanted coca. Direct military effort against the FARC that disrupted it movements had a far greater impact on weakening its military capabilities than eradication.

But eradication in a poor country with a paucity of legal livelihoods and with a labor-intensive illicit economy that can provide employment to hundreds of thousands, if not millions, is not simply ineffective. It is also deeply counterproductive since it enhances the belligerents' legitimacy and increases popular support for them. Over the years, I have interviewed many coca farmers in Colombia, for example, whose sole affinity for the FARC lay in the FARC protection of their coca fields from the government and U.S.-sponsored eradication effort.

Belligerents obtain this political capital by protecting the illicit economy, and hence the local population's reliable source of livelihood, from government efforts to suppress it. Sometimes, they bargain with traffickers for better prices on behalf of the farmers, and provide otherwise absent social services and public goods, such as clinics, infrastructure, and dispute resolution mechanisms. In short, belligerents use the illicit economy to transform themselves into security providers and economic and political regulators. This political legitimacy is frequently thin, but nonetheless sufficient to motivate the local population to withhold intelligence on the belligerent group from the government if the government attempts to suppress the illicit economy. Such intelligence is critical for winning a counterinsurgency effort.

Four factors largely determine the extent to which belligerents can benefit from their involvement with the illicit economy: the state of the overall economy; the character of the illicit economy; the presence (or absence) of thuggish traffickers; and the government response to the illicit economy.

- The state of the overall economy – poor or rich — determines the availability of alternative sources of income and the number of people in a region who depend on the illicit economy for their livelihood.
- The character of the illicit economy – labor-intensive or not – determines the extent to which the illicit economy provides employment for the local population.
- The presence (or absence) of thuggish traffickers, and
- The government's response to the illicit economy (which can range from suppression to laissez-faire to legalization) determine the extent to which the population depends on the belligerents to preserve and regulate the illicit economy.

In a nutshell, supporting the illicit economy generates the greatest political capital for belligerents if the state of the overall economy is poor, the illicit economy is labor-intensive, thuggish traffickers are active in the illicit economy, and the government has adopted a harsh strategy, such as eradication.

Instead of destroying the poppy, coca, and marijuana fields, postponing eradication at least until conflict has ended, and ideally until legal livelihoods are in place is more likely to enhance counterinsurgency effectiveness. Other policies, such as interdiction against drug traffickers and their labs, are easier to calibrate with a counterinsurgency effort, but they too are extremely unlikely to bankrupt belligerents.

But governments can, and many times have, prevailed against belligerents without disrupting their money flows: by winning the hearts and minds of the population and increasing their own military forces, such as in Thailand against the various ethnic and Communist insurgencies in the 1970s or in Peru against the Shining Path in the 1990s. The successes against the FARC in Colombia came despite, not because of, eradication. In Afghanistan, the United States government and ISAF have been able to see how eradication of the poppy fields has pushed the Afghan population into the hands of the Taliban, and the Obama Administration has defunded centrally-led eradication. Individually governors of Afghan provinces occasionally engage in eradication, such as in Helmand, but their efforts have been meager, since intense eradication is politically unsustainable for most of them. The U.S.-led counter-narcotics efforts now center on the interdiction of Taliban-linked drug-traffickers and the development of alternative livelihoods.

In fact, this sequencing of security first, then intense counter-narcotics policies, also enhances counter-narcotics efforts: Good security is an essential requirement for the success of any counter-narcotics policy – be it mailed-fist eradication or rural development efforts.

In *Shooting Up*, I provide three sets of recommendations:

1) how to optimize efforts against illicit economies with counterinsurgency and conflict mitigation;
2) how to enhance the effectiveness of counter-narcotics policies in sustainably reducing the size of the drug trade and diminishing the power of crime groups; and
3) how to include 2nd and 3rd degree effects into regulation considerations.

Some of these recommendations are:

- *When dealing with labor-intensive illicit economies in poor countries, governments should undertake efforts to suppress those economies that affect the wider population only after military conflict has been brought to an end.*
- *Military forces, whether domestic or international, should focus on directly defeating the belligerents and protecting the population.* They can be most effective at supporting policies to suppress illicit economies by focusing on providing basic security. Without such security, efforts to suppress illicit economies will not be effective.
- *If belligerents have not yet penetrated an illicit economy, governments should make every effort to prevent them from doing so or tempt the belligerents into suppressing the illicit economy themselves, provided the government can distance itself from such a policy and offer material help to the population.*
- *Governments also should explore the possibility of licensing particular illicit economies.*
- *Governments should avoid treating traffickers and belligerents as a unified actor, and therefore strengthen the bond between them; instead, they should explore ways to pit the two actors against each other.*
- *Interdiction efforts should be designed to limit the coercive and corruptive power of criminal groups, rather than being dominantly focused on stopping illicit flows.*
- *Governments and their international partners must address the demand for illicit commodities and contraband.*
- *Governments and international organizations need to consider where the illicit economy is likely to re-emerge if suppression efforts in a particular country or region are effective.*
- *Governments and international organizations need to consider the possibility that other illicit economies will replace the current one if suppression succeeds.*
- *Finally, when deciding on particular regulations and prohibitions, including international sanctions, governments and international organizations need to seriously consider whether the harm resulting from such a prohibition and its enforcement will be greater than the harm resulting from a laissez-faire approach.*

Vanda Felbab-Brown is a fellow in Foreign Policy Studies and a member of the 21st Century Defense Initiative at the Brookings Institution. She also teaches in the Security Studies Program at Georgetown University's School of Foreign Service. An expert on international and internal conflict issues, including counterinsurgency, she has published widely on the interaction between illicit economies and military conflict and has testified before Congress about her work. She is the author of ***Shooting Up: Counterinsurgency and the War on Drugs*** (Washington, DC: Brookings Institution Press, 2009). The research on which this book is based received the American Political Science Association's Harold D. Lasswell Award for the Best Dissertation in the Field of Public Policy.

BIANA S.A.

PRODUCTION OF NBC GAS MASKS AND FILTERS

The COBRA NBC gas mask is of Greek technology and fully meets the operational requirements of all international specifications, such as:

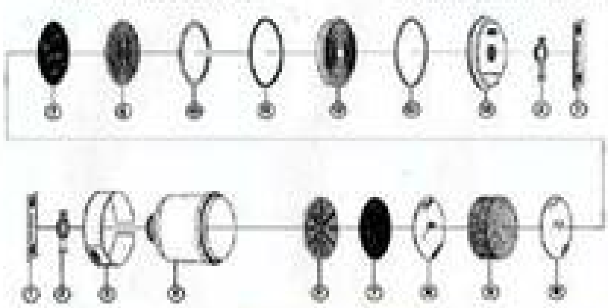
- NATO specifications: NATO (AC/225)/Pannel VII/D 103,
- German specifications: TL 4240-016 and
- Greek specifications: Ministry of National Defense (MND) / General Defense Directorate (GDAEE).

DRINKING DEVICE

CORRECTION GLASSES

MICROPHONE DEVICE

VOICE AMPLIFIER



1. Filter cap safety tape
2. Filter cap
3. User instructions label
4. Filter canister
6. Perforated disk
7. Canvass
8. Felt
9. Activated carbon
10. Upper perforated disk holding ring
11. Rubber ring
12. Particle filter
13. Particle filter tightness ensuring material
14. Filter cover

WITH EXPORTS TO GERMANY, ARAB COUNTRIES AND CYPRUS

Development and Production of the rubber parts

Quality Control Laboratories

BIANA S.A. PRODUCTION OF NBC GAS MASKS AND FILTERS

10 APOLLONIOU STR. GR 194 00 KOROPI GREECE TEL.: +30 210 662 3910
FAX: +30 210 662 4724 INTERNET: www.biana.gr e-mail: anargyrou@biana.gr

TÜV HELLAS
TÜV
EN ISO 9001

The Muslim Brotherhood in Egypt

By Yehudit Barsky

Allah is our objective.
The Prophet is our leader.
Quran is our law.
Jihad is our way.
Dying in the way of Allah is our highest hope.

Slogan of the Muslim Brotherhood

The Muslim Brotherhood Society, or *Jama'iya Al-Ikhwan Al-Muslimun* (also referred to simply as *Ikhwan*), was formed in Ismailiya, Egypt, in 1928 by Hasan Al-Banna, a charismatic schoolteacher and Islamist preacher. Al-Banna formulated a politicized, extremist form of Islam as a means of confronting Western moral and cultural influence among Egyptians. The Brotherhood's goal is to eliminate all Western influence and create an Islamist state in Egypt and, ultimately, the world.

Al-Banna sought to explain the malaise of Egyptian society in his time as being due to what he portrayed as the corrosive influence of Western culture. He accused government officials and other prominent members of Egyptian society of abandoning Islamic principles and behaving in an immoral fashion due to Western influence. The remedy, he insisted, was a revival and reestablishment of an Islamic state that would return Muslims to the pinnacle of their military, historical, and cultural glory. He pointed to the Caliphate, the historic Islamic empire and the most celebrated period of Islamic history, as the template for his vision of an Islamic state. In a 1947 letter to Egypt's King Farouk titled «Towards the Light,» Al- Banna asserted that the only way to return to those days of glory was to re-establish shari'a, Islamic law, as the source for governance as well as for societal and personal behaviors.[1]

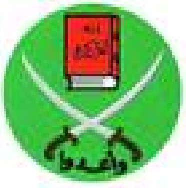
In his teachings, Al-Banna preached a return to the Prophet Muhammad's strategies during the early days of Islam in the seventh century, strongly emphasizing each Muslim's personal obligation to carry out jihad, which he defined as physical warfare.

In a tract from the 1930s titled «Jihad,» Al-Banna writes:

> *Jihad is an obligation from Allah on every Muslim and cannot be ignored nor evaded. Allah has ascribed great importance to jihad and has made the reward of the martyrs and the fighters in His way a splendid one. Only those who have acted similarly and who have modelled themselves upon the martyrs in their performance of jihad can join them in this reward. Furthermore, Allah has specifically honoured the Mujahideen [those who fight jihad] with certain exceptional qualities, both spiritual and practical, to benefit them in this world and the next. Their pure blood is a symbol of victory in this world and the mark of success and felicity in the world to come.*[2]

Drawing a parallel between the times of the prophet Muhammad and the present, Al-Banna portrayed non-Muslims as idol worshipers and placed a central focus on spreading Islam and fighting what he termed the "enemies of Islam." The purpose of jihad, he asserted, was not for the personal glory or gain of Muslims: "Rather, jihad is used to safeguard the mission of spreading Islam. This would guarantee peace and the means of implementing the Supreme Message. This is a responsibility which the Muslims bear, this Message guiding mankind to truth and justice."[3]

Symbol of the Muslim Brotherhood



Jihad plays a central role in the ideology of the Muslim Brotherhood, which is also reflected in the symbol of the movement. It consists of a circular green background signifying Islam. Superimposed over it are the Quran, representing the centrality of its teachings for the movement, and two crossed swords below it, denoting jihad. Below the swords is the Arabic word وَأَعِدُّوا "wa'adu," meaning "make ready" or "prepare yourselves." It refers to this verse in the Qur'an which is interpreted by the Brotherhood as an exhortation to engage in jihad against the enemies of Muslims today:

> *Against them make ready your strength to the utmost of your power, including steeds of war, to strike terror into (the hearts of) the enemies of Allah and your enemies, and others besides, whom ye may not know, but whom Allah doth know. Whatever ye shall spend in the cause of Allah, shall be repaid unto you, and ye shall not be treated unjustly.*[4]

Impact Today

Al-Banna's writings, the core ideological texts of the Muslim Brotherhood, remain the basis for the ideology of the movement and the curriculum for the indoctrination of its initiates today. In the early years of the movement, his writings were distributed as pamphlets in mosques, Brotherhood-affiliated charitable institutions, and coffeehouses. The movement established its own mosques, schools, and sports clubs in order to spread its ideology, and by the time of Al-Banna's death in 1948, the Brotherhood is believed to have garnered some 2 million followers in Egypt.[5] Today Al-Banna's writings are promoted and distributed by the Muslim Brotherhood and its affiliated organizations via the Internet.

Al-Banna's strategy and tactics for establishing an Islamist state have become a template for the Brotherhood's activities throughout its history. As a means of achieving a critical mass of supporters, Al-Banna prescribed a long-term course of indoctrinating the Muslim masses in the ideology of his movement, which would ultimately bring the establishment of an Islamist state, and it became a template for the Brotherhood's activities throughout its history. This strategy of Islamization is referred to as da'awa, meaning "invitation" or "outreach," and is still in use today.

Terror Activities

In parallel to these activities, Al-Banna created an underground paramilitary wing called the "Special Apparatus," which carried out attacks against the British as well as a campaign of bombings and assassinations that also targeted Egyptian Jews.[6] The Brotherhood leadership regularly engaged in violent anti-Semitic rhetoric against Egyptian Jews which incited attacks against the community, including the torching of the Alexandria synagogue.[7] On the international level, Al-Banna supported Haj Amin Al-Husseini, the Mufti of Jerusalem who worked for the Nazis to recruit international Arab support for Germany. The Nazis provided subsidies to the Brotherhood, which were coordinated by Al-Husseini, and part of the funds were used to purchase arms.[8] Members of the Brotherhood were also later recruited to take part in the 1948 war against Israel, which they considered to be part of their obligation to engage in jihad.

The Brotherhood was declared illegal in 1948 after it was accused of assassinating Egyptian Prime Minister Muhammad Al-Nuqrashi. Later that year Al-Banna was assassinated, reportedly by a member of the Egyptian security forces.

The movement subsequently supported the 1952 Free Officers military coup, and was then briefly permitted to operate more freely. But in 1954, when the Brotherhood was considered responsible for an unsuccessful assassination attempt on Egyptian president Gamal Abd Al-Nasser, it was again declared illegal. Thousands of its members were arrested, imprisoned, and tortured, and the movement was forced to shift its operations underground. Its most prominent ideologue of that period, Sayyid Qutb, was executed in 1966. Others left for Saudi Arabia and the Gulf countries.

In 1971, President Anwar Al-Sadat, Abd Al-Nasser's successor, seeking to counter the political influence of Communists and Nasserists who were trying to oust him, looked to the Brotherhood as a countervailing force that could assist him in maintaining power. He declared a general amnesty for the imprisoned members of the Brotherhood. But this period of cooperation was short-lived. The Brotherhood turned against Al-Sadat for rejecting the implementation of shari'a and the establishment of an Islamic state, and for signing a peace treaty with Israel. The Egyptian Islamic Jihad, an offshoot of the Brotherhood, assassinated Al-Sadat in 1981. After Husni Mubarak succeeded Al-Sadat as president, Egypt's 1958 Emergency Law was reenacted, giving the government power to arrest individuals without charging them with a crime and to detain prisoners indefinitely, limiting freedom of expression and assembly, and establishing a special security court. The emergency laws have been in effect ever since and were extended for two more years in 2010.[9]

The Brotherhood's Global Reach

Although the Muslim Brotherhood was originally established in Egypt, its activists and ideology have spread throughout the Muslim world as well as within Muslim communities in the West, including Europe and the U.S. Its activists have also spawned terrorist organizations, most prominently Al-Qaida, whose second-in-command, Ayman Al-Zawahiri, started out as a Brotherhood activist and then created the terrorist organization Egyptian Islamic Jihad. He became an official founding member of Al-Qaida in 1998.

Today the Brotherhood claims branches in over 80 countries.[10] Each branch maintains ideological affiliation to the movement even though in many cases local branches of the movement will establish themselves as separate entities with different names. Hamas, for example, is the Palestinian branch of the Muslim Brotherhood, and Tunisia's Al-Nahda Movement, led by Rashid Al-Ghanushi, is the Muslim Brotherhood branch in that country. Turkey's AKP originated in the Muslim Brotherhood and, similarly, the Islamic Action Front in Jordan and the Iraqi Islamic Party are branches of the Muslim Brotherhood in their respective countries.

Political Support within Egypt

Due to the numerous crackdowns by the government against the movement, the Brotherhood has focused on Islamization through social welfare projects, establishing its own infrastructure of social services among the poor and disenfranchised members of Egyptian society that are not served by the government. These services have generated sympathy and support for the movement among Egyptians.

The Brotherhood has also focused its efforts on garnering power through involvement in private organizations. Via the democratic process, it now controls professional and student associations that are considered to be the most prominent nongovernmental organizations in the country.[11]

Since 1984, the Brotherhood has engaged in open political activity, running independent candidates in Egyptian parliamentary elections. In 2005 it won 20 percent of the vote, resulting in 88 seats.[12] It is estimated that the Brotherhood could win up to 30 percent of the vote in new elections.[13] Although there has not been a poll directly examining Egyptians' sympathies for the Brotherhood, the views of Egyptians were similarly reflected in a recent Pew study. It indicated that 31 percent of Egyptians see a struggle between modernizers and Islamic fundamentalists in their country, and 59 percent of that number identify with Islamic fundamentalists.[14]

Future Prospects

The current General Guide of the Muslim Brotherhood, Muhammad Badi, has demonstrated adherence to Hasan Al-Banna's ideology by reiterating its principles in a series of recent sermons. In a September 2010 sermon he reasserted that the Qur'an should be the constitution of the state, and declared it the duty of Muslims to enact Islamic law.[15]

Badi has also promoted jihad as a central means of returning Islam to its former glory. In April 2010 he declared, «Muslim leaders, Islam, to which you belong, advocates jihad as the only means for setting the Ummah's [nation's] situation aright.» He continued, «Our revival, majesty, and glory depend on the return to righteousness, which will only be achieved through resistance and the support of [resistance] in every way – with money, arms, information, and self [sacrifice].» Badi further proclaimed that it is the «obligation» of Muslims to stop all negotiations with Israel and to «support all forms of resistance for the sake of liberating every occupied piece of land in Palestine, Iraq, Afghanistan, and all [other] parts of our Muslim world.»[16]

In a September 2010 sermon, Badi asserted that the U.S. «is now experiencing the beginning of its end, and is heading towards its demise....» He further declared that the victory of Muslims against their enemies was preordained and called upon Muslims to rise against Israel and the U.S.: «Resistance is the only solution against the Zio-American [sic] arrogance and tyranny, and all we need is for the Arab and Muslim peoples to stand behind it and support it.»[17]

Prior to Egypt's first round of parliamentary elections in November 2010, Badi denounced the Mubarak regime and called for its removal «by peaceful means outlined in the constitution and the law.»[18] During the 2011 Egyptian revolt, Badi called upon Egyptians to continue the «blessed uprising» until the deposal of the Mubarak regime, and insisted that «the Egyptian people, from all groups, refuse to negotiate with the ruling regime.»[19]

The Brotherhood initially played a low-key role in the Egyptian mass anti-government demonstrations, but its leadership gradually began to amplify its demands, focusing on the removal of the Mubarak government. While the Brotherhood was not involved in the early days of the demonstrations, its activists joined the secular organizers of the anti-Mubarak revolt. They were careful not to call attention to their Islamist agenda and did not display Muslim Brotherhood banners or shout the traditional chants of the movement.

On the ground in Tahrir Square, however, they played a leading role. The presence of the Brotherhood volunteers was ubiquitous: they manned checkpoints, provided hot tea to the protestors, and participated in the demonstrations by chanting, "Welcome to Free Egypt!"[20] Rashad Bayoumi, the deputy leader of the Brotherhood, asserted that his members were involved in the demonstrations, but emphasized that their participation was part of a revolution against the regime, not an Islamist revolution: «We are taking part. Thousands of our members are on the streets. But we are saying that this isn't a Muslim revolution. This is a revolution against Mubarak!»[21]

Representatives of the movement living abroad called for an end to the regime in a more directly. Sheikh Yusuf Al-Qaradawi, the Muslim Brotherhood's spiritual leader and most prominent ideologue, is the author of fatwas legitimizing suicide bombings against Israeli civilians and U.S. military personnel, and expresses vehemently anti-Semitic views. His comments were regularly broadcast in Tahrir Square at the epicenter of the demonstrations. In a January 29 interview on Al-Jazeera that was broadcast from his home in Qatar to the demonstrators he declared, «Go away, Mubarak, leave this people alone! Enough, you've ruled for 30 years already! Dozens have been killed in one day. You cannot stay, Mubarak!» He continued, «On behalf of hundreds of thousands of religious clerics in Egypt and in the Muslim world I'm calling on you to leave your country.«[22] He also played a significant role by encouraging the protestors to come to Tahrir Square by declaring that participating in the demonstrations was an Islamic obligation and staying home was forbidden.[23]

In another sermon to the protestors Al-Qaradawi directly called on the Egyptian army to depose Mubarak and demanded the appointment of the head of the country's constitutional court as president. A week after Mubarak's deposal, Al-Qaradawi returned to Egypt to preach a sermon in Tahrir Square at the victory celebration of the demonstrators.

On February 4, Rashad Bayoumi, the deputy Brotherhood leader, sounded one of the movement's core political agenda items, declaring, "After President Mubarak steps down and a provisional government is formed, there is a need to dissolve the peace treaty with Israel."[24] Muhammad Ghanem, a Brotherhood spokesman in London, went even further, calling for war with Israel and stopping the passage of ships through the Suez Canal: «I am absolutely certain that this revolution will not die, and that the next step must be one of civil disobedience. This civil disobedience will generate strife among the Egyptians. This disobedience must include halting passage through the Suez Canal, stopping the supply of petroleum and natural gas to Israel, and preparing for war with Israel.»[25]

Conclusion

Since Mubarak's departure, the Brotherhood has declared that it will form a political party to run in new elections but will not ru for the presidency. The Brotherhood's leadership has been especially cautious to emphasize that it wants participation in the political process without overtly promoting its Islamist agenda. This stance makes it possible for it to work with the secular leadership of other potential political parties.

Based on its prior history and recent statements by its General Guide, the Brotherhood will likely bide its time until the formation of a new Egyptian government before testing the new regime by raising its Islamist agenda. The Brotherhood's current situation is similar to that of Hamas, which built its support on an agenda of reform and providing social welfare services. The Brotherhood may focus its efforts on the democratic process of transforming support for its social welfare projects into political power at the polls. Employing the Hamas model, it may use the new political playing field as a means of Islamization to transform Egypt into an Islamist state, increasing its political power through its social welfare infrastructure until it can take control through the democratic process, carrying out a coup d'état, or both.

The current Egyptian transition has given the Brotherhood a new lease on political life. Its recent statements nevertheless indicate that it has not changed its extremist political agenda, which remains a cause for concern among Egyptians and observers of the situation throughout the world.

Yehudit Barsky is director of AJC's Division on Middle East and International Terrorism.

Bibliography

[1] Hasan Al-Banna, «Towards the Light,» May 1947/Rajab 1366, IkhwaanWeb, official English language website of the Muslim Brotherhood,; http://www.ikhwanweb.com/article.php?id=802

[2] Hasan Al-Banna, «Jihad,» Young Muslims of Canada website, youth division of Islamic Circle of North America; http://web.youngmuslims.ca/online_library/books/jihad

[3] Hassan Al-Banna, «Jihad,» Young Muslims of Canada website; http://web.youngmuslims.ca/online_library/books/jihad

[4] Qur'an, Surat Al-Anfal, 8:60, Yusuf Ali translation, SearchTruth.com, http://www.searchtruth.com/chapter_display.php?chapter=8&translator=2#60

[5] "Profile: Egypt's Muslim Brotherhood,» BBC News, January 28, 2011; http://www.bbc.co.uk/news/world-middle-east-12313405

[6] Ibid.

[7] Richard S. Levy, ed., Anti-Semitism: A historical encyclopaedia of prejudice and persecution, (Santa Barbara, California: ABC CLIO, 2005) 478-479.

[8] Brynjar Lia, The Society of the Muslim Brothers: The rise of an Islamic mass movement, 1928-1942, Reading, UK: Ithaca Press, 1998) 178-179.

[9] «Egyptian Emergency Law Is Extended for 2 Years,» New York Times, May 11, 2010; http://www.nytimes.com/2010/05/12/world/middleeast/12egypt.html

[10] «Glimpse Into the History of [the] Muslim Brotherhood,» IkhwaanWeb, June 10, 2007; http://www.ikhwanweb.com/article.php?id=794

[11] John Walsh, «Egypt's Muslim Brotherhood,» Harvard International Review, March 6, 2006; http://hir.harvard.edu/perspectives-on-the-united-states/egypt-s-muslim-brotherhood

[12] «Mohammad Badi: A Voice in the Government,» Newsweek, November 29, 2010; http://www.newsweek.com/2010/11/29/mohammad-badie-on-egypt-s-muslim-brotherhood.html

[13] «'We Are On Every Street': What the Future May Hold for Egypt's Muslim Brotherhood,» Spiegel Online, February 1, 2011, http://www.spiegel.de/international/world/0,1518,742940,00.html

[14] «Egypt, Democracy and Islam,» Pew Global Attitudes Project, January 31,2011; http://pewresearch.org/pubs/1874/egypt-protests-democracy-islam-influence-politics-islamic-extremism

[15] «An Overview of the Egyptian Muslim Brotherhood's Stance on U.S. and Jihad,» MEMRI, Special Dispatch 3558, February 3, 2011; http://www.memri.org/report/en/0/0/0/0/0/0/4970.htm

[16] «An Overview of the Egyptian Muslim Brotherhood's Stance on U.S. and Jihad,» MEMRI, Special Dispatch 3558, February 3, 2011; http://www.memri.org/report/en/0/0/0/0/0/0/4970.htm

[17] «Muslim Brotherhood Supreme Guide: 'The U.S. Is Now Experiencing the Beginning of Its End,» IkhwanOnline.com, September 30, 2010; translated by MEMRI, Special Dispatch 3274, October 6, 2010; http://www.memri.org/report/en/0/0/0/0/0/193/4650.htm

[18] « General Guide of the Muslim Brotherhood Muhammad Badi', in Pre-Election Interview, Calls to Remove the NDP from Power,» Al-Jazeera, November 24, 2010; translated by MEMRI, Special Dispatch No.3476, December 28, 2010; http://www.memri.org/report/en/0/0/0/0/0/0/4877.htm

[19] «Egypt: Jamaa Islamiya ideologue blasts Muslim Brotherhood,» Al-Sharq Al-Awsat (Saudi Arabia), February 3, 2011; http://www.aawsat.com/english/news.asp?section=1&id=24018

[20] "Egypt: Muslim Brotherhood influence felt at Tahrir Square," GlobalPost.com, February 7, 2010; http://www.globalpost.com/dispatch/egypt/110207/egypt-muslim-brotherhood-tahrir-square

[21] «'We Are On Every Street': What the Future May Hold for Egypt's Muslim Brotherhood,» Spiegel Online (Germany), February 1, 2011, http://www.spiegel.de/international/world/0,1518,742940,00.html

[22] «Top cleric: Mubarak, go away!» Ynet.com (Israel), January 29, 2011; http://www.ynetnews.com/articles/0,7340,L-4020733,00.html

[23] «Top Sunni Cleric: Participating in demonstration is an Islamic obligation,» Ahlul Bayt News Agency (Iran), February 5, 2011; http://abna.ir/data.asp?lang=3&id=224430

[24] "Muslim Brotherhood seeks end to Israel treaty," Washington Times, February 3, 2011, http://www.washingtontimes.com/news/2011/feb/3/muslim-brotherhood-seeks-end-to-israel-treaty/?page=1

[25] «The Middle East Crisis XVI: Muhammad Ghanem, Egyptian Muslim Brotherhood Representative in London, Calls for Civil Disobedience, Including 'Halting Passage through the Suez Canal ... and Preparing for War with Israel,'» Special Dispatch 3558, Al-Alam TV (Iran), January 30, 2011, translation by Middle East Media Research Institute, February 3, 2011; http://www.memri.org/report/ en/0/0/0/0/0/0/4972.htm

EDITOR'S NOTE: The globe is facing a social turbulence in the Muslim world covering the Maghreb, the Levand and Middle East in general. Egypt is the country where struggle for democracy was more prominent – so far. In February 14th, 2011 **George Friedman** for **Stratfor** think tank is commending on the "***Distance between enthusiasm and reality***":

On Feb. 11, Egyptian President Hosni Mubarak resigned. A military council was named to govern in his place. On Feb. 11-12, the crowds that had gathered in Tahrir Square celebrated Mubarak's fall and the triumph of democracy in Egypt. On Feb. 13, the military council abolished the constitution and dissolved parliament, promising a new constitution to be ratified by a referendum and stating that the military would rule for six months, or until the military decides it's ready to hold parliamentary and presidential elections. What we see is that while Mubarak is gone, the military regime in which he served has dramatically increased its power. This isn't incompatible with democratic reform. Organizing elections, political parties and candidates is not something that can be done quickly. If the military is sincere in its intentions, it will have to do these things. The problem is that if the military is insincere it will do exactly the same things. Six months is a long time, passions can subside and promises can be forgotten…… We do not want to be killjoys now, since everyone is so excited and happy. But we should point out that, in spite of the crowds, nothing much has really happened yet in Egypt. It doesn't mean that it won't, but it hasn't yet. An 82-year-old man has been thrown out of office, and his son will not be president. The constitution and parliament are gone and a military junta is in charge. The rest is speculation.

Source: http://www.stratfor.com/weekly/20110213-egypt-distance-between-enthusiasm-and-reality

U.S.A. the Perennial Struggle for a Biological, Chemical, and Nuclear Free Globe

By Vassilios Damiras

In the post Cold War epoch, the United States of America started an extensive and a very expensive program to reduce or even eliminate the dangerous menace of biological warfare, chemical development, and nuclear proliferation. At least three main and important factors underlie this renewed emphasis on proliferation policy and strategy. First, the reduced military menace from the former Soviet Union has increased the relative importance of lesser powers, especially if armed with weapons of mass destruction. Second, certain international political and technological trends are increasing the threat to international security from proliferation. Third, new opportunities are opening for enhancing the current international regimes designed to severely stem proliferation. Since then the American government has spent more than six hundred million dollars and close to a billion dollars in various biological and chemical threat reduction programs and nuclear nonproliferation projects mainly focused on the former Soviet Union Republics. Specifically, American officials focused in the Asian region of the former and notorious Soviet Empire. This policy involved hard, long, and tough diplomatic negotiations.

The former Soviet Republics has been a real challenge for the various American programs focusing on biological, chemical, and nuclear nonproliferation. The toughest of the situation is because; this specific and troubled region has many serious and insurmountable socio-economic, political, and military challenges. After five years of crucial and tough negotiation between U.S. and Kazakh diplomatic and military officials, a U.S. Air Force C-17 cargo plane under heavy security transported several samples of bubonic and pneumonic plague bacteria from laboratories in Kazakhstan to the U.S. Centers for Disease Control and Prevention in Fort Collins, which is located in the State of Colorado. Also both sides mutually agreed that, U.S. and Kazakh chemical and biological scientists will now study the bacteria with the main goal of developing and producing new scientific methods to diagnose and treat the plague.

This specific shipment was part of a larger scheme of cooperative biological threat reduction process between the United States and former Soviet republics in Central Asia. This biological threat reduction has the main purpose and target at protecting against diseases that occur naturally in the region and which could also be exploited by various bioterrorists. In specific terms, several Islamic terrorists or terrorist groups throughout the years have been trying to create a dirty bomb and attack various economic, political, and military installations in Europe, Asia, and in United States. Thus, the U.S. officials are on alert to impede or prohibit that kind of terrorist activities. The bulk of these various projects are funded via the auspices and aegis of the Cooperative Threat Reduction (CTR) Program administered by the U.S. Defense Department. Additionally, the U.S. State Department, U.S. Department of Health and Human Services, U.S. Defense Threat Reduction Agency, U.S. Strategic Command USSTRATCOM, and U.S. Department of Agriculture, which administer projects related to farming, is involved in the project. Later on the U.S. Department of Energy and the U.S. Department of Homeland Security joined the program. Also the U.S. Army, U.S. Navy, U.S. Marines, U.S. Air Force, and U.S. Coast Guard participated in the various elements of the program.

Created and established in 1991, the CTR Program was an unprecedented effort to significantly aid the disintegrating Soviet Union deal with nuclear, chemical, and biological proliferation threats. The initial focus of the program was on the nuclear weapons inherited by three non-Russian republics (Belarus, Kazakhstan, and Ukraine) and on Russia's nuclear weapons, materials, and facilities. The American officials wanted to control these dangerous and lethal weapons in case rogue nation-states or rogue groups wanted to acquire them and utilized them to destabilize global relations among countries. Four-hundred million dollars were originally allocated for the nuclear-related projects. After the significant success of the denuclearization programs of Belarus, Kazakhstan, and Ukraine, and with a bulk of the most pressing Russian nuclear proliferation threats under controlled or even resolved despite the then Russian President and currently Russian Prime Minister Vladimir Putin strange behavior toward the United States, CTR crucial efforts turned their focus to dealing with several and serious bio-threats that menacing the international affairs. This specific and important shift also illustrates the larger emphasis that nation-states around the globe are placing on the role of harmful and deadly infectious disease surveillance in international security and stability procedures.

The U.S. government has invested more than four hundred and thirty million dollars from 1998 through 2007 in its biological and chemical threat reduction programs, which includes funding for various projects in Russia, Kazakhstan, Uzbekistan, Georgia, Azerbaijan, and Ukraine. Annual funding levels have been steadily increasing every year. During this period Kazakhstan received roughly $107.4 million for bio-threat reduction projects and Uzbekistan received $78.7 million. The spending also significantly increased after the horrific terrorist attacks of September 11, 2001 at the World Trade Center in New York City and the U.S. Pentagon in Washington, D.C., which were masterminded and executed by the notorious Islamic terrorist group Al Qaeda and its leader Osama bin Laden.

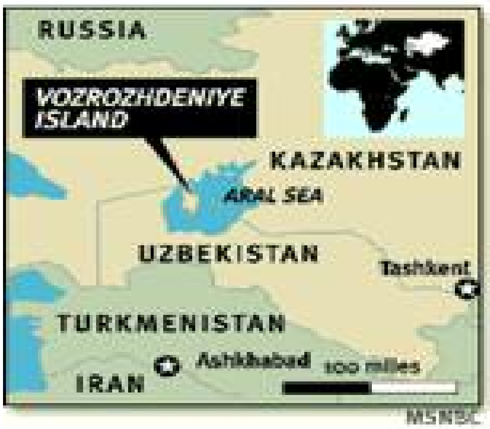
Since 1992, the U.S. Department of Defense (DOD) and the Russian Ministry of Defense (MOD) have been jointly designing and developing projects to considerably improve the safety and security of Russia's nuclear weapons as they are dismantled, transported, and stored at sites throughout Russian proper. Projects have included the delivery to Russia of armored blankets, security upgrade kits for railcars, emergency response equipment, and super containers used during transport. Ongoing Weapons Protection, Control, and Accounting (WPC&A) several projects include upgrading security at weapons storage sites, providing a computerized weapons stockpile system, exchanging unclassified information about nuclear warheads, and providing a drug and alcohol monitoring program for guards at weapons storage sites. From 1992 through 1997, the DOD allocated $116 million of CTR funds for WPC&A programs. By 2000, total WPC&A funding had reached $293.1 million, and the program's total cost is expected to reach $967.7 by FY2007.

Also, the American officials focused on the region incorporated Central Asia, because Central Asia was once at the center of the Soviet biological warfare program. The world's largest and most vibrant bio-weapons military facility, which had a capacity to produce 300 tons of anthrax a year, was situated in northern Kazakhstan in Stepnogorsk. Stepnogorsk was created and established in the 1964, though it is not marked on Soviet maps and it has been variously designated Makinut-2, Tselinograd-25, and Aksu. The area also included and still incorporates a big facility for the extraction of uranium ore associated with the uranium mining areas and deposits are in the north-central region in the Akmola and Kokshetau oblasts of Kazakstan. The Tselinny Gorno-Khimichskii Kombinat (TGK) mines and refinery, centered on the Stepnogorsk district, was at one time the second largest uranium producer in the Soviet Union. Specifically, the center for the manufacture of bacteriological weapons was constructed ten kilometers away from the settlement of Stepnogorsk, a town whose population had grown to over 60,000 by 1989. Building 221 is the heart of the production facility, consisting of three dozen bioreactors with a comprehensive protection system. In late 1990, Biopreparat researchers tested Marburg virus on monkeys and other small animals in special explosion-test chambers at the Stepnogorsk plant.

In addition, during the years of the Cold War, Soviet Chemical scientists extensively tested biological weapons on Vozrozhdeniye Island in the Aral Sea and on Ustyurt Plateau in the Uzbek steppe. The thousands of Soviet biological and chemical scientists who participated in the bio-weapons programs worked daily to protect their country against biological or chemical attack or attacks and to ensure that the Soviet Union had bio-weapons at its disposal, if necessary in case in a vicious war with the United States.

Under the Cooperative Threat Reduction agreement between America and Kazakhstan, about three million dollars has been granted for the dismantling and elimination of biological and chemical military centers, including the one at Stepnogorsk. In 1998, the U.S. Civilian Research and Development Foundation (CRDF) made three additional awards for projects that include scientists from Kazakhstan's Stepnogorsk defense biological research facility. The Stepnogorsk facility is the focus of a special effort by the American and Kazakh governments to redirect defense scientific and engineering resources to civilian work. The U.S. State Department is providing $210,000 to support these additional projects. Moreover the foundation provides training for various bio-security measures and detection. Also, CRDF has expanded its chemical bio-bacterial, and bacteriological research and operations in Albania, Iraq, and Pakistan.

The Vozrozhdeniye (Renaissance or Rebirth) Island test site in the Aral Sea was part of the older, military biological warfare system. The island was apparently chosen for open-air testing of biological weapons because of its geographical isolation. Vozrozhdeniye is located in the middle of the Aral Sea, surrounded by large, sparsely populated deserts and semi-deserts that hindered unauthorized access to the secret site. The island's sparse vegetation, hot, dry climate, and sandy soil that reach temperatures of 60 degrees C (140 degrees F) in summer all reduced the chances that pathogenic microorganisms would survive and spread. In addition, the insular location prevented the transmission of pathogens to neighboring mainland areas by animals or insects. The northern part of Vozrozhdeniye Island, which Kazakhs call Mergensay, is on Kazakhstani territory. The southern two-thirds of the island are in the Karakalpak autonomous region of Uzbekistan.



MSNBC

In 1936, Vozrozhdeniye Island was transferred to the authority of the Soviet Ministry of Defense for use by the Red Army's Scientific Medical Institute. The first expedition of one hundred people, headed by Professor Ivan Velikanov, arrived on the island that summer. The researchers were provided with special ships and two airplanes and reportedly conducted experiments involving the spread of tularemia and related microorganisms. In the fall of 1937, however, the expedition was evacuated from the island because of serious security problems, including the arrest of Velikanov and other specialists.

In 1952, the Soviet government decided to resume biological warfare testing on islands in the Aral Sea. A biological weapons test site, officially referred to as «Aralsk-7,» was built in 1954 on Vozrozhdeniye and Komsomolskiy Islands. The Ministry of Defense's Field Scientific Research Laboratory (PNIL) was stationed on Vozrozhdeniye Island to conduct the experiments. Military unit 25484, comprising several hundred people, was also based on the island and reported to a larger unit based in Aralsk. The PNIL developed methods of biological defense and decontamination for Soviet troops. Samples of military hardware, equipment, and protective clothing reportedly passed field tests at the island before being mass-produced. During the Soviet intervention in Afghanistan, military protective gear developed for Afghan conditions was tested at the PNIL.

Currently, a comprehensive epizootological study of Vozrozhdeniye Island funded and supported by the United States and operated by the Uzbek Center for Prevention and Quarantine, is a significant and very vital addition to indigenous disease surveillance campaigns on the island: Kazakh and Uzbek biological and chemical scientists presently monitor the island for plague and other biological diseases, beyond anthrax, that might have been introduced to the island during Soviet times and could easily spread to the mainland through rodents. The dramatic shrinking of the Aral Sea in recent years further exacerbates the proliferation risks PDF if pathogens remain and sustain on Vozrozhdeniye Island. Birds and rodents are potential carriers of dangerous diseases to the mainland, as are people who visit the island proper in search of several pieces of scrap metal.

When the Soviet Union collapsed, the defense and civilian biological weapons programs were thrown into a serious crisis. By 1992, the new regime in Moscow had abandoned most military and civilian sites related to the programs, and governments in the newly independent republics faced the challenge of dealing with their lethal inheritance. Facilities housing collections of deadly pathogens and microorganisms were left either poorly protected or completely unprotected and vulnerable to theft. The military program abandoned Vozrozhdeniye Island, which had been used as a fabrication and testing ground for biological and chemical weapons, leaving caches of anthrax buried underground and other dangerous microorganisms present in its soil. Thus, the abandonment of biological and chemical waste created for Russia and the wider region a serious and dangerous environmental hazard.

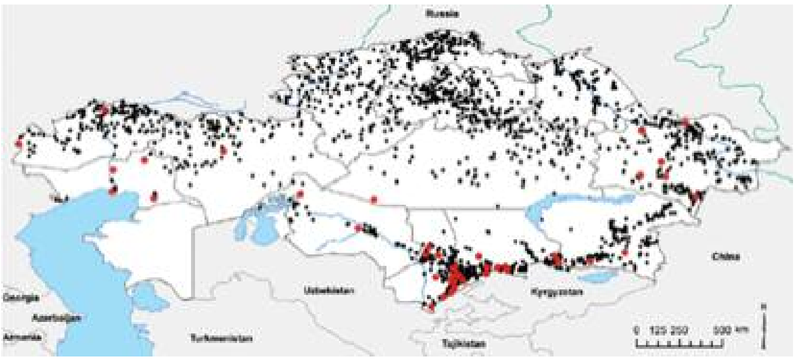
Furthermore, after the Cold War the Russian Federation did not have money to pay their scientists. Thus, thousands of scientists with critical and crucial expertise lost their jobs went unpaid or received meager salaries insufficient to support their families. Moreover, the region had to face with continual outbreaks of highly and dangerous infectious disease, to which it was naturally prone due to serious and catastrophic contamination. Coupled with a serious socioeconomic and political crisis and Central Asia's close proximity to unstable states such as, Afghanistan and Pakistan, the Soviet bio-weapons heritage posed several crucial challenges. Central Asian new independent governments were unaware of the activities took place inside the most sensitive chemical and nuclear facilities involved in the Soviet biological and chemical military program. The resources that the Central Asian governments could allocate to conversion activities were extremely limited, making CTR funding crucial and very important. The United States and Kazakhstan first signed a cooperative threat nuclear and chemical reduction agreement in 1993, to provide for assistance with denuclearization. The agreement was extended in 2000 to further the U.S. assistance in the threat reduction. In Uzbekistan, American cooperation began much later. The initial umbrella agreement was negotiated and signed in 2001.

During the first decade of cooperative biological threat reduction programs, U.S. efforts focused on totally dismantling and even eliminating bio-weapons facilities and destroying bio-weapons agents in Kazakhstan and Uzbekistan, the regions where most key biofacilities were concentrated. By 2000, three key Stepnogorsk buildings were destroyed, while the full greenfielding of the weapons production and testing buildings was dismantled by 2007. In addition, CTR funds also sig nificantly improved the physical protection, safety, and security of the facilities that housed dangerous bio and chemical-agents. The destruction and extensive elimination of bio-weapons facilities on Vozrozhdeniye Island and 150 tons of anthrax in 2002 was followed by the decontamination of the Uzbek part of the island where Soviet military facilities were formally situated.

The extensive bio-threat reduction process in Central Asia has since reached a qualitatively different and a very positive stage. While initial projects dealt mostly with dismantlement, destruction, and elimination, ongoing work emphasizes cooperation and collaborative research with the various regional nation-states. Central Asian scientists are working hard with their U.S. counterparts to strengthen detection and diagnosis of disease outbreaks and to considerable improve the response and reaction to numerous natural epidemics and potential hazardous bio-attacks. For example, a significant amount of funding was given to support Kazakh epidemiological various research and studies of Congo-Crimean hemorrhagic fever, as well as specific studies on factors of anthrax foci. Furthermore, the CTR program PDF also funds Uzbek biological and chemical scientists working on epizootiological and epidemiological mapping of anthrax, plague, and tularaemia, as well as the surveillance of human and animal brucellosis.

In another important project, Kazakh bio-scientists successfully mapped and completed the genetic fingerprinting of ninety three strains of anthrax found in Kazakhstan. Alongside with their Georgian colleagues, these scientists also jointly diagnosed a case of avian influenza and diagnosed and identified the source of an outbreak of Congo-Crimean hemorrhagic fever—a tick, in Uzbekistan. Furthermore, Kazakh chemical scientists from the Republic Sanitary Epidemiological Station in a joint program from relevant research institutes are designing, developing, and implementing a comprehensive study of brucellosis in southern region of Kazakhstan. This study is especially significant from a public health standpoint since there is a high incidence rate of brucellosis among the animal and human population in the country; it is highest in the areas bordering with China, Uzbekistan, and Kyrgyzstan. The ongoing project will able scientists to diagnose brucellosis within a two-hour to one-day period instead of the current forty eight-hour to twelve-day span.

Several recent chemical reduction projects promise to further help counter highly infectious diseases in the region. The United States intends to give funding to research by the Kazakh Scientific Center for Quarantine and Zoonotic Diseases in Almaty on especially dangerous pathogens. A contract of $800,000 was allocated to Kazakhstan's Research Institute for Biological Safety Problems in Otar to start working and analyzing on an avian influenza virus. The project commenced in 2007. The purpose of the project is to extensively monitor avian flu agents among wild and domestic birds, as well as among people with a high risk of contracting the disease (e.g. employees of battery farms, medical workers, and hunters) and to study and analyze the virus's biological properties. An important spin-off effect of similar chemical projects sponsored by internationally funded programs is that participating chemical facilities often receive up-to-date technology, which allows the scientists to work on new innovative scientific studies. The Research Institute of Virology in Uzbekistan received $800,000 for the study of arbovirus infections in the South Aral region.



Anthrax outbreaks in Kazakhstan, 1937–2005. Each dot represents an outbreak; red dots indicate that cultures were isolated and analyzed from these outbreaks.
Source: http://www.cdc.gov/EID/content/16/5/789-F1.htm

Together with the United States, Kazakhstan, Uzbekistan, and other former Soviet republics are designing, developing, and operating an extensive network of surveillance and diagnostic labs. The labs are connected with an Electronic Integrated Disease Surveillance System via various epidemiological monitoring stations. Kazakhstan already owns and operates two biological monitoring stations; Uzbekistan, six; Georgia, four; and Azerbaijan, one. Once collected and gathered, integrated human and veterinary surveillance data is sent off in near-real time to national and U.S. counterparts' biological and chemical facilities.

In 2011, the Cooperative Threat Reduction (CTR) program overarching purpose and mission is to partner with willing nation-states to reduce the serious threat of nuclear and chemical weapons of mass destruction (WMD) and related biological and nuclear technologies, expertise, and materials. Furthermore, this specific program aims the dismantling and destruction of the various Soviet-era nuclear weapons such as, the Intermediate Range Ballistic Missiles (IRBMs) SS-18 and SS-19, the several types of the Medium Range Ballistic Missiles (MRBMs), the various types of the Long Range Ballistic Missiles (LRBMs), the numerous Intercontinental Ballistic Missiles (ICBMs) and their respective silos and the associated Launch Control Center (LCC). Also, the program targets to eliminate all the mobile launchers. Moreover, this project eliminates Submarine Launch Ballistic Missiles (SLBMs) and the launchers from Delta class and Typhoon class Russian Nuclear Ballistic Missile Submarines (SSBNs).

The aforementioned program expands the U.S. Department of Defense Security Assessment and Training Center (SATC) at Abramovo base to serve as the regional training and sustainment center. The SATC will compliment the Far East Training Center (FETC). The new center will provide a classroom building, student dormitory, maintenance and repair workshop, warehouse, garage, and associated equipment for MOD-R. Also, the program gives money for safe and secure weapons transpiration with special equipped cars with highly sophisticated monitor equipment. Also, it allocates money for secure rail transportation. The transportation part of the project comes under the agreement Nuclear Weapons Transportation Security Implementing Agreement.

The chemical and biological threat reduction part of the agreement focuses on especially dangerous pathogens (EDPs). It allocates money for improving the biological safety and security (BS&S). Furthermore, this program considerable enhances the capabilities of partner nation-states to detect, report, and interdict illicit trafficking in various hazardous and menacing WMD or related bacteriological life threatening materials. This kind of viable cooperation between America and the Central Asian republics are very vital and important for their own regional security, wider regional security, and global stability.

In addition, in 2011, the U.S. Defense Threat Reduction Agency introduced the Caspian Sea Maritime Proliferation Prevention (Azerbaijan). This counter biological and chemical project supports and assists the development of a comprehensive capability to detect and interdict life threatening WMD and related biological and chemical weapons or agents along Azerbaijan maritime border on the Caspian Sea. It supplies maritime surveillance equipment and procedures; repair and upgrade of existing naval vessels; modern equipment for boarding crews; including high sophisticated devices to detect various biological and chemical WMD; the construction, repair, and upgrade of command and control maintenance, and various logistics facilities; and construction of a highly technological and sophisticated operating location along Azerbaijan southern coast to improve the on-station time and expand the operational patrol areas of the state border service-Coast Guard.

Since the very early days of their strong cooperation with the United States, the Central Asian nation-states have demonstrated high degree of openness and an extensive transparency. If political and military will prevail and all sides overcome old and archaic bureaucratic behavior and implementation hurdles that occur along the way, the cooperative threat reduction process will continue to not only strengthen public health and bio-defense capacities and capabilities but also serve the larger purpose of building a strong trust between Washington and the various Central Asian governments. Thus, it is imperative the United States to continue assisting and monitoring the situation in the region. If the United States withdrawn the anti-biological and anti-chemical projects will collapse making easier for terrorists to find a way and manufacture a dirty bomb. The American government must continue the policy of establishing tough obstacles for countries of acquiring chemical, biological, and nuclear agents. It is mandatory to control these dangerous and extremely hazardous chemical, biological, bio-bacterial, bacteriological, and nuclear agents if the United States wants global stability.

Vassilios Damiras is a multilingual consultant with a great experience in counter-terrorism and counter-intelligence. He holds a PhD and MA in History (Loyola University, Chicago, IL) and MA in Political Science (Illinois State University, Normal, IL). Currently he is the Vice President and Co-founder of GTing and Global Defence Consulting, LLC; also Director, International Affairs and Security at Nova Vista Capital Advisors, LLC. He is the Director/Editor of SAS International Relations Magazine. His main interests focus in: U.S. National Security, Geopolitical Analysis, Strategic Studies, Force Protection, Human Intelligence, Law Enforcement, Global Intelligence, Terrorist Financing, Counterinsurgency, International Affairs, Asymmetric Threat Operations, Strategic Intelligence, Homeland Security, Chemical, Biological, Radiological, and Nuclear Weapons and Issues, and U.S. National Missile Defence. In the past he served as consultant at US Republican Party.

A Falcon Communications Ltd Publication

CBRNe WORLD

2010 Media Kit

Preparing for the non conventional threat

The most effective medium to reach the CBRNe equipment and services buyer and specifier

Organisers of the annual CBRNe Convergence Conference & Exhibition and CBRNe FOCUS Workshops

www.cbrneworld.com

Medical/Hospital CBRNE defence

Is the medical/hospital community ready to deal with a chemical-radiological (CR) terrorist attack in megapolis' environment? – Athens 2004 Olympic Games experience
By Ioannis Galatas

Submitted in fulfillment of the requirement for the degree of Master of Arts *in* International Terrorism, Organized and Global Security - Coventry University - September 2010. ***Modified for the purposes of the Newsletter.***

We have to be lucky all the time.
They have to be lucky only once!
IRA spokesman's comment following the unsuccessful attempt to murder former UK Prime minister Margaret Thatcher

When planning, think as a terrorist!
When implementing, think as a victim!
Operational logo of Olympic Games 2004 Hospital CBRN Response Unit, Army General Hospital of Athens, Greece

Hope for the best.
Prepare for the worst!
Common logic!

Introduction

Human brain is the recipient of myriad stress effects. It responds by initiating about 1400 different activities affecting all body organs and systems. From the very first moment primitive man faced a life threatening beast, terror was amongst these stimuli that it was meant to follow him, in different forms, throughout his evolution. Terror for life was elicited in his strives to survive adverse climate phenomena, opposite tribes or pandemics. Then it was territorial expansion, containment of vital resources, exploitation of new worlds, political wars. This kind of terror became a part of his evolution and man acclimatized and at the same time desensitized to the idea of dying for a cause – important or less important makes no difference.

During the last two centuries, this terror element gradually chanced face and new era terrorism produces terror most often without a cause – although all actions do have a causative substrate hidden. But even then there was always a direct relationship between the terrorist and the terrified victim. There was contact – eye contact, physical contact. Victims could see it coming; they could anticipate the end. During the First Word War (WW I) this "contact" changed dramatically. This "contact" disappeared. Death became "atmospheric"; nerve gases were coming from nowhere. Terrified victims stood still observing their comrades dying and wait for their turn to dye as well. This new form of terror was far above the stimuli brain could process – even in the battlefield. Perhaps this was the main reason that opposing forces involved in the Second World War (WW II) including Hitler himself, were so reluctant to use chemical weapons although they had tons of them stored in their arsenals.

World community relaxed and thought that this "bad dream" would be gone for good. It was too terrifying to think the other way. Even the atomic bombing of Hiroshima and Nagasaki was not heavily criticized at that time with the excuse of ending WW II for good. Then at the end of the 20th century, a disturbed Japanese fanatic was inspired with an idea aiming to destroy Japanese nation. His cult members manufactured both biological and chemical weapons and they were willing to release them against their own society. The sarin attack in the Tokyo's subway in 1995 signalled the beginning of a new era in terrorism. Similar to that troops experienced in the European battlefields during WW I and that of Iran-Iraq conflict in the 1980s only now the delivery area is the urban environment and the targets were ordinary civilians; men, women and children going to their work, their school, their playgrounds.

Six years after that incident, the combination of the bloodiest terrorist attack ever against the Unites States and the "anthrax letters' campaign" made world to realize that these threats were there to stay like the Damocles' Sward over their heads. Mass gathering events represent the perfect environment for a terrorist attack with weapons of mass destruction. In that respect, every four years when global community is preparing for the next Olympic Games, humanity is equally preparing to confront this new threat that might change the course of history.

This is why the medical contribution to this new era CBRN terrorism is immensely important. In an incident involving release of CBRN agents, the medical system will be the one that will take the heat. Victims will rush to hospitals for assistance. Big hospitals, small hospitals, community hospitals, private hospitals, private surgeries – all will be whelmed with casualties. All must be ready to deal with mass contaminated casualties. The medical community must be prepared in advance to deal with such casualties. It might look like dealing with a rare, exotic disease. But imagine tens or hundreds of people suffering from the same exotic disease at the same time! The basis of health policy worldwide is that "prevention is better than treatment". We practice this principle in daily routine. Why cannot we expand it to the remote possibility of a CBRN terrorist incident in urban environment?

This dissertation provides some insides of conventional terrorism such as definitions, major terrorism incidents worldwide, trends in international terrorism and targeting, that will serve as the substrate to understand the transformation of old to new era terrorism (Chapter One). A short outline of chemical and radiological terrorism through time is provided in Chapter Two. Chapter Three reviews the attitude of medical community towards new emerging threats; current situation in the United States and the European Union is analysed as well. In Chapter Four, the experience gained from the active involvement in the CBRN planning for the 2004 Olympic Games, is projected through an overall C-R response plan for urban hospitals. Finally, in Chapter Five, an effort is made the "problems identified" during the 2004 Olympic Games in Athens to become "lessons learned" for the benefit of the London 2012 Olympic Games.

CHAPTER ONE – Terrorism in the 21st Century

Definitions of terrorism

Terrorism[1] derives from the French analogue "*terrorisme*" which is based on Latin verbs "*terror*" and "*terrere*" – "great fear" and "frighten" respectively. When Cimbri tribe attacked Rome (105BC) the city came to a status of "*terror cimbricus*" – state of panic and emergency. In France, the period 1793-1794 is described as "La Terreur" (Reign of Terror). The Jacobin Club in the post-Revolutionary France used the term "terrorists" to define themselves; their actions termed "terrorism" attributed to the arrests or executions of their political opponents.

In general, the term "terrorism" has been controversial through time. Mainly because it depends in which side you are. Many say that terrorism is a coin with two sides: one for terrorists and one for freedom fighters. In that respect, an objective definition of terrorism looks utopian since the subjective part will always dominate. What is strictly objective is the final outcome of a terrorist action. It is the civilians who suffer the consequences and experience, fear, terror and death toll. Bruce Hoffman in his book "Inside Terrorism" writes[2]:

> *Terrorism is a pejorative term. It is a word with intrinsically negative connotations that is generally applied to one's enemies and opponents, or to those with whom one disagrees and would otherwise prefer to ignore. (...) Hence the decision to call someone or label some*

> *organization 'terrorist' becomes almost unavoidably subjective, depending largely on whether one sympathizes with or opposes the person/ group/ cause concerned. If one identifies with the victim of the violence, for example, then the act is terrorism. If, however, one identifies with the perpetrator, the violent act is regarded in a more sympathetic, if not positive (or, at the worst, an ambivalent) light; and it is not terrorism.*

In the same motive Ben Saul approaches a generally accepted definition of terrorism as following[3]:

> *Terrorism' currently lacks the precision, objectivity and certainty demanded by legal discourse. Criminal law strives to avoid emotive terms to prevent prejudice to an accused, and shuns ambiguous or subjective terms as incompatible with the principle of non-retroactivity. If the law is to admit the term, advance definition is essential on grounds of fairness, and it is not sufficient to leave definition to the unilateral interpretations of States. Legal definition could plausibly retrieve terrorism from the ideological quagmire, by severing an agreed legal meaning from the remainder of the elastic, political concept. Ultimately it must do so without criminalizing legitimate violent resistance to oppressive regimes – and becoming complicit in that oppression.*

Perhaps the most important remark that most often is forgotten is the fact that killing is not the primary target of terrorism acts. According to Brian Jenkins "*terrorists desire many people to observe in fear, not a lot of people dead*[4]". In the same motive, Ehud Sprinzak denotes "*terrorism has nothing to do with killing. It is a form of psychological warfare where murdering a small number of people, persuades the rest of us that it is our turn*[5]".

For historical reasons it is of interest to review some of the proposed definitions from organizations worldwide:

Unite Nations definitions

1. League of Nations Convention (1937): «*All criminal acts directed against a State and intended or calculated to create a state of terror in the minds of particular persons or a group of persons or the general public*[6]«.
2. United Nations Security Council Resolution 1566[7] defined terrorism as:
   Criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organization to do or to abstain from doing any act.
3. According to United Nations General Assembly resolution 49/60[8] terrorism represents:
   Criminal acts intended or calculated to provoke a state of terror in the general public, a group of persons or particular persons for political purposes are in any circumstance unjustifiable, whatever the considerations of a political, philosophical, ideological, racial, ethnic, religious or any other nature that may be invoked to justify them.

European Union's definitions

The European Union addresses terrorism as criminal offence against people and property[9]:

> *... given their nature or context, may seriously damage a country or an international organisation where committed with the aim of: seriously intimidating a population; or unduly compelling a Government or international organisation to perform or abstain from performing any act; or seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation.*

United States definition

The United States has defined terrorism under the Federal Criminal Code (Chapter 113B, Section 2331 of Part I of Title 18) as following[10]:

(1) the term «international terrorism» means activities that -

(A) involve violent acts or acts dangerous to human life that are a violation of the criminal

laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State;
(B) appear to be intended -
(i) to intimidate or coerce a civilian population;
(ii) to influence the policy of a government by intimidation or coercion; or
(iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and

United Kingdom's definition

Terrorism Act 2000[11] defines terrorism in the United Kingdom:
(b) the use or threat is designed to influence the or to intimidate the public or a section of the public and
(c) the use or threat is made for the purpose of advancing a political, religious or ideological cause.
(2) Action falls within this subsection if it
(a) involves serious violence against a person,
(b) involves serious damage to property,
(c) endangers a person's life, other than that of the person committing the action,
(d) creates a serious risk to the health or safety of the public or a section of the public or
(e) is designed seriously to interfere with or seriously to disrupt an electronic system.

From the above definitions and many other available, it is prominent that almost all include certain criteria such as target, objective of the perpetrator, motive, perpetrator description and legality of the terrorist action taken. In that respect civilians represent the main target of terrorism regardless if in many instances an early warning has been issued (usually by phone – case reports in Greece). Fear production is the second objective – and the most important of all. Intimidation accompanying fear is directed against governments, societies or groups within. Achieving political or religious goals is the third objective. It is difficult to define the perpetrators in a terrorist incident – especially if their action has a global effect (i.e. September 11th, 2001 attack). In that respect "silence" may provide safe heaven against countermeasures from the strong country involved – especially if "state-sponsored terrorism" is involved. Finally, the legality of terrorist action is sometimes controversial especially when it is addressed against military targets (guerrilla/asymmetric warfare).

Major terrorist incidents around the world (following 911 incidents)

Major terrorist incidents worldwide with more than 100 people killed[12] are recorded below:

11 September 2001
Incident: Two domestic jetliners crashed onto World Trade Center in New York, USA. A third airplane crashed onto Pentagon in Alexandria, Virginia. Passengers of a fourth aircraft on the way to Washington DC, attacked highjackers onboard and finally the plane crashed in Somerset County, Pennsylvania.
Death toll: 2,993 dead (on ground and airplanes) – 8.700 injured
Targets: Civilians, military/civilian defence personnel
Means: Jetliners turned to "flying bombs" following en route high jacking.

12 October 2002
Incident: Bombs exploded in front of a nightclub in Kuta, Bali.
Death toll: 202 dead (2/3s foreigners) – 350 injured.
Targets: Civilians – foreign tourists.
Means: IED, VBIED.

26 October 2002
Incident: 41 Chechen terrorists stormed a theatre in the Nord-Ost theatre in Moscow, Russia.
Death toll: 129 dead (hostages), 41 terrorists killed – 653 rescued.
Targets: Hostages civilians (around 800 – including 75 foreigners)
Means: Light weapons, explosives – Russian counter-terrorist forces used fentanyl (incapacitating gas used in anaesthesiology) to induce unconsciousness.

27 February 2004
Incident: Bomb exploded on a ferry en route from Manila to Bacolod, Philippines.
Death toll: 118 dead – 9 injured.
Target: Ferry boat – civilians (sleeping time)
Means: IED (4kg of TNT inside a television set

11 March 2004
Incident: Multiple bombings during rush hours on trains in three stations in Madrid, Spain.
Death toll: 191 dead – 1.876 injured.
Targets: Civilian commuters– foreign tourists (47 killed)
Means: IEDs – three more bombs defused hidden in backpacks.

3 September 2004
Incident: Three days standoff by Chechen terrorists at a school in Beslan, North Ossetia, Russia
Death toll: 336 civilian hostages killed, 30 terrorists – 727 injured
Targets: Civilians (parents, teachers and school children), policemen
Means: Light/heavy weapons, explosives

11 July 2006
Incident: Multiple bombs exploded during evening rush hour on commuter trains in and near Mumbai, India.
Death toll: 200 dead – 714 injured.
Targets: Commuter trains (first class cars) - civilians
Means: IEDs (RDX explosives and pencil-sized timers were used)

14 August 2007
Incident: Multiple bombings in villages Al-Qataniyah and Al-Adnaniyah, Iraq.
Death toll: 520 dead – 1.500 injured
Targets: Civilians of the Yazidi sect, 1000 houses destroyed, 500 damaged
Means: VBIEDs – disguised trash tankers supposed to carry food (2 tons of explosives)

18 October 2007
Incident: Bombings during crowd greeting of the former Prime Minister of Pakistan Benazir Bhutto in Karachi, Pakistan.
Death toll: 139 dead – 540 injured
Targets: former Prime Minister, state officials, followers
Means: Grenade, suicide bomber (15-20kg of explosives)

26-29 November 2008
Incident: Multiple attacks in Mumbai, India by a group of 10 terrorists who took hostages in a two-day siege
Death toll: 174 dead (many foreigners) **–** 327 injured, one terrorist captured alive.
Targets: several locations (café, train station, hospital, synagogue, 2 hotels) – police forces
Means: Bombs, VBIED, heavy weapons

25 October 2009
Incident: Bombing near government buildings in Baghdad, Iraq.
Death toll: 160 dead, 540 injured
Target: Ministry of Justice, Ministry of Municipalities and Public Works, staff members, civilians (many children)
Means: VBIEDs (1000 kg and 700 kg of explosives in two vehicles)

28 October 2009
Incident: Bombing at a marketplace in Peshawar, Pakistan
Death toll: 118 dead (including seven children from a single family)
Target: Meena Bazaar marketplace (mostly used by women)
Means: Bomb (150 kg of explosives, remotely detonated)

Trends in international terrorism

Late 1990s has been a turning point in terrorism affairs. It was then that “new era terrorism” term was coined to identify new terrorist operational methodologies and violence escalation. Globalization of terrorism is the first characteristic to be noted. Terrorist organizations are still relatively small groups but their structure became more complex and their operational radius longer and wider. Old era terrorist groups transformed to “networks” ruled by personal relationships based to web connections and affiliations. The resulting web transformed from national to trans-national and even international. It is not “core” al Qaeda anymore but rather an “al Qaeda affiliated network” with branches in various parts of the world (i.e. AQIM, AQAP). Observed transformation is partly due to low cost international travelling and modern communication technologies. Uncontrolled mass migration especially towards Western Europe eased translocation of “seeds” of new era terrorism. These “seeds” grow up, spread and flourish through the digital social space of internet. Exportation of terrorism from the active battlefields of Iraq, Afghanistan and Somalia became a reality. Well trained combat-experienced individuals can now “retire” in the West and form small terrorist cells or groups or act as “lonely wolves”. Besides their experience they imported new methodologies that might surprise counter-terrorism organizations in the near future.

Ideology transformed as well. In modern times, religious-driven ideology and nationalism predominate among terrorists despite their original background. Behind the open face of this religious ideology, a rising demand for radical transformation of hosting societies based on their religious principles and way of life is hidden. Peaceful (for the time being) “Musulmanization” of Europe progressing in accordance to the rising percentage of Muslim immigrants in EU countries, is of particular notice. Only recently, hosting societies are beginning to realize that their new “citizens” are trying to change their political systems and replace them with their own (i.e. Sharia law).

A third characteristic of new era terrorism is that terrorists no more seek public acceptance. In that respect, they do not really “care” for the results of their actions and the mass casualties produced. This characteristic makes them extremely dangerous for the integrity of social network. Usage of weapons of mass destruction (i.e. sarin gas attack against subway commuters in Tokyo), signifies their new perception of value of human life. It became obvious from the listing of major terrorist incidents above, that the “over 100 fatalities” cases are now the rule not the exception. This also signifies a shift in brutality accompanying lethality. The rare phenomenon of suicide-bombing does not surprise any more.

Currently two parameters predominate: violence for violence’s shake and symbolism of some kind (often none). Western way of life might in part be responsible for this. Modern generations grew up by watching wars live on their television screens and their violence threshold is high. There are many to support the idea that the next “9-11” must be much more spectacular, much more deadly and widespread ever. In that respect, a chemical or radiological (dirty bomb) attack might make the “desired” difference. According to Peter Neumann “*forecasting is not as easy as drawing a straight line from the past. Unexpected events can play a major part in shaping the dynamics and wider framework within which terrorism takes place*[13].”

Terrorism targets

From the major terrorist incidents presented it is obvious that the main pattern is “anyone-anytime-anywhere”. Two parameters are of critical importance: Number of people gathered and society impact (plus mass media coverage expected). Impact on society is derived from the inability of the state to protect its own population, symbols of authority, society’s institutions, infrastructure and state officials while cannot end terrorism itself providing a peaceful living environment.

Coping with this, most preferred urban targets could be: state buildings, ports, airports, trains and train stations, hospitals, bridges, city tunnels, banks, embassies, factories, power plants (hydroelectric, nuclear), water supplies and pipelines, refineries and oil/gas pipelines, computer networks and symbolic national monuments.

Special attention should be given to hospitals. In the past, all buildings or installations bearing a “cross” or “half-moon” were considered as “sacred”. Despite the international laws forbidding action against sanitary organizations and installations, it was a common perception that wounded people (both civilians and military) where “out of the game” – a kind of “gentlemen agreement”. In recent times, many terrorist actions directed against hospitals (i.e. in Iraq or India). This represents a shift in tactics and hospitals might now become the “ultimate soft target”. If you deprive hope from the wounded or the contaminated by making hospitals unavailable, then terror produced will be highly multiplied and “death” would be the next logical step to anticipate.

Other factors in targeting selection include the high degree of surprise resulting in mass panic and societal paralysis, the drama of the attack, the presence of mass media that will spread fear in all directions, and the ability to repeat the attacks causing a pathologic status of “endemic insecurity[14]” affecting both the populace and the governors.

CHAPTER TWO – New emerging threats

CBRN threats' overview

Before the World Trade Center attack in 2001, the abbreviation "NBC" was really meant "**N**o**B**ody **C**ares". This was a common joke among defense people who never expected to be confronted with the terror of WW I. Not even the chemical attack in Tokyo (1995) motivated international civilian and military communities to take pre-emptive actions against emerging threats. After "9-11", "NBC" gradually transformed to "CBRN" according to possibility of application and recently modified to CBRNE with "E" deriving from "Explosives" that are expected to accompany the release of weapons of mass destruction.

There are reports for use of chemical substances in the histories of many civilizations such as the Chinese, the Greeks and Byzantium ("liquid fire"). During WW I, it was the Germans who surprised Allied forces by releasing chlorine gas during the Battle of Ypres (1915). In the next two years, 1.2 million casualties were attributable to chemical warfare resulting in more than 90.000 deaths[15]. Although available in both sides, CWAs were not used in WW II.

Throughout the remainder of the 20th century, chemical weaponry continued to be developed and used in certain conflicts around the world (Persian Gulf War, Iran-Iraq War).

In 1993, the Chemical Weapons Convention (CWC) was finalized. This treaty prohibits the development, production, stockpiling, and use of chemical weapons and provided for the verification and destruction of known stockpiles. The Organization for the Prohibition of Chemical Weapons (OPCW) was set in 1997 in The Hague to supervise CWC. Currently 188 nations, 98% of the global population, have joined the OPCW[16]. Israel and Myanmar have signed but not ratified CWC while five states (Angola, Egypt, North Korea, Somalia, Syria) have neither signed nor acceded CWC.

Chemical terrorism

Chemical Warfare Agents

According to OPCW the term chemical weapon is applied to "any toxic chemical or its precursor that can cause death, injury, temporary incapacitation or sensory irritation through its chemical action. Munitions or other delivery devices designed to deliver chemical weapons, whether filled or unfilled, are also considered weapons themselves[17]."

The most well known chemical weapons are: choking agents – chlorine and phosgene, blister agents – mustard and lewisite, blood agents – hydrogen cyanide, and nerve agents – sarin, soman, VX. Some toxic chemicals, and/or their precursors, are of dual usage – especially in industry worldwide. Only in the case that they are produced and stockpiled in amounts that exceed requirements for those purposes they are considered as chemical weapons.

Under the term "toxic industrial chemicals" there is a wide variety of substances used in large quantities in the chemical industry such as acids, ammonia, bases, chlorine and other inorganic substances. Toxic industrial chemicals are manufactured, stored, transported, and used worldwide. They can be in the gas, liquid, or solid state. These substances can be chemical hazards or physical hazards if accidentally or deliberately released. The US National Environmental Law Center reported that "34,500 accidents involving toxic chemicals were reported to the EPA's Emergency Response and Notification System between 1988 and 1992, meaning that on average, a toxic chemical accident was reported nineteen times a day in the United States, or nearly once every hour[18]."

The most well-known chemical accident is the one that took place in Bohpal, India (1984), where methyl isocyanate was released in densely populated areas causing the death of 3.800 citizens and producing disabilities to more than 11.000 individuals[19].

Pulmonary (chocking) agents

Phosgene, chlorine, ammonia, hydrogen sulfide and hydrogen chloride belong into this category. Many of these agents are widely used in modern chemical industries (plastics, pesticides) and are most commonly involved in industrial chemical releases.

Phosgene is a white to pale yellow gas that smells like mown grass or musty hay. Chlorine a greenish gas smells like bleach while hydrogen sulphide smells like rotten egg. Latent period is usually within minutes to 48 hours. These gases are heavier than air and therefore accumulate in low-lying areas. They react with water in mucous membranes and produce corrosive substances, such as hydrochloric acid (chlorine, phosgene) or nitric acid (ammonia). Destruction of the alveolar-capillary membrane of the respiratory tract and leak of fluid in the interstitial tissue, results in ARDS.

Humans expose to these agents is by inhalation and skin and eye contact. In liquid form these agents may contaminate water or food and people can be exposed via consumption. Damage provoked depends on water solubility and direct tissue reactivity, dose and duration of exposure.

The diagnosis of pulmonary agent exposure is clinical. Management is mainly based on rapid decontamination.

There is no specific antidote.

Hemotoxic agents (bloo.d agents)

Cyanide, cyanogen chloride, cyanide salts (sodium or potassium cyanide) belong to this category.

Cyanide was also manufactured between WW I and WW II and has been used in concentration camps and in the Iran-Iraq war in the 1980s; also for assassinations and suicides. It is widely used in the industry (plastics, fertilizers, photography); it is also a combustion product elicited in house fires, considered to play a significant role in smoke inhalation morbidity.

It is a colorless gas or white solid that smells like bitter almonds (only some people are genetically predisposed to smell it). It provokes symptoms immediately (seconds to minutes). Gases are lighter than air and very volatile in liquid or solid salts' form. Chemical asphyxiants replace oxygen in the hemoglobin molecule and inhibit oxygen transport to the cells causing tissue hypoxia. Certain cyanide salts may also be corrosive to skin and eyes.

Human exposure is by inhalation (gas), skin and eye contact (liquid or solid) or by ingestion. Damage depends on route of exposure, concentration and duration of exposure.

Diagnosis is based on blood cyanide levels. Decision to administer antidotes is clinical and should not await test results.

Management of casualties depends on rapid dry (clothes' removal) or wet decontamination.

There are cyanide antidotes available (dicobalt edetate or sodium nitrate with sodium thiosulphate). Cyanokit® is the only FDA-approved emergency antidote[20] (hydroxocobalamin) indicated for both known and suspected cyanide poisoning.

Vesicants (blister agents)

Members of this category are mustards (nitrogen and sulphur) and organic arsenicals (lewisite, phosgene oxime).

Vesicants were manufactured as chemical weapons between the two world wars and mustards were used in the Iran-Iraq war in the 1980s. These agents are not used in industry, but quantities of them still exist in the arsenals of various countries and are under the process of destruction.

Lewisite may smell like geraniums while mustards may smell like garlic, fresh onion or mustard. The latent period for lewisite is immediate; for mustards it is more delayed (4-12 hours). It is important to know that these two agents can be mixed in order to produce both early and late symptomatology.

Vesicants are oily volatile liquids, pale yellow to amber that in gas form are heavier than air and accumulate in low-lying areas. They cause tissue damage by alkylation, similarly to radiation, affecting all rapidly replicating cells (cell death).

Human exposure is due to inhalation (gas), absorption through intact skin, eye contact with liquid or gas and ingestion (rare).

Damage depends on concentration and duration of exposure, humidity and environmental temperature.

The diagnosis is clinical. Urine mustard metabolites (thiodiglycol) may be measured in specialised laboratories; also urine arsenic levels after suspected exposure to lewisite. Laboratory tests can be used at a later stage to confirm exposure and should not delay treatment or treatment decisions.

Rapid dry/wet decontamination is critical.

There is NO antidote for mustards. In contrast, there is a specific antidote for lewisite (dimercaprol or British Anti-Lewisite [BAL] or alternatives: 2,3-DMSA and 2,3-DMPS).

there is clinical suspicion of exposure and pulmonary oedema, chemical burn with history of late decontamination (>15 min from exposure) with skin damage >5% BSA. Do not patch eyes; instead administer atropine eye drops for blepharospasm and ophthalmic ointment to prevent eyelids from sticking together. Usual burn care for the skin damage (analgesia, debridement, dressings)

Nerve agents (cholinesterase inhibitors)

Two categories available: "G-agents" (tabun, sarin, soman, cyclosarin) and "V-agents" (VX, Russian VX).

Nerve agents are extremely toxic chemical weapons and were manufactured between world wars. They were used in the Iran-Iraq war in the 1980s and during terrorist attacks in Matsumoto (1994) and Tokyo (1996). They are not used in industry, but quantities of them still exist in the arsenals of various countries and are under the process of destruction. Organophosphate pesticides in general have been banned from use in the EU, but accidental or deliberate (e.g. suicide) exposures are not uncommon.

G-agents are clear, colorless liquids, odorless or may smell kind of fruity. V-agents are brown oily liquid at room temperature and are odorless. Both categories act immediately.

Nerve agents are volatile liquids, colorless to brown at room temperature. As vapors are heavier than air and accumulate in low lying areas (i.e. basements). They act similarly to organophosphate pesticides by inhibiting acetylcholinesterase enzymes, causing extreme cholinergic stimulation of CNS, and peripheral muscarinic and nicotinic receptors dysfunction by the accumulating acetylcholine.

Human exposure in due to: inhalation (gas or aerosol), absorption through intact skin, eye contact with liquid or gas or ingestion (rare).

Damages provoked depend on route, dose and duration of exposure. Progression of symptoms should alert medical staff for continued exposure, inadequate decontamination or inadequate treatment.

Diagnosis of nerve agents' exposure is clinical. Laboratory tests (red cell cholinesterase activity, plasma cholinesterase), can be used at a later stage to confirm exposure and should not delay treatment or treatment decisions.

Rapid decontamination is critical.

There is combined treatment available (atropine [large doses], pralidoxime and benzodiazepines) and should be administered as fast as possible.

Japan – Sarin gas attack in Tokyo's subway

In Tokyo, approximately three million workers and students travel daily via subway. On Monday morning (07:55) of March 20th, 1995 the terrorist group of Aum Syrinkio organized and executed the release of nerve agent sarin into five subway cars on three separate subway lines passing through Kasumigaseki (home of police HQ) and Nagatachō (home to the Japanese government).

St. Luke's International Hospital was in closest proximity to the subway stations attacked[2]. At 08:16 the hospital's administration was alerted. At 08:16 first subway victims arrived at the Emergency Department complaining mostly for eye pain and dim vision. Until 09:20, more than 500 patients arrived (in total 640 within 75 minutes following alert call). More than 100 physicians **of all medical specialties**, 300 nurses and volunteers were available to provide health care.

During the time subway incident took place, in the hospital there was a television crew to film the opening of a new hospital's ward. Their film documentary[22] vividly shows that hospital personnel dealed with chemical casualties in the usual way they would react if confronted with a highway car accident. No precautions, no decontamination, no personal protective equipment for the EMS personnel. There was delay in confirmation of the nature of toxic substance; no sufficient antidote stockpile was available. In general, these people had no idea of what they are dealing with in order to provide specialized care and protection. The same applied for first responders and health providers escorting casualties to the hospital (secondary contamination en route due to closed windows).

In total, 13 commuters were killed (two of them at the hospital), 640 presented in the hospital and more than 5.000 people required emergency medical evaluation (worried well) in **169 hospitals[23] all over the city**.

It is also important to note that victims arrived at the hospital by ambulances (10%), minivans of Fire Defence Agency (5.5%) and **by non-medical vehicles (84.5%)**[24]. Perhaps the most important consequence, other than the shock of the highly industrialized Japanese society, was the fear provoked regarding the safe usage of mass transportation means. This fear is still present (personal remark), especially during the rush hours when commuters are "packed" into subway cars.

Radiological terrorism

Analysis of radiological threats – radiological disperse devices

Radiation is a type of ionizing energy, emitted by certain materials which cannot be detected by human senses. It is important to differentiate between a nuclear and a radiological event. The first results from the fusion of atoms, which produces a significant and highly destructive wave of heat, light and radiation. The latter may involve an explosion and release of generally smaller amounts of radiation compared to a nuclear event.

The radiation injury depends on the dose of radiation received, the type of radiation (alpha, beta or gamma) and whether the exposure involves internal or external contamination.

All types of radioactive sources or material used for industrial or medical purposes pose radiological threat and may result in a radiological emergency. Such events may involve the misuse of abandoned sources, transport emergencies, accidental leaks or spills of radioactive material or intentional use of radioactive material in conjunction with explosives (Radiation Dispersion Device – RDD or dirty bomb).

Effects of radiation are visible with minutes or days after the exposure, depending on the dose of radiation absorbed. Radiation acts directly on tissues and causes biological changes (tissue water becomes ionized and by creating free radicals it binds to proteins, enzymes and other molecules resulting in biological changes). The effects of radiation on live cells are either *stochastic* (the dose is related to the increasing possibility of occurrence of an effect – carcinogenesis, genetic effects) or *non-stochastic* which are directly dose-dependant.

Radiation exposure occurs when this particular type of energy penetrates the human body to cause its effects. Factors determining exposure to radiation are mainly: time (shorter time means shorter exposure), distance (the longer the distance from the source means less exposure) and shielding (barrier between the body and the source). Internal contamination signifies inhalation, ingestion or contamination of open wounds with radioactive dust or other material. External contamination implies the existence of radioactive dust or other material on the skin, hair or clothing of the exposed.

Acute radiation exposure in high dose, usually in short time, on large body surface area to penetrating radiation, results in acute radiation syndrome (ARS). Symptoms occur in 4 phases: prodromal, latent, illness, recovery/death and highly depend on the amount of the absorbed radiation dose.

Radiation can be detected only by specific equipment (i.e. Geiger counter). Radiation detected on nasal or oral swabs indicate internal contamination by inhalation or ingestion. Complete blood count with white cell differential to monitor absolute lymphocyte count is a reliable method of clinical follow-up.

Management of radiological casualties is based on decontamination with simultaneous measurement of radiation levels. It is mandatory to remove victims from the area of exposure. Equally important is the removal of the radioactive agent from the patient. In certain cases may need to repeat washing until radiation level is twice the background or remains unchanged. Decontamination of contaminated victims should be done as soon as possible but it should NOT delay or interfere with life threatening interventions. Individuals who have been exposed but are not contaminated do not require decontamination.

In the event of internal contamination specific agents may be available to dilute or compete with their radioactive counterpart or help eliminate specific radio-nuclides (i.e. potassium iodide for radioactive iodine to protect the thyroid gland, Prussian Blue for radioactive thallium or caesium, DTPA for plutonium and americium, deferoxamine for plutonium and iron, stable strontium, calcium, zinc and iron to compete with the respective radioactive elements). Diuresis facilitates the removal of tritium, as well as radioactive sodium and potassium; gastric lavage and cathartics may also be needed for the excretion of the radioactive agent. Frequent reassessment and monitoring blood tests, is usually required. General supportive care is equally important (analgesia, symptomatic treatment for nausea, vomiting and diarrhoea, aggressive prevention/treatment of infections, use of haematopoietic growth factors). In whole body exposure, surgeries need to be performed within 48 hours or after recovery of the bone marrow.

United Kingdom: Alexander Litvinenko's incident

Alexander Litvinenko, aged 43 years, a former officer of the Russian Federal Security Services, escaped prosecution in Russia and received political asylum in the United Kingdom. Through his books, «*Blowing up Russia: Terror from within*« and «*Lubyanka Criminal Group*«, he severely accused his former employees for terrorism acts aiming to bring candidate Vladimir Putin to power. On 1 November 2006, he suddenly fell ill and was hospitalized at the Barnet Hospital[25]. He died three weeks later (November 23rd), becoming the first confirmed victim of lethal polonium-210-induced acute radiation syndrome. According to attending physicians "Litvinenko's murder represents an ominous landmark: the beginning of an era of nuclear terrorism[26]."

Litvinenko was poisoned by consuming contaminated tea. Polonium was identified as the cause of death only a few hours before he passed away since this isotope emits only alpha particles and hospitals had radiation equipment directed to gamma rays specifically. Alpha radiation can be stopped by a sheet of paper and of course by intact human skin. If digested or inhaled polonium interferes with living cells like a "short range cellular weapon". The dose administered was calculated to be about 10 micrograms (200 times the median lethal dose of 238 μCi).

Health Protection Agency's scientists followed all possible paths of contamination within British territories by mapping all contacts and places visited by the victim itself and the people he met before becoming sick[2]. A reference contamination level of 10 Bq cm^{-2} was proposed by HPA for monitoring and decontamination. Levels of contamination below this value do not need remediation on health grounds, although it is good practice to remove contamination where this is easily achievable[28].

The social impact of this "first" "dirty man" was immense. State agencies were overwhelmed by worried well in both notional and international level. It was further magnified when British Airways published a list of 221 flights of a given "contaminated" aircraft involving 33.000 passengers from 52 countries (including Greece). The cost of incident management and monitoring by the Department of Health has been estimated to 2 million pounds[29]. If these are the consequences of one man contaminated with a radioactive isotope, it is more than easy to imagine what will happen in case of detonation of a dirty bomb in a megapolis environment…

Dirty bomb

Dirty bomb is a simple IED that can be constructed by combining conventional or high explosives (i.e. RDX, C4) with a small quantity of a radio-isotope. The result would be not too many casualties attributed to the explosion itself but the radio-contamination of extended areas within city limits (i.e. commercial or financial centre). These areas will resemble "ghost towns" of Wild West era in the United States. Construction materials absorb all kind of radiation and decontamination is very difficult not to say impossible. The economic cost to decontaminate and the financial disturbance in daily activities will be enormous with direct implication to the state itself.

So far there is no dirty bomb explosion recorded worldwide. But there are certain worrisome incidents[30] that must be taken into account since they underline the fact that the "threat is real!"

- **November 1995 - Moscow, Russia**: A Chechen terrorist group announces through a television station its ability to construct a dirty bomb. In order to prove this they give directions on how to find the IND buried in Ismailovsky Park in Moscow. A container with caesium was recovered…
- **December 1998 - Argum, Chechnya:** Chechen Security Service announced

that a container with radioactive material attached to a mine was hidden near a railway line 10 miles from capital Grozny.

- **June 2001 - Kandalaksan, Russia:** Illegal entrance to a nuclear-powered lighthouse in isolated coastal Murmansk County resulted in hospitalization of two people due to high strontium exposure. There are 132 similar lighthouses which are currently unguarded and lack of regular inspection …
- **December 2001 - Lja, Georgia**: Woodcutters or border frontier guards found abandoned two heat-emanating containers that thought to be used for heating purposes. After a few hours the eleven men felt sick and went to local hospital. The International Atomic Energy Agency revealed that each container used in radio-thermal generators during the Soviet era, contained 40.000 curies of strontium (emitting radiation equivalent to that following the Chernobyl incident).
- **June 2002 - Chicago, Illinois, USA:** Jose Padilla, a gang member with affiliation to al Qaeda was arrested in O'Hare Airport on suspicion of a dirty bomb plotting. He is currently detained.
- **January 2003 - Herat, Afghanistan:** Diagrams and computer files uncovered in the Herat Province by British intelligence agents pinpointed to al Qaeda and a small dirty bomb. Perhaps the isotope included derived from medical devices available unguarded at that time in Kabul. The device has not been found…
- **August 2010 – Chisinau, Moldova:** Police seized 1.8 kg radioactive uranium-238 and arrested a group of smugglers demanding 9 million euro[31].

According to the Nuclear Threat Initiative *"…in the United States alone, as of 2008, companies have reported losing track of almost 1,700 radioactive sources since 1998*[32]*."* The material is ready out there, waiting…

Brazil: The Goiânia's incident

In the end of 1985, scavengers stormed the abandoned Instituto Goiano de Radioterapia in Goiânia, Brazil and recovered a caesium-137 teletherapy unit thought to be of some scrap value. When attempted to dismantle the unit, the source capsule was ruptured. The remnants were sold to a junkyard owner who noticed that they "glow blue" in the dark. This "phenomenon" attracted many relatives and visitors and parts were distributed to several families. Then the problems began in the form of gastrointestinal symptoms not initially attributed to irradiation. When the connection with the scrap was evident, public health authorities were notified and involved.

The specialized team sent by the Brazilian Nuclear Energy Commission discovered that over 240 citizens were contaminated with caesium-137. Four of them subsequently died and 85 houses were significantly contaminated. During the process of land decontamination approximately 4.000-5.000 m^3 of waste material were encapsulated into 12.500 drums and 1.470 boxes[33]. More than 100.000 individuals (mostly "worried well") were tested for radiation in the national stadium of the city. Not to mention the economic impact for this tourist city or the disruption of the social web following the incident.

The Goiânia incident is **the closest resemblance to a dirty bomb so far**. One can only imagine the impact of the detonation of a "real" dirty bomb taken into account that the half life of the isotope caesium-135 and that of caesium-137 are 2.3 million years and 30 years respectively[34]!

CHAPTER THREE – Attitude of medical community towards new emerging threats

Is the medical community prepared and willing to deal with new threats?

Almost nine years after the hecatomb of blood in World Trade Center and the Pentagon in the United States, is the medical community prepared and willing to deal with new emerging threats? An optimistic observer might comment that although there are many things to be done, certain progress has been made especially in certain parts of the world. A pessimistic observer will categorically state that not many things have been done so far. A logical observer should note that current situation is in the middle. In that respect we must rely on the objective observer who will support his opinion with facts and figures. If this is the case, then the situation regarding medical/hospital preparedness to deal effectively with chemical and radiological terrorist threats is rather worrisome!

This complies with my personal view and it was the main drive to select this theme for my dissertation. During the 2004 Olympic Games in Athens, I served as CBRN consultant at the Olympic Games Safety Committee (OGSC). I recall the first meeting of the subcommittee on CBRN planning: seventy five entities, bodies and organizations – many were health-oriented – in a round table meeting. The first question was shocking: "what NBC acronym means?" My immediate thought at that very moment was: "We have a big problem to solve!" It was obvious that just a handful of CBRN experts – mainly from the military – had to educate all these people in order to be able to communicate with them. It took many months and endless meetings on various hot topics like the magnitude of the threat, the expected death toll, who is entering where, who is assisting whom, equipment and training issues, drills and exercises, acceptance of international assistance, international CBRN safety advisory board, personnel issues, organized professional unions' objections on role and involvement and many more.

The main objection was two-fold: First it was the inherent "logic" that "it will not happen to us!" This was accompanied by a similar "logic" that release of CBRN agents in a megapolis environment was too inhumane to happen! These basic "logics" were accompanied by the unwillingness of medical/hospital personnel (mainly physicians) to be involved in the management of CBRN casualties. Almost all of them rejected their involvement in "hot" and "warm" zones' operations since they had not the training required. Most of them thought that this was a job for the military physicians to do – as part of their military medicine training. A second point of traction was the fact that training in medical CBRN defense required a lot of reading, a lot of practical/physical training, new unfamiliar and uncomfortable equipment and frequent exercising both theoretical and field oriented. In fact it was like going back to their time of intern training for acquiring their medical specialty. And they did not need that! Young health professionals spent a lot of time and effort to become specialists. At that time, most of them were practicing their specialty in various hospitals and their private offices. They needed to invest into their training in order to achieve a better financial status for them and their families. If they were involved in medical CBRN operations, their plans should be delayed and that was not cordially accepted.

A second objection had to do with the post-Olympiad era. What if they stuck to this field of medicine and let their initial objective become a secondary job? Then it was the fact that they had to spend all summer-time period into training and stay alert in shifts during the Games. In addition, there was no allowance budgeted for their specialized involvement. In one hand there would be their colleagues who would enjoy their summer vacations or go to the Games and on the other hand would be them training, sweating, reviewing plans, make adjustments, work on their personal protective equipment, practice familiar techniques with unfamiliar rubber gloves or try to persuade their hospitals on the modifications that should be done in order to be able to protect their colleagues from possible contamination in a case of a real CBRN terrorist incident.

Lack of relevant knowledge multiplied their concerns and inner fears. They have never heard of nerve gases' effects, they have never seen mustard casualties; there was no relevant curriculum during their medical years' studies. Not to mention that most of the bibliography available on the Internet was in English (language barrier). Then they have never been in a protective gear ever.

I must admit that the first time in such a gear could be kind of traumatic. Increased respiratory resistance due to the filters attached into gas masks makes breathing difficult and laborious. Certain claustrophobic behaviors arise due to the isolation feeling when the mask is on. Operating with personal protective gear is affected by physical status, ambient temperatures and tasks to perform. Those who work in EMS departments are familiar with the stress they experience when dealing with conventional traumas. Add the additional stress of a contaminated blast victim to have a virtual picture of the imaginary tasks these people were asked to perform in an environment dangerous for their own lives as well. Physicians suppose to save ALL victims they are dealing with. It is their duty resulting from their Hippocratic Oath. But things in CBRN triage are totally different and difficult to be incorporated into their medical/ethical *modus operandi*. It looked inhuman to let people die in order to treat others with a better chance to survive!

These high-lights are some of the many that medical and nursing personnel had to face and learn to live with. Their concerns were well understood and tried to alleviate via explanation of the basics and by showing them that everything had to do with the right training. But most of them were not willing to participate because the main question into their mind was: "What is it for me?" This specialized training would not be an "add-on" to their curriculum vitae and it would not provide any future benefits; only "troubles" and "future responsibilities". Who is pursuing them in our modern self-centered times and lives any way? It was then, in a very critical turning point, that they (through their unions) threaten to go on strike during the Olympic Games. It was then that the state decided to involve military hospitals as Olympic Hospitals in order to deal mainly with CBRN casualties.

It was decided that Army General Hospital of Athens will be the core hospital with neighboring Air Force General Hospital to provide support personnel and absorb inpatients from Army Hospital in case of a real CBRN incident and Navy Hospital to provide logistical support. It was late January 2004 when I was asked to create a new hospital-based CBRN response unit.

Although military CBRN experts were strongly supporting the idea that there was a gap in the overall CBRN planning when comes to management of contaminated mass casualties, those responsible for the execution of the plan (mainly first responders: police and fire service) focused greatly on the "operational part" of the incident. It was well known from previous mega-terrorist events that the "golden hour" is a period that evaporates fast. In fact what can really be done is to cordon the area and try to evacuate walking casualties from the incident site. On the contrary, "medical operations" may last for many hours and even days or months.

When I participated in a medical-oriented course on the consequences of chemical weapons held by OPCW in Iran (2003), I was amassed when informed that more than 20.000 patients where in the follow-up program for victims of the Iran-Iraq war era in the 1980s! The course was held at the Baqiyatallah Military Hospital of Tehran. Within the hospital's premises, there is an outpatient clinic dedicated to chemical victims. Participants were given the opportunity to actively examined these patients and talk with them. It was a unique chance for a medical doctor to actually see a "mustard eye" or patients with "mustard scars" in their bodies. These patients were young during the chemical attacks of the past – even small children. Now they have to suffer for the rest of their lives due to the consequences of the inhuman release of chemical weapons in urban populace. It was also a good chance to discuss these items with specialized Iranian physicians with vast experience in management of chemical casualties. This is a "must" to participate course and I strongly recommend it to all medical staff involved in CBRN medical operations[35]. This experience was our strong point to support the opinion that medical CBRN operations should be equally supported – in vain.

Finally, OGSC realized the existence of the gap and ordered measures. I was given 67 people from the Army General Hospital and asked to "transform" them into an "Olympic Hospital CBRN Response Unit" that will be deployed in the parking lot of the hospital ready to deal with CBRN casualties during the mega-event.

People selected were not volunteers, many of them had families and children and all of them had no relevant experience or knowledge about CBRN agents. All the remarks made above about the general attitude of medical/nursing personnel regarding involvement is such operations were apparent during our first meeting at the amphitheatre of the hospital. Anger, fear, skepticism, objections, insecurity where among the many feelings filled the air during this first meeting. It was proven that military medical personnel were also not prepared for this kind of job. But the military had no excuse to turn this task down. It was the pride of the military medical corps that eventually over-run all objections and hesitations. At this point it is worthy to mention that motivation is very important for those involved in such operations. The point of view saying "*why don't you take as an example our colleagues in the United States, Great Britain or Israel who are doing their best to be prepared for events of this kind*" was confronted with the common belief that "*they are prepared because they are in contact with the enemy*". In that respect, "introduction to international terrorism" is a very effective tool to reverse this attitude by proving to the audience that "*what is thought to be very far away from us is in fact outside our doorstep*!"

After the first eight hours of introductory presentations on medical CBRN defense issues, all these feelings changed to a universal enthusiasm and all were eager to be actively involved in this new exciting field of expertise. Ignorance produces fear, lack of training produce fear as well. On the other hand, "knowledge is power" and practical training replaces doubts with certainty and confidence. Acclimatization with personal protective equipment greatly helps performance and overcoming discomfort derived from this type of protective gear. For my surprise female personnel proved to be more durable than males and more enthusiastic in fulfilling tasks.

In close cooperation with OPCW (activation of Article "X"[36]) and other foreign organizations, the unit's personnel was trained in several countries abroad, given the opportunity to absorb different training techniques and methodologies. This training created different groups within the unit who strongly support their training against that of others. There was the "Swiss Group", the "British Group", the "Czech Group" and so forth. But all of them eventually compose their expertise to construct a new "Greek Know-How" that would be suitable for the Olympic Games. Through countless exercises, in different ambient temperatures, personnel were acclimatized to the difficulties of summer time operations. The entire unit cooperated closely to finalize the response plan. We followed the principle that a plan should be short, clear and effective. Multi-pages plans are nice when on library selves; it is of no use if something real appears. One must always have in mind that "*no plan stands in front of the enemy!*" Flexibility is a "must to have" ability in order to overcome difficulties and surprises. Leadership during that time was also a big challenge. The model of "personalized command" was chosen and it worked efficiently. In fact it was a combination of "authoritarian-participative-delegative" command styles addressing personalities and problems in a personal manner.

A surprising element that arose during that preparatory period was the fact that many hidden adventurous personalities came to the surface strengthening the view that people involved in extreme situations or activities, have personalities slightly deviating from what is broadly characterized as "normal". Most of the times, these personalities are trapped in daily reality and routine. The so-called "T-personality" ("T" from "Thrill seeking") might be a useful tool in selective the right people to do this job. According to Ron Watters[37]:

> *The world has become far too safe, and heretofore unknown lands are mapped in far too much detail. As a consequence, we need as many outlets as possible for people to participate in challenging outdoor activities. We need wilderness lands; we need rock climbing areas; we need wild rivers; we need outdoor schools, and given proper environmental safeguards, we need free and unfettered access to outdoor areas. The right to risk is unalienable. It makes our society healthier and more vibrant.*

To establish more sophisticated selection criteria, one might take advantage of the work of Ernest Noble's group on prevalence of dopamine D2 and D4 receptors associated with risk-taking behaviour[38] (D2 gene: 20% of people, D2+D3 genes: 30% of people). Future controlled studies on dopamine receptors in CBRN personnel might reveal surprising results.

From all the above, it is obvious that although medical/hospital personnel are neither ready nor willing to participate in medical CBRN operations, knowledge, continuous training, acclimatization and motivation can change this attitude for the benefit of the societies in danger.

Current situation in the United States

The United States declared "war against terrorism" soon after the September 11th, 2001 terrorist attack in New York. One might assume that nine years after this momentous date, this country should be medically shielded against new emerging threats. Current situation is presented below through a series of scientific papers collected from US National Library of Medicine, National Institutes of Health (PubMed.gov):

In 2001, Wetter et al studied hospital preparedness (224 hospital emergency departments in 4 north-western states) for victims of chemical or biological terrorism. They concluded that "*Hospital emergency departments generally are not prepared in an organized fashion to treat victims of chemical or biological terrorism. The planned federal efforts to improve domestic preparedness will require substantial additional resources at the local level to be truly effective*[39]."

In 2002, Mann's group studied public health preparedness for mass-casualty events in all 50 states focusing in planning, coordination, training, resource capacity and preparedness for chemical/biological terrorism[40]. Most states had a disaster plan (94%) but only a few (38%) had a bioterrorism component. Personal protective equipment was lacking in 49 states and only 10% of hospitals in all states had decontamination facilities. Therefore, the group concluded that:

> *These findings suggest that disaster plans are prevalent among states. However, key programs and policies were noticeably absent. Communication systems remain fragmented and adequate training programs and protective equipment for health personnel are markedly lacking. State-wide trauma systems may provide a framework upon which to build future medical disaster readiness capacity.*

Higgins, Wainright, Lu and Carrico in 2004 assessed preparedness for mass casualties' events in short and long-terms hospital in a single state by employing the Mass Casualty Disaster Plan Checklist[41]. Their comments were as following: "*Hospital mass casualty preparedness efforts were in an early stage of development at the time of this survey, and some critical capabilities, such as isolation, decontamination, and syndromic surveillance were clearly underdeveloped. Preparedness planning was more advanced among hospitals located in counties participating in Metropolitan Medical Response System Program.*"

In 2005, the study of Niska and Burst focused in bioterrorism and mass casualty preparedness in US hospitals as part of the annual National Hospital Ambulatory Medical Care Survey[42]. Main results: (1) most hospitals had plans for dealing with new emerging threats (chemical – 85.5%, biological – 84.8%, radiological/nuclear – 77.2% and explosives – 76.9%), (2) Hospitals' percentages of training their staff in any kind of exposure ranged from 92.1% (nurses) to 49.2% (medical residents), (3) Although explosions are the most common form of terrorism, drills for these incidents were staged by only one-fifth of hospitals.

The possibility of a terrorist attack employing the use of chemical or biological weapons of mass destruction (WMD) on State of Mississippi was explored via a questionnaire survey by Bennett in 2006[43]. According to his findings state hospitals scored well in education and training (89.2%), decontamination facilities (75.7%) and pharmaceutical stockpile (56.8%). Hospitals scored badly in increasing surge capacity (59.5%) and laboratory diagnostic services (91.9%). In conclusion:

> *…hospitals in the State of Mississippi, like a number of hospitals throughout the United States, are still not adequately prepared to manage victims of terrorist attacks involving chemical or biological WMD which consequently may result in the loss of hundreds or even thousands of lives. Therefore, hospitals continue to require substantial resources at the local, State, and national levels in order to be «truly» prepared.*

Reilly, Markenson and DiMaggio conducted in 2007 a similar state-wide study on EMS personnel preparedness[44]. Their results indicate that:

> *Lack of training and education as well as the lack of necessary equipment to respond to WMD events is associated*

> *with decreased comfort among emergency medical services providers in responding to chemical, biological, and/or radiological incidents. Better training and access to appropriate equipment may increase provider comfort in responding to these types of incidents.*

These studies and many others available in medical bibliography support the overall impression that although many things have been done, much more needs to be done.

Current situation in European Union

Six EU member-states (Bulgaria, Czech Republic, Germany, Greece, Poland and the UK) participated at the ETHREAT (European Training for Health Professionals on Rapid Response to Health Threats) consortium representing highly specialized organizations and institutes on public health issues. The National and Kapodistrian University of Athens was responsible for the management and coordination of the project (2005-2008) as well as for the cooperation of the whole partnership with the European Commission (Directorate for Public Health), which co-financed the project. I participated in this project as CBRN consultant.

The final product of ETHREAT Project was to create a manual aiming to assist training institutions, universities and public health authorities in the education of health professionals, so as to enhance the European human capital on the timely identification, the management and response to events that could be the result of deliberate attacks with the use of biological, chemical and radiological agents.

Moreover, the project team explored the opinions of their target audience and of European experts on the existence and appropriateness of currently available programmes, as well as the desired content of an educational package by surveying front line health professionals (FLHP) and PH and CBRN experts in the European Union (EU) member states (MS). An outline of the major findings from the questionnaires disseminated is presented in Appendix A.

During the 2006 annual conference of the 14th European Public Health Association and following oral presentation of the ETHREAT Project, we concluded[45]:

> *Our results reveal a gap in the base of medical CBRN defence in all EU countries at the level of front line health professionals that will deal first with WMDs casualties in urban environment. Therefore, emphasis will be placed on strategies for the diffusion of the final educational material in all the 25 member-States and particular to the students of medical and nursing schools with final aim the incorporation of the relevant material to the last year of medical and nursing studies.*

CHAPTER FOUR - Medical defense against chemical-radiological terrorism in urban environment

Hypothetic scenario

13:00 – *In a busy multi-store shopping mall people start falling down with convulsions and frothy saliva coming out from their mouths. People panic and call the police. Police crew that arrived on site experienced similar symptoms. Head of mall security calls police HQ and give a brief description of the incident. First responders arrive at the incident site after 30 minutes. An explosion takes place at the parking entrance of the mall where responders were gathered ready to enter the complex.*

14:00 – *A second explosion is heard from the area in front of the Parliament where change of guard is taking place and hundreds of tourists are watching. A second wave of first responders is directed to the new incident area. Automatic radiation detectors alarmed for high radiation levels. It was a dirty bomb…*

One might say that a combined chemical-radiological-explosion terrorist attack is kind of science fiction. It might be; but it is better to hope for the best and prepare for the worst. A logic concept that we tend to forget when planning for disasters that might happen to us as well!

Important clarification: Following directives and proposals are valid for a CBRN incident that evolves in a randomly selected urban area. In case of known targets (i.e. during the opening ceremony of Olympic Games), the deployment of forces and mode of action (triage, decontamination, evacuation etc) is totally different and it is not within the scope of this paper. Also, the contaminated plume generated in this realistic scenario is expected to be limited affecting only a few blocks' area compared with other forms of CWAs release (i.e. chemical munitions, multiple chemical attacks in subway system etc).

At the incident site

Three important statistics

To start with it is important to memorise **three important numbers**[46]: Approximately **10-20%** of the people at ground zero will stay there because they are dead or severely contaminated and/or wounded. The second number to remember is that approximately **80%** of the people involved in the incident will flee to every possible direction – including those with minor lessons and mild contamination. They will panic and will be directed to all medical facilities available in this area or near their residence – perhaps later on depending on the agent released. The third import number is the varying ratio **"1:5"** regarding "contaminated vs. worried well" individuals that will soon overwhelm hospitals' surge capacities[47]. These numbers are critical in CBRN response planning because they represent normal reactions of people involved in a catastrophe. An equally important issue is that CBRN planners must have personal training and experience in all levels of PPE. It is common practice "people who know things not to sign and those who sign not to know things from inside!" Just theory is as dangerous as the threat society itself is facing.

Golden hour

People evacuating the incident site in combination with the explosions' effects will create traffic chaos in an area of many blocks surrounding the attack area. Soon traffic will come to a stop and there will be no free lanes for first responders to move in order to approach the hot zone. Massive fire engines, police cars, ambulances, mobile decontamination units might be available but they will be "sitting ducks" unable to arrive on time. And time defined as the "golden hour" is critical since it is "*the hour immediately following traumatic injury in which medical treatment to prevent irreversible internal damage and optimize the chance of survival is most effective*[48,49]*."*

Although this definition derives from conventional accidents, military battlefields or urban terrorist attacks, it is of value for CBRN incidents as well. The difference is that in case of CWA release it might be "golden minutes" instead of "golden hour". So it is taken almost for granted that first responders and specialized medical units will arrive late to assist those that will remain on site and most probably they will be dead on arrival. Perhaps the only good solution available for urban environment is that of the Israeli "Magen David Adom" (national emergency medical, disaster, ambulance and blood bank service). Part of their first responders crews are on motorcycles that can penetrate heavy traffic fast and arrive on time at the incident site.

First responders at the incident site

Hypothetically, first responders do arrive at the incident site on time. What will be their medical contribution to the victims on the spot? For the reasons already described: minimal to none. The main problem is that nobody knows the nature of the agent released. Common practice is to enter hot zone with totally encapsulated gear (Level "A"). Common objection is that when **in Level "A"** the window from donning to doffing is approximately 20 minutes (maximum 40 minutes). The main objective of this team is to go in, evaluate the situation and report, activate their detectors and report, take samples (if possible) and then get out. It is almost impossible to practice medicine on site, to carry loads of possible antidotes, stop bleeding, support ventilation and carry stretchers for the wounded or contaminated victims. The only reason for justifying the presence of medically qualified personnel (fire or police medics) inside the hot zone is to provide assistance to first responders themselves in case someone is wounded by falling debris, fire from remaining terrorists, secondary explosion aiming first responders or accidental tearing of PPE thus exposing responders to contaminated environment.

It is of note that if police crew practice the **"1-2-3" rule** (one person down is normal might be a hear attack or just faint, two people down proceed with cautious, three and more down step aside, secure perimeter, report and wait for assistance) upon arrival they might be alive and able to assume duties mainly by directing panicked people out and securing the perimeter until more forces arrive on site. It would be also ideal if they had personal **escape hoods** that would have protected them from the agent released and would provide them enough time to do their job safely[50].

At the hospital

Casualties seek medical assistance

People escaped from the incident site will return to their homes or rush to the nearest hospital available. If the hospital is very close to the incident site it would be caught by surprise – especially if they have not notified in advance (common practice). With zero reaction time, even if the hospital has the proper structures, personnel, PPE, plan and procedures, frustrated crowd with rush into EMS premises demanding medical assistance. Depending on the agent released this might lead to the contamination of EMS personnel or even other areas of the hospital. The basic principle "save the savers to operate" will be compromised in just a few seconds. A second problem in near by hospitals is the fact that they have not enough security personnel to control the crowd and in many instances not a perimetric fence to forbid unauthorized entrance into the hospital area. But even if there is a fence it might be jumped over by people who believe that their lives are at stake. Security personnel are valid for daily routine and car/visitors control but totally insufficient when dealing with many people some of which are contaminated. They do not have PPE, they lack specialized training, they do not know how to protect themselves while on PPE. Most probably they will run away to save themselves.

Hospitals that are located far away from the incident site might also be caught by surprise if they speculate that casualties will go the nearest to the incident's site, hospital. In Tokyo (12.3 million inhabitants) ALL hospitals and clinics accepted more than 5.000 casualties from the sarin incident at the metro system. In that respect all hospitals within megapolis' limits must be prepared to deal with CBRN mass casualties. An alternative might be to shut down those hospitals that lack resources to deal with such emergencies. It might sound unethical but life will continue in the aftermath of the incident and health is a mandatory asset for the society. Another expected phenomenon would be all casualties to rush in the near by hospital while at the same time, another well prepared hospital but in a lesser proximity, might manage no casualties at all! Therefore casualties' guidance and redirection is as important as medical assistance itself.

Casualties arrive at the hospital

Following the Tokyo incident, more than 85.5% of those involved arrived at the hospital with their own cars, taxis, mini-vans or even buses. So there is no need to send vast numbers of ambulances at the incident site. They will serve better if they provide assistance to the one or more hospitals that will be overwhelmed with casualties. It is of note that ambulances windows must keep their windows open to dissolve further the contaminants absorbed on victims' clothing.

Hospital security

Hospital must be secured by sufficient police forces in PPE who have relevant training. It is important police forces to be there well in advance before first casualties arrive.

Hospital's CBRN Response Unit

This is the biggest problem in all CBRN plans and directives. Should it be permanent or deployable? What is the best composition of such a medical team? What should be the motivation to participate? What would be the criteria for selection? Who will cover equipment and training expenses?

From what it has already been mentioned above, the nature of the incident dictates hospital to have a dedicated CBRN response team that will operated in fixed installations outside the main building of the hospital. This might be possible for hospitals in close proximity to chemical plants or major targets. Although it is ideal, hospitals' authorities consider it as loss of people, resources and time.

A second option might be to train and equip all the personnel involved in EMS departments. This is a more realistic approach but certain individuals might fail to operate under PPE mainly for various reasons (i.e. age, fitness, medical conditions, etc). This is the best proposal taken into consideration that decontamination facilities for both walking and ambulatory casualties will be fixed and ready. Then all that it takes is the time to don and this can be minimized by continuous training and acclimatization to PPE.

EMS CBRN Response Unit

By choosing the latter option what must been done next is to make a response plan that will be proportionate to the available personnel and the duties they have to perform. This will determine the type of equipment that must be purchased. It would be wise to have a commn *modus operandi* that will be practiced by all medical facilities nation-wide. In that respect there will be compatibility of equipment and homogeneity of training and standard operational procedures.

Duties

The EMS CBRN Response Unit must have a single operational goal. That is to contain contamination outside the hospital's premises. They will become the barrier between the contaminated outside environment and the inside of the hospital where their colleagues will continue to operate safely without PPE and in support of the Unit. It must be clear to all that a "clean" chemical or radiological casualty can be handled thereafter safely and "as usual".

Main duties to be performed at the hospital parking lot or other suitable area (Figure 1):

NOTE: This area is considered as gradually contaminated area (warm zone)

(1) Initial detection of incoming casualties (Detection Station)

All incoming casualties are scanned for possible contamination. Chemical/radiological contamination detection time depends on the number of incoming victims. If they are only a few modern detection equipment can be

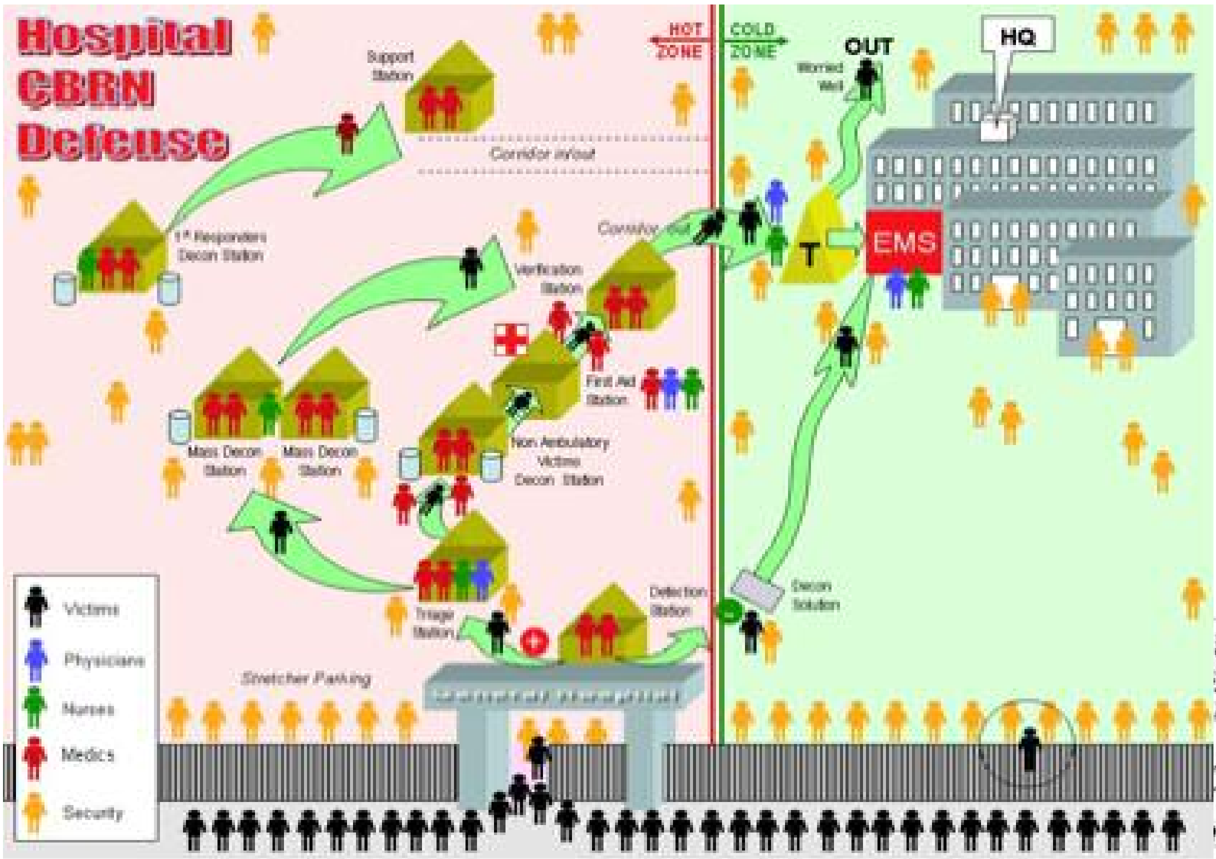


Figure 1 – Hospital CBRN defence plan – Working Stations

used. It is of note that detection takes some time to accomplish and it should be done in specific mode from head to toe. If the victims are many and in order to avoid overcrowd in the main gate of the hospital, simpler but equally effective CWAs' detection can be done by using special chemical colorimetric papers that indicate exposure or not. These self-adhesive papers can be stacked onto mouth pieces for single usage. If the incomer has been declared "clean" he follows security personnel to a "decontamination tank" containing a solution that will clean any small amounts of agents from his shoes. Then they proceed to the EMS department. If the incomer has been declared "contaminated", he is given further directions to proceed to the Triage Station. Both procedures are applied to non-ambulatory victims as well

(2) Triage of incoming casualties (Triage Station)

All "contaminated" incomers are passing through Triage Station. If they are walking victims or those with minimal injuries are given instructions, to proceed to the Mass Decontamination Station. If they on stretchers, CBRN triage methodology is applied. Most preferred system is the START (Simple Triage and Rapid Transport) triage system[51] that classifies victims into certain categories of medical priority ("immediate", "delayed" and "deceased»). On each victim a paper (Japan) or plastic (Israel) triage card of different colour is attached. If plastic, information about the victim can be recorded by punching holes in them using a finger[52].

In 2007, Japanese researchers proposed a system that combines triage with cards under the name STARDOMCCP (Simple Triage and Rapid Decontamination of Mass Casualties with Colored Clothes Pegs System)[53]. This system employs ordinary inexpensive clothes pegs in 7 colours: Red (emergency care), Yellow (semi-emergency care), Green (non-emergency care) and Black (expected) while White is for dry decontamination (clothing removal) and Blue for wet decontamination. In each victim two pegs define its medical/decontamination status. Employing a more military style recording (Israel), triage personnel might use permanent (waterproof) pens to write directives/notes directly on the skin of the victim (especially important for doses of antidotes provided; also info stay with the victim all the way to EMS).

Many clinical triage algorithms' models have been proposed so far the optimal management of mass terrorist events' casualties. When EMS personnel have to deal with vast numbers of victims "the simpler is the better"[54]. Victims should be periodically re-evaluated for possible changes into their clinical/priority status.

(3) Decontamination of non-ambulatory (NA) victims (NA Decontamination Station)

This is the most difficult mission for the personnel involved since they will have to simultaneously manage contamination and (in many instances) conventional wounds. Record the victim and provide a wrist bracelet with a unique number (or barcode). Use same number to identify victim's valuables placed in double-sealed bags. If there are bandages applied in advance, remove them and replace them following copious irrigation of the wound. With water/saline or bleach? This is a controversial question; the main objective is to remove contaminants from inner tissues as soon as possible and as thoroughly as possible; both are effective[55]. Cut all clothes and dispose them. Proceed fast but carefully. If victim deteriorates during decontamination ask assistance from the near-by First Aid Station. Usually decontamination is performed on a special roller system that allows easy rolling of victim from one station to the other.

(4) First Aid provision to NA victims (First Aid Station)

One of the myths surrounding medical CBRN operations is that medical staff cannot perform while being into their PPE. Mainly because of the heavy rubber gloves that accompany this type of protective gear. The truth is that many things can be done with appropriate training and methodology. First personnel can replace rubber gloves with two sets of surgical gloves (white) and a third one (purple) on top of them. This method is safe for the saver and provides extra sensitivity and feeling. Replace purple gloves every five minutes or when a new patient arrives.

There are three procedures that are life-saving and can be done on site: provide antidotes (i.e. atropine [auto-injectors or regular vials for hospital usage), control bleeding (with the aid of haemostatic means (i.e. haemostatic sand in a sponge [Quiklot™ and similar] for single use) and support airways (remove excessive salivation blocking the airways (i.e. nerve agents) all the way to regular intubation. Following the latter, patient can be connected with breathing support apparatus or bag-valve-mask ventilator[56] (providing they have a CBRN filter attached – i.e. compPAC™ ventilator or AMBU™ Mark III Resuscitator). In fact, among the long list of first aid equipment supplied from the hospital (regular items), only ventilation support (above) need to be purchased separately.

For training purposes, the First Aid Station environment can be duplicated in a dedicated hospital simulation room ("tent-in-a-room"), where EMS personnel can be regularly trained[57]. In that respect, the Laerdal's latest SimMan™ 3G with NBC module and accompanying software could make the difference and are highly recommended.

(5) Mass decontamination of walking casualties (Mass Decontamination Station)

While waiting to be decontaminated, walking casualties must be asked to remove ALL their clothes (dry decontamination). This simple method can be live saving since it reduces contamination to minimum. Certain problems emerge during this procedure. Even if their life is at stake, certain people will refuse to remove them completely for their own reasons (physical condition, modesty, religion). There is no reason to insist on this. Rephrase your orders to "as many clothes as possible and desire."

Then it is the language barrier that might complicate things. Do not assume that all victims understand English. A good solution (but expensive) is to have electronic message boards that can show messages in many languages. Instead you can use inexpensive placards with multi-lingual messages.

Try to have the unclothing area as protected as possible (mass media are everywhere – even airborne!). This will be an add-on for victims to reluctantly discard their clothes.

Give clear instructions on the washing procedure and time. Stress the fact that hard brushing is no better than normal brushing that leave skin intact. Let families be together. Separate males from females. Record patients and give them a wrist bracelet with a unique number (or barcode) printed. Collect all their valuables and put them in double-sealed bags where same referral number is attached. In the aftermath, there will be many that will claim their valuable Rolex watch now missing… Let them have their eye-pieces, hearing aids or walking canes if they cannot function without them.

Have some nurses or medics to keep an eye on the victims during the decontamination process. Some might deteriorate during washing and need first aids or transfer to the First Aid Station. During hot weather conditions, decontamination can be performed with cold water (that reduces vasodilatation of skin thus reducing absorption[58]). If the incident takes place during winter time, warm water should be used to avoid hypothermic reactions. Provide a post-decontamination clothing kit (like those surgery personnel is using).

(6) Verification of decontamination for (Verification Station)

Following decontamination of walking on NA casualties, it is wise to confirm it by having victims check-out through Verification Station. Properly equipped personnel will detect if there is residual contamination present. If there is, individual must repeat the decontamination process again given priority. If there is no contamination present, individual is accompanied via the "out corridor" (warm/cold zones border) to the hospital main triage area for thorough evaluation and hospitalization if required.

(7) Decontamination line for first responders (First Responders Decontamination Station)

There is a standard operational procedure that cannot be surpassed by any means: **First responders DO NOT operate unless they have their separate decontamination line in place**. Personnel in PPE (various levels – "A", "B", "C"), cannot wait in line with victims waiting to be decontaminated – for obvious reasons. If operations going to last for many hours, it is advisable to deploy a collective protection (COLPRO) tent where personnel can rest, replace filters, hydrate etc.

Main duties to be performed at the warm/cold zones' border:

(8) Thorough triage of "clean" casualties (Hospital Triage Station)

The moment contaminated victim becomes "clean" then it can be handled as usual by EMS personnel without PPE being necessary. At the Hospital Triage Station patients will be hospitalized if this becomes apparent according to their clinical status. In the same area, a team of psychiatrists and psychologists will evaluate possible "worried well" individuals and direct them to return home this avoiding the overwhelming of the hospital[59]. It is clever to provide written instructions on "what to do" in case delayed symptomatology develops.

It is of note that "psychological desensitization" of all personnel involved in field medical CBRN operations is mandatory for their well being on the long run[60]. This is something that is usually forgotten even during the daily routine of an EMS department.

Radiological casualties

All the above apply for external radiological contamination following detonation of a dirty bomb in urban environment as well. Regarding internal radiological contamination certain specialized measures should be taken in cooperation with nuclear medicine and physics medical authorities of the hospital.

In that respect a special entrance for radiological casualties should be provided, personnel should have protection against radiation and casualties should be hospitalized in rooms or wards with radiation protection construction with autonomous ventilation/air-conditioning and bathroom facilities. The "good" thing (sic) is that a dirty bomb will produce relative small number of casualties depending on the explosives used and most of them will die immediately on site or waiting to be evacuated. The remaining of the casualties with minor injures but with inner contamination should be distributed to many hospitals with the above mentioned specifications (usually not enough to cover all victims).

What is for sure is that triage is more complex than that of CWAs release since it combines radiation with blast injuries that make even small lesions extremely threats for the survival of the victim – not to mention the future consequences of exposure to radiation[61]. Although the radiation plume is not expected to last long and will settle within the next hour, it is the winds that can make it bigger in combination with to the "urban canyon effect" that produces air currents moving to various directions through high building usually existing downtown.

The last big problem that all first responders will face is to rapidly calculate the radiation doses that will permit them to operate safely in both the "hot" and "warm" zones. In general: "the time limitation for responder occupancy of a zone is based on the risk to a person/responder for developing a radiation-induced cancer (<0.5% per 5 rem), which characteristically does not occur until years or decades later.[62]"

CHAPTER 5 - Medical/hospital chemical-radiological defense during the 2012 Olympic Games in London, UK

Athens' 2004 Olympic Games medical/hospital CBRN defense experience

As military CBRN consultant attached to the 2004 Olympic Games Security Committee and Commandant of the Olympic Hospital CBRN Response Unit deployed at the Army General Hospital of Athens there are certain "problems identified" that will be collectively presented herein:

Pre-games status:

General attitude: "It will not happen to us…" This small sentence was the biggest obstacle all CBRN-related specialists were facing in almost all levels of authority. Focused on traditional/conventional terrorism all relevant authorities had no faith that weapons of mass destruction could be released during the biggest athletic event of mankind. Even after the 9-11 incident and "anthrax-letters" they were reluctant to admit that this is the new reality and that the least we could do was to take this under serious consideration. Of course, CBRN defense for such a major event required a lot of money that would exaggerate further the already out of control budget.

Medical/Hospital personnel/structures: When come to medical/hospital/ public health entities, the situation was much more primitive. Medical people had minimum to zero knowledge regarding CBRN threats and their consequences on humans and societies. The same applied for CBRN crisis management that is totally different than any other medical crisis during peace time. It took a lot of time to re-educate all these entities and try to make them realize the magnitude of the problem. But even the extended presentation of the Tokyo, Bohpal and Guiânia incidents did not bend their skepticism.

A second severe point of traction was their attitude in participating in “hot” and “warm” operational zones. Sterile objection could be replaced with productive willingness to learn and participate. With some limited exceptions from the EMS people, they strictly refused any kind of involvement.

What was the case on personnel preparedness the same was applied for CBRN structures’ preparedness. During the Games, Olympic Hospital CBRN Response Unit was the only hospital-oriented unit deployed in all five Olympic cities. It was the only unit that was ready to accept CBRN casualties – mainly chemical and few inner radio-contaminated victims. An effort to create a new bio-safety lab (BSL Level “3”) was failed – the lab was ready made but manning was absent. Same applied for the negative pressure ward (12 beds able to expand to 24) that has been equipped with negative pressure capabilities (including a central Microgenix™ air purification system[63]), but it was faulty constructed by a civilian constructor who did no follow detailed guidelines given.

Despite the past global experience of SARS and avian flu only a few hospitals in Greece had a handful of negative pressure wards. Mass decontamination at hospitals? A joke! Most probably they would wait for firemen to arrive and create “water curtains”. Or even worse: redirect all casualties to the “specialized” Army Hospital! CBRN response plan? Yes, they all had copies of the master CBRN plan where there was a big entity devoted to medical mass casualties. But big plans are not easy to study and implement.

Total lack of CBRN PPE: With the exception of EMS personnel, hospitals lacked PPE. Medical planners must realize that theory and practice when come to CBRN operations go hand-by-hand. A few lectures on weapons of mass destruction are NOT enough to make audience realize how hard it is when you don the PPE and you asked to save lives.

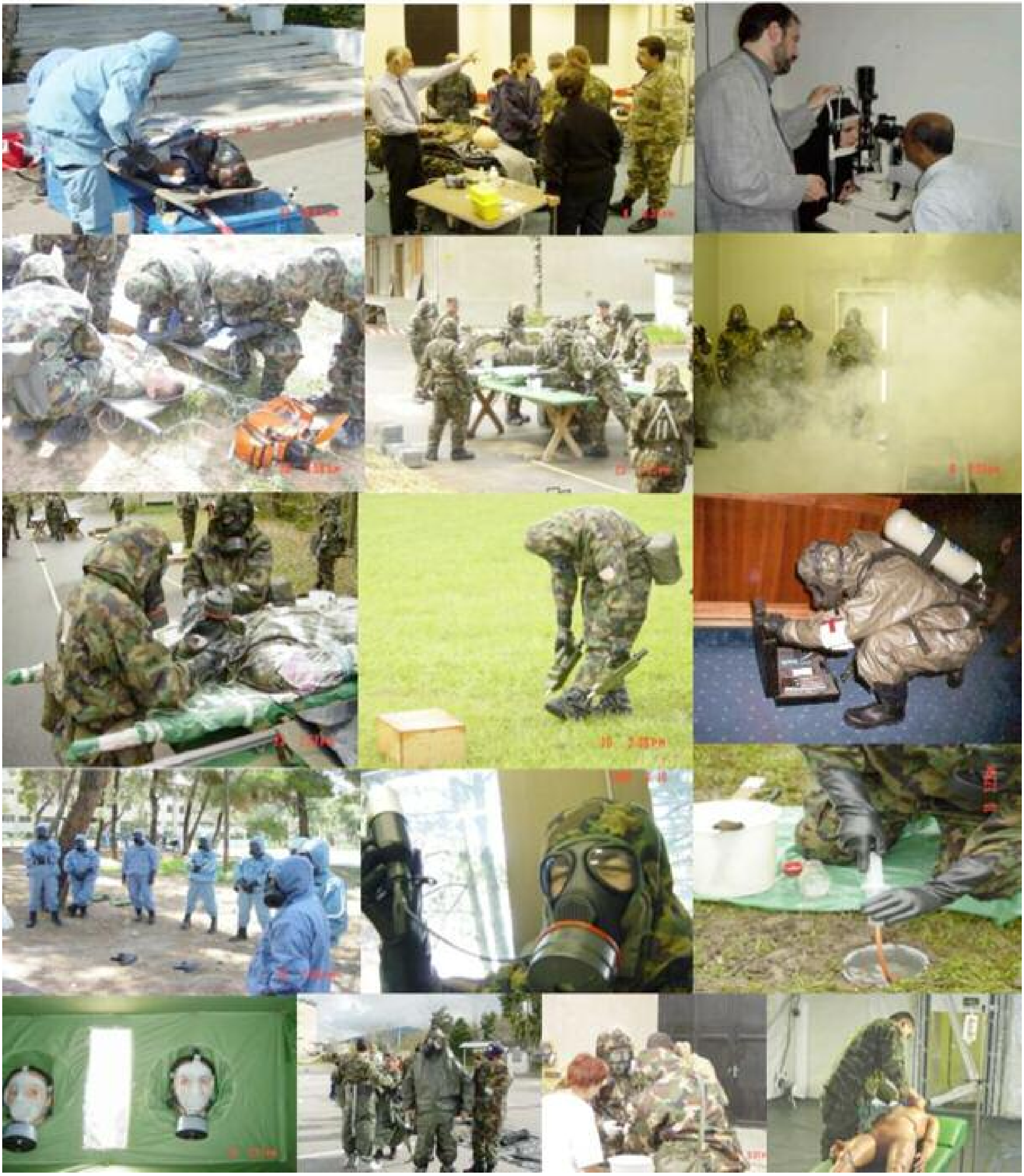
Let us suppose that all hospitals’ EMS departments were equipped with PPE stored in a special room. Can anybody imagine the moment that the threat becomes real and they open the room to distribute PPE? What if in that particular shift, chief surgeon on duty is a doctor with a history of double by-pass just 6 months ago? Does anyone really believe that all these people will last more than 15 minutes? Medical people must feel when in PPE as comfortable as with their white blouses! (exaggeration? perhaps; but most close to reality). At the Army Hospital, unit’s personnel were practicing daily, march, run, load and upload stretchers, even slept on PPE – even with ambient temperatures of 35^0 to 40^0 C! It was hard, but the purpose was sacred – we had a mission to accomplish!

Lack of cooperation/integration between civilian-military medical systems: Although both systems practice same medicine, a hidden competition arose during the Olympic Games. This competition transformed to opposition when mass CBRN casualties were put on the table. The opinion that this is a “military medicine issue” was universal and their attitude firm. On the other hand, military hospitals are just hospitals that take care of the enlisted personnel, veterans, their families and a few categories of civilian patients. Military medical personnel did not had a special kind of training on how to cope with CBRN casualties – especially in urban environment that is so different from field operations. But still it was a matter of “military medicine”. Even amongst military hospitals there was argument on who will be in charge and take the heat in case of a real CBRN terrorist incident. The establishment of the Medical CBRN Response Unit supported by Air Force General Hospital and Naval Hospital of Athens was a solution that worked out well.

ATHENS' 2004 OLYMPIC GAMES

ARMY HOSPITAL CBRN RESPONSE UNIT

Preparation Phase



ATHENS 2004

ATHENS' 2004 OLYMPIC GAMES

ARMY HOSPITAL CBRN RESPONSE UNIT

Deployment Phase

HOSPITAL CBRN RESPONSE UNIT

Olympic Games' status

During the Olympiad in Athens (the first summer Olympiad after 9-11), the Olympic Hospital CBRN Response Unit was ready on-time and in place in full alert.

A second military medical-oriented CBRN unit created in the last half of 2003 was also ready. The target of this Joint Medical CBRN Unit (250 physicians-nurses-NCOs), was to support first responders (police, firemen) in operations within the "hot" and "warm" zones. At the same time they could provide support to Army Hospital's existing unit, to Olympic Hospitals near incident's area or to Olympic Hospitals located in the four participating Olympic cities.

NATO provided the NBC Battalion that in full composition was stationed in the city of Chalkis (approximately 88 km away from Athens). The historian of the future might reveal who choose this location and what international planners had in mind in case of a real CBRN terrorist incident. CBRN planners must once and for all realize that being "ready and far away" is not as important as being "ready and on the spot". In CBRN operations time is not money; "time is life!"

Post Olympiad status

Military sector: The Olympic Hospital CBRN Response Unit was gradually diminished and finally dissolved by the end of 2004. Military medical hierarchy believed that after the Games the threat was not real anymore projecting the heavy daily work schedule that left no time for continuation of training, drills, equipment maintenance etc.

The Joint Medical CBRN Unit was transformed to a Joint CBRN Platoon located in Athens. This was the only gain for the military. At least now Hellenic Armed Forces we have something ready to deploy and assist if needed.

The BSL-3 lab turned to be an ordinary microbiology lab while the negative pressure ward is now used for hospitalization of daily infectious disease cases – mostly as an isolation area with limited access. What a disappointment for those dreamed a new era in military medicine… The original dream of a just a few people for a hospital-based CBRN unit supported by a BSL-3 lab and a negative pressure ward dissolved by the lack of ability of "those who sign" to have a look in the future to come. The inner belief of "nothing will happen to us" prevailed – one more time!

Civilian sector: After the Games, civilian sector returned to normal. CBRN adventures and possibilities were forgotten overnight. Those involved in certain medical CBRN trainings were absorbed in various services and desired continuity and passing the experience to new generations was thrown to a drawer and left in the dark. More or less the same applied for first responders although police still conducts some training seminars from time to time. Officials in high places tend to forget or forget at will, that people with certain specialization and training are getting older, transferred to desk offices, transferred to other cities or have new duties while many of them retire or die. If a new generation of people involved in management of new emerging threats fails to exist, then state CBRN preparedness will return to zero soon. Until next time something "big" will happen somewhere in the world. Then mobiles will start ringing again (it is of note that the "diagnosis" of the agent released in Tokyo was made by a retired "chemical colonel" who was watching the news), plans will be back on the table for revision, new units will be formatted, veterans will be asked to participate because they have the knowledge and experience – but it might be too late.

Key-points regarding medical/hospital chemical-radiological defense during the 2012 London Olympic Games

In August 2010, the United Kingdom will have the pleasure and pride to host the Summer Olympiad. It is a common secret that security is the number one priority for the hosting country. It is also known that the United Kingdom is among the top five countries that terrorists would love and pursue to attack for many reasons. Global television coverage of this major event provides the best opportunity to pass their message to the rest of the world and succeed a strike to remember to the infidels. A strike that has to be "bigger" from 9-11 in order al Qaeda, affiliated and franchise to "keep face" (keep respect) amongst Muslim world. Perhaps a simultaneous strike with 10 airplanes crashed in urban targets within the country's major cities would do the job. A chemical or radiological attack downtown London is even better. A combination will raise the long board to immense heights!

In that respect, a few key-points will be referred below regarding medical/hospital CBRN defense during the Games:

- Time left is barely enough to feel the gaps in medical CBRN defense.
- All hospitals in London and other Olympic cities must be prepared to deal with mass CBRN casualties. Chemical and radiological casualties should be a priority.
- All EMS departments' personnel must be trained in CBRN operations and acclimatize in PPE usage and performance.
- Find the right ways to motivate hospital personnel. Work with these people and listen to their needs and hesitations. It would be nice to do it "for the Country and the Queen!" But at the beginning of the 21st century, are you sure that this alone will work?
- All hospitals must have the same CBRN response plan. The plan must be short and clear, threat-specific, with defined duties and responsibilities.
- Mass decontamination facilities must given priority. Hospitals do not have to buy expensive decontamination systems; an open-minded plumber with dedication and inspiration will do the job. Choose the biggest wall of the hospital and fill it with showers (even better have water from the top and two more water-jets for trunk and lower extremities). Construct a waste water collection tank underneath and connect it with the main drainage system. Construct many isolation panels like those you have at the hospital wards. Privacy is ready. It might look primitive but will do the job!
- Program many drills: threat-specific and combination drills; hospital drills, drills between hospitals, national drills, hospital-first responders drills; table-top, night and day drills.
- Cooperate with OPCW for chemical defense issues could be extremely fruitful along with activation of "Article X" applied for all member-states. It does not matter how big country Great Britain is. CBRN events are bigger than countries! Why taking the risk to do it all by yourself?
- Medical CBRN Defense and/or Terror Medicine should be included in the curricula of last years of medical/dental/pharmaceutical/ veterinary/nursing and public health schools. This is the only solution to private future front line health professionals with some basic knowledge of new emerging threats and their effects on humans, livestock and environment. If the young doctor is unaware of anthrax then for people coming to his shift or his private practice, his differential diagnosis would be between "flu" and "flu". Do you think that your surgeons have the knowledge and practical experience to deal with suicide-bombing blast injuries? The training package (presentations, manuals, pocket cards, practical training) can be done once and then disseminated to all schools of interest. A good starting point might the already existing guide from Health Protection Agency entitled "CBRN incidents: Clinical management and health protection[64]" or the ETHREAT manual[65] for front-line health professionals entitled "How to respond to radiological, biological and chemical threats". For the practical training (if applicable) the Defence Nuclear, Biological and Chemical Centre [DNBCC] at Winterbourne Gunner (Salisbury) would be ideal. You can even create an entirely new "UK Medical CBRN Training School" that will serve universities' needs. There are many experienced people (in national and international level) who can facilitate the program with minimum cost. Take advantage of your military medical personnel on duty in Afghanistan. They are more than willing to transfuse their unique expertise to domestic colleagues. Take advantage of the medical innovations used in the war field to strengthen your medical shield in the inland. Involve retired medical personnel with active experience from IRA era. They can teach things that younger generations of doctors cannot imagine or read in the books. Unfortunately, evolution usually walks through wars and losses of human life.

Conclusions

When in 1995 members of the Aum Shinrikyo cult attacked Tokyo's subway by releasing nerve gas sarin, the world was shocked.

was the first usage of chemical warfare agents in megapolis environment and a new shift in terrorism. Since then, and especially following "anthrax letters" campaign accompanying the 9-11 incidents in the United States, the possibility of employment of weapons of mass destruction by terrorists of the future became more evident. It is not "NoBody Cares" (NBC) anymore. Instead new emerging threats are amongst top three mega-threats Western societies will be asked to confront. CBRN agents provide destruction, produce terror, gain sky rocket media ratings and sometimes might even achieve political gains.

In all CBRN plans, medical/hospital CBRN defence represents the "weak link". State bodies tend to invest in operational aspects of CBRN operations forgetting that medical consequences might last months or even years. On the other hand, medical community in general is not very willing to be involved in such operations. Basically it is ignorance and lack of specialized knowledge that creates an exotic environment when comes to chemical weapons or dirty bombs. The key to this problem is training in both theory and praxis. Theory and praxis turns a medical student to thoracic surgeon. Theory and praxis turns an EMS physician to medical CBRN specialist. Without training one cannot sew even a button! It is totally understood that such training requires time and effort, physical conditioning and dedication. This is the part that motivation plays an important role. The questions: "what is it for me?" and "why should I be involved?" must be addressed carefully and with good will in order to achieve the final goal – volunteering. You can not force medical people to do things. Medicine is a vocation and not just a profession!

A second problem roots within the administration attitude. If people in high places do not believe that new emerging threats pose a danger to the society, then it is extremely difficult to make a good plan. Specialized equipment cost sufficient amount of money, training cost money as well – and time. At the same time, hospitals' are always on the look for financing in order to cover daily expenses and future projects. Spending money for a program that will last only for a few weeks looks like an unnecessary investment that will bring no gain to the hospital especially when "nothing is going to happen to us!" All those involved in administrative duties must realize that the threat is here to stay! It is an investment of life and if only one time repays its money it will be worth investing into it.

Problems identified during the 2004 Olympic Games in Athens regarding medical/hospital CBRN defence remained unsolved during the next Olympiad in China and are expected to be there during the London 2012 Olympic Games. They have to do more with the nature of the threat than the organizational concepts of the hosting countries. Perfection in counter-terrorism does not exist. Terrorists will always have the benefit of surprise and they will be always a few steps ahead their prosecutors. The solution is to minimize the distance from them in order to save as many lives as possible. It is impossible to train all doctors and nurses on how to deal with new threats. Let us train as many as possible. It is impossible to have all hospital ready and prepared to accept mass contaminated casualties. Let us focus to as many hospitals as possible. We cannot provide multi-figure bonuses to those involved in extra duties and responsibilities. We can give them a symbolic contribution to their devotion to the main cause: to organize the safest Olympic Games ever!

United Kingdom cannot organize medical CBRN defence completely by its own. Even great nations need international assistance especially from countries that have already been through the agony of organizing the biggest sports event in the world. It has nothing to do with national pride, technological development, science proficiency and all the qualities characterizing great nations. It has to do with the safety of British people and their guests from all over the world that will visit United Kingdom to celebrate in unity this major event. In that respect, people must work together against a common enemy – terrorism!

APPENDIX A

ETHREAT PROJECT AT A GLANCE

ETHREAT
European Training for Health Professionals
on Rapid Response to Health Threats

QUESTIONNAIRE ONE – For Front Line Health Professionals

Questions on: demographics, CBRN plan availability, CBRN training, PPE confidence, PPE in work place, discriminate of natural vs man-made incidents, preparation/knowledge regarding CBRN threats.

- **Questionnaires delivered: 531**
- **Origin of questionnaires: 22 EU countries**

Participants' age distribution:

- **30-39** (29.9%)
- **40-49** (26.4%)
- **50-59** (20.8%)

Participants' profession:

- **Physicians** (45.5%)
- **Nurses** (14.3%)
- **Public health officers** (26.8%)

Participants' working status:

- **Civilian** (96.5%)
- **Military** (3.5%)

National CBRN plan available:

- **No** (49.4%)
- **Yes** (50.6%)

Knowledge of whom to contact in case of deliberate incident:

- **No** (32.9%)
- **Yes** (67.1%)

Last CBRN training was:

- **<6 mo** (19.5%)
- **12 mo** (12.6%)
- **24 mo** (18.2%)
- **36 mo** (4.8%)
- **>48 mo** (17.7%)
- **Never** (27.3%)

Confidence in PPE usage :

- **Very low/Low** (17.3%)
- **High/Very high** (28.5%)

Access of PPE in workplace:

- **Very low/Low** (9.5%)
- **High/Very high** (35.9%)

Discriminate natural vs man-made incidents:
Chemical

- Very poorly/Poorly (55.8%)
- Well/Very well (31.6%)

Biological

- Very poorly/Poorly (60.2%)
- Well/Very well (30.3%)

Radiological

- Very poorly/Poorly (57.1%)
- Well/Very well (27.3%)

How well prepared for:
Chemical

- Very poorly/Poorly (53.3%)
- Well/Very well (37.2%)

Biological

- Very poorly/Poorly (47.2%)
- Well/Very well (46.8%)

Radiological

- Very poorly/Poorly (57.6%)
- Well/Very well (28.6%)

Level of knowledge regarding:
Anthrax

- Very poorly/poorly (32.5%)
- Well/Very Well (64%)
- No (3.5%)

VHF

- Very poorly/Poorly (35.9%)
- Well/Very well (57.6%)
- No (6.5%)

Nerve agents

- Very poorly/Poorly (52%)
- Well/Very well (42.9%)
- No (5.2%)

Mustard

- Very poorly/Poorly (52.4%)
- Well/Very well (34.7%)
- No (13%)

QUESTIONNAIRE TWO – For CBRN Experts

Question: What proportion of FLHPs in your country is adequately prepared to recognize and manage biological, chemical and radiological incidents?

- **Questionnaires delivered: 93**
- **Origin of questionnaires: 16 EU countries**

Biological incidents

0% - 24%	42.9%
25% - 49%	17.5%
50% - 74%	15.9%
75% - 100%	4.8%
Do not know	19%

Chemical incidents

0% - 24%	38.1%
25% - 49%	23.8%
50% - 74%	12.7%
75% - 100%	6.3%
Do not know	19%

Radiological incidents

0% - 24%	52.4%
25% - 49%	17.5%
50% - 74%	3.2%
75% - 100%	4.8%
Do not know	22.2%

Brigadier General (ret) **Ioannis [John] Galatas** was born in 1958 and graduated from the Military Medical Academy and the Medical School of the Aristotelian University of Thessaloniki in 1982. He is specialized in Allergy and Clinical Immunology and held the position of Head, Department of Allergology & Clinical Immunology for more than 20yrs. Since 2001 he specialized as CBRN officer and planner trained in a number of countries (including Iran) abroad. His main focus is "Medical/Hospital CBRN Defense". During the 2004 Athens' Olympic Games, he served as Commandant of the "Olympic Hospital CBRN Response Unit" – the only hospital-based specialized unit deployed for the Games. He holds a PhD degree in Medicine and a Master's Degree on "International Terrorism, Organized Crime and Global Security" from Coventry University, UK. In that respect he is very much interested and willing to be involved in "counter CBRNE operations" for London 2012 Olympiad. He is the Editor (since 2005) of the on-line "CBRNE-Terrorism Newsletter". Since Aug 2010 he is the CBRN Scientific Coordinator at Research Institute of European-American Studies (RIEAS) and holds the position of Vice Chairman of Greek Intelligence Studies Association (GISA). His last military appointment (since 2007) before his voluntarily retirement in Aug 2010, was as Head of the Department of Asymmetric Threats at the Intelligence Analysis Branch, of Joint Military Intelligence Division of the Hellenic National Defense General Staff in Athens., Greece.

Bibliography

[1] Definition of terrorism. URL: http://www.experiencefestival.com/a/Terrorism_-_Etymology/ id/5163807 (Accessed: August 11, 2010)

[2] Bruce Hoffman (1999). Inside Terrorism. Columbia University Press; pp. 1-288

[3] Ben Saul. "Defining 'Terrorism' to Protect Human Rights" in Sydney Law School Legal Studies Research Paper. No. 08-125 (2008) p.11.

[4] Brian M. Jenkins, "Will Terrorists Go Nuclear?" *Orbis* 29, no. 3 (Autumn 1985): 511.

[5] Ehud Sprinzak, "The Great Superterrorism Scare," *Foreign Policy* (Fall 1998): 122

[6] *Ben Saul (2006). The Legal Response* ***of*** *the* ***League of Nations*** *to Terrorism. Journal* ***of*** *International Criminal Justice, Vol. 4, No. 1, pp. 78-102,*

[7] *United Nations Security Council Resolution 1566. URL: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N04/542/82/PDF/N0454282.pdf?OpenElement*

[8] United Nations General Assembly A/RES/49/60 (1995). Measures to eliminate international terrorism. URL: http://www.undemocracy.com/A-RES-49-60.pdf

[9] Council Framework Decision of 13 June 2002 on combating terrorism (2002/475/JHA). Official Journal of the European Communities. URL: http://www.statewatch.org/news/2002/jul/frameterr622en00030007.pdf

[10] US Code - Section 2331. FindLaw for Legal Professionals. URL: http://codes.lp.findlaw.com/uscode/18/I/113B/2331

[11] Terrorism Act 2000. URL: http://www.opsi.gov.uk/acts/acts2000/pdf/ukpga_20000011_en.pdf

[12] Wm. Robert Johnston (2010). Incidents of Mass Casualty Terrorism. URL: http://www.johnstonsarchive.net/terrorism/wrjp394.html

[13] Peter R. Neumann (2008). Terrorism in the 21st century- Compass 2020. URL: http://library.fes.de/pdf-files/iez/06063.pdf

[14] Nicholas Berry. Targets of terrorism. Center for Defence Information – Terrorism Project. URL: http://www.cdi.org/terrorism/moretargets.html.

[15] First War War. Weapons of War – Poison Gas. URL: http://www.firstworldwar.com/weaponry/gas.htm

[16] Organization for the Prohibition of Chemical Weapons (2010). Status of participation in the CWC. URL: http://www.opcw.org/about-opcw/member-states/status-of-participation-in-the-cwc/

[17] Organization for the Prohibition of Chemical Weapons. Basic Facts on Chemical Disarmament. Brief description of chemical weapons. URL: http://www.opcw.org/news-publications/publications/basic-facts/#c4128

[18] Environmental Research Foundation (1994). Chemical accidents. URL: http://www.ejnet.org/rachel/rehw408.htm#1

[19] Jackson B. Browning (1993). Union Carbide: Disaster at Bhopal. Jackson Browning Report - Union Carbide Corp. URL: http://www.bhopal.com/pdfs/browning.pdf

[20] Meridian Medical Technologies. Cyanokit. URL: http://www.cyanokit.com

[21] Amy E. Smithson, Leslie-Anne Levy (2000). Ataxia: The Chemical and Biological Terrorism Threat and the US Response. Report No. 35. The Henry L. Stimson Centre. URL: http://www.stimson.org

[22] YouTube: Tokyo Sarin attack 1. URL: http://www.youtube.com/watch?v=00oFivBQdjo&feature=related
YouTube: Tokyo Sarin attack 2. URL: http://www.youtube.com/watch?v=LqMiKvjR9yY&feature=related
YouTube: Tokyo Sarin attack 3. URL: http://www.youtube.com/watch?v=ROHLeELHPXs&feature=related
YouTube: Tokyo Sarin attack 4. URL: http://www.youtube.com/watch?v=VOLtV2nBexc&feature=related
YouTube: Tokyo Sarin attack 5. URL: http://www.youtube.com/watch?v=GITkHxrP_XE&feature=related

[23] David E. Kaplan and Andrew Marshall. The cult at the end of the world: The incredible story of Aum. London: Arrow Books Ltd. (Random House UK Ltd.),

1996; pp.1-310.

[24] *Ibid.*21.

[25] Patterson, Andrew J (2007). Ushering in the era of nuclear terrorism Critical Care Medicine, Volume 35, pp.953-954

[26] James M. Acton; M. Brooke Rogers; Peter D. Zimmerman (2007). Beyond the Dirty Bomb: Re-thinking Radiological Terror. *Survival*, Volume 49, Issue 3, pp. 151 - 168

[27] Steve Boggan (2007). Who else was poisoned by polonium?» London: Guardian Unlimited. 5 June 2007. URL: ttp://www.guardian.co.uk/science/story/0,,2095599,00.html?gusrc=rss&feed=18. Retrieved 5 June 2006.

[28] Health Protection Agency (UK). Polonium 2010. URL: http://www.hpa.org.uk/Topics/Radiation/UnderstandingRadiation/UnderstandingRadiation-Topics/Polonium210/

[29] Polonium-210: The Public Health Response. Royal College of Surgeons, London, 27 March 2007. URL: http://iopscience.iop.org/0952-4746/27/3/M02/pdf/0952-4746_27_3_M02.pdf

[30] Lexi Krock and Rebecca Deusser. Dirty bomb – Chronology of events. URL: http://www.pbs.org/wgbh/nova/dirty-bomb/chrono.html

[31] The Irish Times. Moldova seizes radioactive uranium. 24 August 2010. URL http://www.irishtimes.com/newspaper/breaking/2010/0824/breaking66.html (Accessed: 24 August 2010).

[32] The Nuclear Threat Initiative (NTI) - Prevention of Radiological Terrorism: Obstacles to Preventing Radiological Terrorism. URL: http://www.nti.org/h_learnmore/rad-tutorial/chapter05_03.html

[33] International Atomic Energy Agency (1988). The radiological accident in Goiânia. STI/PUB/815. URL: http:// *www-pub.iaea.org/MTCD/publications/PDF/Pub815_web.pdf*

[34] Brown, F.; Hall, G.R.; Walter, A.J. (1955). «The half-life of Cs137». *Journal of Inorganic and Nuclear Chemistry* **1**: 241–247

[35] OPCW Calendar of Events: URL: http://www.opcw.org/events-calendar (Accessed: 05 February 2010)

[36] OPCW: Chemical Weapons Convention – Article X. URL: http://www.opcw.org/chemical-weapons-convention/articles/article-x-assistance-and-protection-against-chemical-weapons/

[37] Watters, Ron (2003). The Wrong Side of the Thin Edge. To the Extreme: Alternative Sports, Inside and Out. Robert E. Rinehart and Synthia Sydnor (eds). Albany: State University of New York Press, 2003: 258-259.

[38] Ernest P. Noble, Tulin Z. Ozkaragoz, Terry L. Ritchie, Xuxian Zhang, Thomas R. Belin, Robert S. Sparkes (1998). D2 and D4 Dopamine Receptor Polymorphisms and Personality. American Journal of Medical Genetics (Neuropsychiatric Genetics) 81:257–267.

[39] D C Wetter, W E Daniell, and C D Treser (2001). Hospital preparedness for victims of chemical or biological terrorism. Am J Public Health. 2001 May; 91(5): 710–716.

[40] Mann NC, MacKenzie E, Anderson C. (2004). Public health preparedness for mass-casualty events: a 2002 state-by-state assessment. Prehosp Disaster Med. 2004 Jul-Sep;19(3):245-55.

[41] Higgins W, Wainright C, Lu N, Carrico R (2004). Assessing hospital preparedness using an instrument based on the Mass Casualty Disaster Plan Checklist: results of a statewide survey. Am J Infect Control. 2004 Oct;32(6):327-32.

[42] Niska RW, Burt CW (2005). Bioterrorism and mass casualty preparedness in hospitals: United States, 2003. Adv Data. 2005 Sep 27;(364):1-14.

[43] Bennett RL (2006).Chemical or biological terrorist attacks: an analysis of the preparedness of hospitals for managing victims affected by chemical or biological weapons of mass destruction. Int J Environ Res Public Health. 2006 Mar;3(1):67-75

[44] Reilly MJ, Markenson D, DiMaggio C (2007). Comfort level of emergency medical service providers in responding to weapons of mass destruction events: impact of training and equipment. Prehosp Disaster Med. 2007 Jul-Aug;22(4):297-303.

[45] E Andriopoulou, I Galatas, A Baka, W Kirch, A Fuchs, J Kyncl, J Dowie, D Szosland, V Koycheva, E Tavoulari, I Kot-

sioni, A Linos (2006). European training for health professionals on rapid response to health threats following biochemical terrorism incidents. European Journal of Public Health, Vol. 16, Supplement 1. p.123.

[46] Ann Göransson Nyberg. MASs-casualties and Health-care following the release of toxic chemicals or radioactive materials (MASH Project): WP6-Report. 30 March 2009. URL: http://www.mashproject.com/index.php?option=com_content&view=article&id=10&Itemid=13 (Accessed: 23 August 2010).

[47] Fred P. Stone. The "worried well" response to CBRN events: analysis and solutions. The Counterproliferation Papers. Future Warfare Series No. 40. USAF Countreproliferation Center. Air University: Maxwell Air Force Base, Alabama. June 2007; pp. 1-64.

[48] Merriam-Webster Online Dictionary. Golden hour – definition. URL: http://www.merriam-webster.com/medical/golden%20hour

[49] Lerner EB, Moscati RM (2001) The golden hour: scientific fact or medical "urban legend"? Acad Emerg Med 2001;8:758–760.

[50] Alan King. Going for the Gold. CBRNe World – Spring 2009. URL: http://www.cbrneworld.com/pdf/09_spring_Going_for_Gold.pdf

[51] Critical Illness and Trauma Foundation, Inc. START triage system. URL: http://www.citmt.org/start/ flowchart.htm (Accessed: 22 December 2009)

[52] Zoraster RM, Chidester C,Koenig W (2007). Field triage and patient maldistribution in a mass-casualty incident. *Prehosp Disast Med* 2007;22(3):224–229.

[53] Okumura T, Kondo H, Nagayama H, Makino T, Yoshioka T, Yamamoto Y (2007). Simple triage and rapid decontamination of mass casualties with the colored clothes pegs (STARDOM-CCP) system against chemical releases. *Prehosp Disast Med* 2007;22(3):233–236.

[54] Bond WF, Subbarao I, Kimmel SR, Kuklinksi J, Johnson C, Eberhardt M, Vozenilek J (2008). Testing the use of symptom-based terrorism triage algorithms with hospital-based providers. *Prehospital Disast Med* 2008;23(3):234–243.

[55] Levitin H, Siegelson HJ,Dickinson S, Halpern P, Haraguchi Y,Nocera A, Turineck D (2003). Decontamination of mass casualties — Re-evaluating existing dogma. *Prehosp Disast Med* 2003;18(3):200–207.

[56] Schumacher J,Weidelt L, Gray SA, Brinker A (2009). Evaluation of bag-valve-mask ventilation by paramedics in simulated chemical, biological, radiological, or nuclear environments. *Prehosp Disaster Med* 2009;24(5):398–401.

[57] Haim Berkenstadt, Amitai Ziv, Daphna Barsuk, Inbal Levine, Amir Cohen, Amir Vardi (2003). The Use of Advanced Simulation in the Training of Anesthesiologists to Treat Chemical Warfare Casualties. Anesth Analg 2003;96:1739 –42

[58] Clarke SFJ, Chilcott RP, Wilson JC, Kamanyire R, Baker DJ, Hallett A (2008). Decontamination of multiple casualties who are chemically contaminated: A challenge for acute hospitals. *Prehospital Disast Med* 2008;23(2):175–181

[59] Leiba A, Goldberg A, Hourvitz A,Weiss G, Peres M, Karskass A, Schwartz D, Levi Y, Bar-Dayan Y (2006). Who should worry for the "worried well"? Analysis of mild casualties center drills in non-conventional scenarios. Prehosp Disast Med 2006;21(6):441–444.

[60] Ruzek JI,Walser RD,Naugle AE, Litz B, Mennin DS, Polusny MA, Ronell DM, Ruggiero KJ, Yehuda R, Scotti JR (2008). Cognitive-behavioral psychology: Implications for disaster and terrorism response. *Prehospital Disast Med* 2008;23(5):397–410

[61] Hrdina CM, Coleman CN, Bogucki S, Bader JL, Hayhurst RE, Forsha JD, Marcozzi D, Yeskey K, Knebel AR (2009): The "RTR" medical response system for nuclear and radiological mass-casualty incidents: A functional TRiage-TRansport-TReatment medical response model. *Prehospital Disast Med* 2009;24(3):167–178

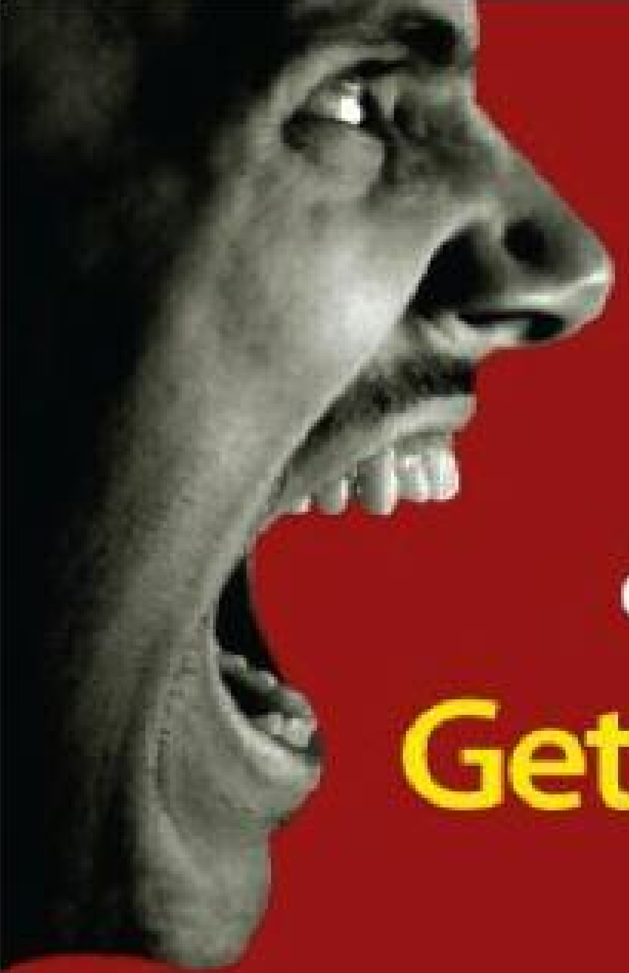
[62] C. Norman Coleman, Chad Hrdina, Judith L. Bader, Ann Norwood, Robert Hayhurst, Joseph Forsha, Kevin Yeskey, Ann Knebel (2009). Medical Response to a

Radiologic/Nuclear Event: Integrated Plan from the Office of the Assistant Secretary for Preparedness and Response, Department of Health and Human Services. Ann Emerg Med. 2009; 53:213-222

[63] Clark AJ, Bird H, Goodyear D, Reid K, Webber D, Whatley P (2000). Trials assessment report: Prototype air filtration system. DERA, CBD Porton Down (an Agency of the UK Ministry of Defense) – Commercially sensitive. pp.1-32

[64] Julia Heptonstall, Nick Gent (2005). CBRN incidents: Clinical management and health protection. Health Protection Agency; pp.1-65

[65] EUROPA, DG Health and Consumer Protection, Public Health. ETHREAT Project. URL: http://ec.europa.eu/health/ph_projects/2004/action2/action2_2004_02_en.htm#4



Chem News

Organization for the Prohibition of Chemical Weapons (OPCW)

Source: http://www.opcw.org/news-publications/publications/facts-and-figures/

A Global Convention to Ban Chemical Weapons

The CWC aims to eliminate an entire category of weapons of mass destruction by prohibiting the development, production, acquisition, stockpiling, retention, transfer or use of chemical weapons by States Parties. States Parties, in turn, must take the steps necessary to enforce that prohibition in respect of persons (natural or legal) within their jurisdiction.

All States Parties have agreed to chemically disarm by destroying any stockpiles of chemical weapons they may hold and any facilities which produced them, as well as any chemical weapons they abandoned on the territory of other States Parties in the past. States Parties have also agreed to create a verification regime for certain toxic chemicals and their precursors (listed in Schedules 1, 2 and 3 in the Annex on Chemicals to the CWC) in order to ensure that such chemicals are only used for purposes not prohibited.

A unique feature of the CWC is its incorporation of the 'challenge inspection', whereby any State Party in doubt about another State Party's compliance can request the Director-General to send an inspection team. Under the CWC's 'challenge inspection' procedure, States Parties have committed themselves to the principle of 'any time, anywhere' inspections with no right of refusal.

Making the Convention Work

To make sure that the CWC is implemented effectively, States Parties are obliged to designate or establish a National Authority. This body escorts OPCW inspections of relevant industrial or military sites; submits initial and annual declarations; assists and protects those States Parties which are threatened by, or have suffered, chemical attack; and fosters the peaceful uses of chemistry. In addition, the National Authority acts as the focal point in the State Party's interaction with other States Parties and the Technical Secretariat of the OPCW.

The Secretariat supports States Parties in their national implementation of the CWC. The focus of this work is to provide advice and assistance to the staff of National Authorities, in order to help them enhance their skills and expertise to facilitate effective, autonomous, national implementation. The Technical Secretariat coordinates and hosts regular meetings of the National Authorities from around the world. CD-ROM, DVD and website information packages on CWC implementation are available.

Every State Party must implement the provisions under the CWC at the national level. This includes enacting penal legislation encompassing all activities prohibited. Each State Party is obliged to provide other States Parties with its fullest cooperation to expedite prosecution. Legal experts have formed regional networks to facilitate the adoption of national legislation that bans and criminalises the misuse of chemicals as weapons.

Some figures on national implementation follow:

- 182 National Authorities have been established.
- 126 States Parties have informed the Organisation of the legislative and adminis-

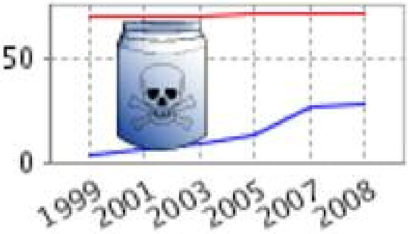
trative measures taken to implement the Chemical Weapons Convention.

- 83 States Parties have legislation covering all key areas.

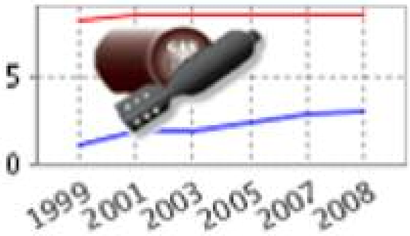
Since 1997, over 2,800 participants —including more than 1,400 sponsored participants from all geographical regions— have received support in the CWC's effective national implementation through OPCW meetings, workshops and training courses.

Chemical Weapons Destruction Under Way

The 7 States Parties (A State Party, Albania, India, Iraq, the Libyan Arab Jamahiriya, the Russian Federation, and the United States of America) which have declared chemical weapons must destroy 8.67 million items, including munitions and containers containing in total, 71,194 metric tonnes of extremely toxic chemical agents. Albania, India and a third country have completed destruction. By comparison, a tiny drop of a nerve agent, no larger than the head of a pin, can kill an adult human being within minutes after exposure. The OPCW verifies that the destruction process is irreversible. At the same time, States Parties in the process of destroying chemical weapons are obliged to place the highest priority on the safety of people and on protecting the environment.



44,131, or 61.99%, of the world's declared stockpile of 71,194 metric tonnes of chemical agent have been verifiably destroyed. (As at 30/09/2010)



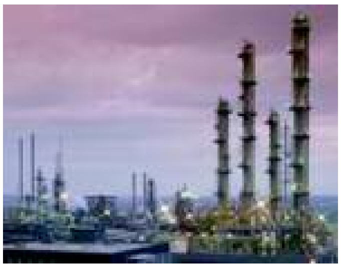
3.95, or 45.56%, of the 8.67 million chemical munitions and containers covered by the CWC have been verifiably destroyed. (As at 30/09/2010)

The OPCW has developed an internationally unique, peer-reviewed, and certified analytical database, containing information on over 3,400 chemical weapons-related compounds. This database is essential for on-site verification activities of OPCW inspection teams, and is also made available to States Parties. Official Proficiency Tests are conducted to select, certify, and train States Parties' laboratories for the analysis of chemical weapons-related compounds in the event of off-site analysis of authentic samples. 20 laboratories have been designated.

- From Entry into Force of the CWC (April 1997) until 30/09/2010, the OPCW has conducted 4,167 inspections on the territory of 81 States Parties, including 2,305 inspections of chemical weapon-related sites. 195 chemical weapon-related sites have been inspected out of a total of 227 declared.
- 100% of the declared chemical weapons stockpiles have been inventoried and verified.
- 180 initial declarations have been received.
- 100% of the declared chemical weapons production facilities (CWPFs) have been inactivated. All are subject to a verification regime of unprecedented stringency. 64 of the 70 CWPFs declared to the OPCW have been either destroyed (43) or converted for peaceful purposes (21). 13 States Parties have declared CWPFs: Bosnia and Herzegovina, China, France, India, the Islamic Republic of Iran, Japan, the Libyan Arab Jamahiriya, the Russian Federation, Serbia, the United Kingdom of Great Britain and Northern Ireland, the United States of America, and another State Party.

Declared and inspected CW sites				
	States Parties which have declared Facilities	Declared Sites or Facilities	Inspections Conducted	Sites Inspected
Chemical Weapons Production Facilities	13	70	420	67
Chemical Weapon Destruction Facilities	6	37	1,309	37
Chemical Weapons Storage Facilities	7	38	426	36
Abandoned Chemical Weapons	3	35	55	25
Old Chemical Weapons	13	47	95	30
Total		227	2,305	195

Industry verification and non-proliferation



The world's chemical industry manufactures the compounds we depend on in our daily lives. Some very common chemicals can, if misused, be employed directly, or through further synthesis with other substances, as chemical weapons.

Together with governments, and with the support of the global chemical industry, the OPCW prevents the spread of chemical weapons.

From April 1997 to 30/09/2010, the OPCW has conducted 4,167 inspections on the territory of 81 States Parties, including 1,862 inspections of industrial sites. 1,103 industrial sites have been inspected out of a total of 5,450 declared.

Worldwide, 4,913 industrial facilities are liable to inspection.

International Cooperation in the Peaceful Uses of Chemistry

While the CWC seeks to ban chemical weapons, it also provides for international cooperation among States Parties in the pursuit of chemistry for peaceful purposes. International cooperation is promoted in many areas: from sponsoring chemical research to guaranteeing legal assistance; from developing and improving laboratory capacity to specialised internships and training in CWC implementation and safe chemical management. The provisions of the CWC have to be effectively and stringently implemented to ensure that a global chemical weapons ban is achieved. Support programmes, funded by the States Parties, enhance the OPCW's abil-

Declarations and inspections (Article VI of the CWC)				
	States Parties which have declared Facilities	Declared Sites or Facilities	Inspections Conducted	Sites Inspected
Schedule 1	22	27	212	36
Schedule 2	38	468	512	254
Schedule 3	36	491	295	234
Other Chemicals Production Facilities, incl DOC/PSF	80	4,464	843	579
Total		5,450	1,862	1,103

Programme	Description	Beneficiaries
Associate Programme	Established in 2000, it facilitates capacity building, industry-related national implementation of the CWC and promotes good practice in chemical manufacturing and safety.	181 Associates from Africa (72), Asia (50), Latin America (31), Eastern Europe (24) and Western Europe and Other States (4) have participated.
Analytical Skills Development Course	Established in 2004, it assists qualified analytical chemists to acquire further practical experience in the analysis of chemicals related to the national implementation of the CWC.	This course has benefited 186 chemists from Africa (75), Asia (42), Latin America (42), Eastern Europe (22) and Western Europe and Other States (5).
Conference Support Programme	Established in 1997, it facilitates the exchange of scientific and technical information, provides financial support for the organisation of conferences, workshops and seminars on special topics relevant to the CWC and facilitates participation in such events.	1,765 participants from Africa (506), Asia (392), Eastern Europe (355), Latin America and the Caribbean (233) have benefited from these events. In addition, the OPCW sponsored 190 events in Africa (40), Asia (42), Eastern Europe (37), Latin America (12) and Western Europe and Other States (59).
Research Projects Programme	Established in 1997, it assists small-scale research projects in targeted countries for the development of scientific and technical knowledge in the field of chemistry for industrial, agricultural, research, medical and other peaceful purposes relevant to the CWC.	382 projects in Africa (135), Asia (118), Eastern Europe (2), Latin America (124) and Western Europe and Other States (3) have benefited from this programme.
Internship Support Programme	Scientists and engineers from developing countries conduct advanced research in laboratories in industrialised countries.	76 interns from Africa (39), Asia (18), Eastern Europe (7), Latin America (11) and Western Europe and Other States (1) have so far been supported by the OPCW.
Laboratory Assistance Programme	Established in 1997, it aims at improving the technical competence of laboratories engaged in chemical analysis and monitoring.	61 laboratories in Africa (22), Asia (17), Eastern Europe (7), Latin America (14) and Western Europe and Other States (1) have benefited from this programme.
Equipment Exchange Programme	Facilitates the transfer of used and functional equipment to publicly funded laboratories and other academic institutions in developing countries from institutions in industrialised countries.	68 transfers in Africa (27), Asia (9), Eastern Europe (12), Latin America (19) and Western Europe and Other States (1) have been undertaken.

ity to hinder prohibited activity and to extend the benefits of peaceful uses of chemistry to all. The OPCW Associate and Internship Support programmes provide specialised training in modern industrial practices and skills development to chemists and engineers from States Parties whose economies are either developing or are in transition. Industrial internships and research projects provide insight into best-practice methodology in the safe management of chemicals and in the implementation of the CWC. The Secretariat supports the exchange of scientific and technical information among States Parties to promote the peaceful uses of chemistry. A variety of research projects in developing countries are also funded in part by the OPCW. Research in any of the following areas may be considered for financial support: environmentally sound technologies for the destruction of hazardous chemicals, analytical detection systems for toxic chemicals, safer alternatives to Scheduled chemicals, medical treatment for accidental exposure to hazardous chemicals, and practical applications for natural products in agriculture and medicine.

From Entry into Force of the CWC (29/4/1997) to 31/12/2008, the International Cooperation programmes have had 2,909 beneficiaries, including 186 analytical chemists, 181 Associate Programme participants, 1,765 Conference Support participants, 76 interns, 190 conferences, 61 laboratories, 382 research projects, and 68 transfers of used and functional equipment.

Beneficiaries by region: Africa (916), Asia (688), Latin America and the Caribbean (486), Eastern Europe (466) and Western Europe and Other States (353).

The following table describes the different international cooperation programmes run by the OPCW and the number of beneficiaries, including a regional breakdown, for each of them, since Entry into Force of the CWC in April 1997.

Protecting Each Other

Chemical weapons are frightening and dreadful weapons. They inflict excruciating and long-term suffering on a mass scale. Some States Parties have the capacity to protect their populations against chemical weapons, while others do not. All States Parties have pledged to provide assistance and protection to fellow Member States threatened by the use of chemical weapons or attacked with chemical weapons. Resources from a Voluntary Fund for Assistance, as well as individual offers of equipment and trained personnel, are available, should the need arise to swiftly dispatch assistance and expertise. A network of protection experts consults regularly on the means to improve the ability of States Parties to respond to the use of chemical weapons and to protect civilian populations. If a State Party requests assistance, the Technical Secretariat is responsible for the effective coordination of the assistance and protection measures provided by States Parties. These capabilities can include expertise in predicting hazards, in detecting and decontaminating chemical agents, in medical relief, and in on-site coordination with humanitarian and disaster response agencies.

Latest updates on assistance and protection:

- The OPCW Technical Secretariat organises courses aimed at providing training to first responders, government experts and emergency response units in building and developing national and regional capabilities and emergency response systems against the use, or threat of use, of chemical weapons. 2,200 participants from Africa (350), Asia (600), Latin America (500) and Eastern Europe (750) have benefited.
- 76 States Parties have pledged assistance under paragraph 7 of Article X.
- 129 States Parties have provided information on national programmes related to protective purposes, paragraph 4 of Article X.
- 43 States have contributed to the Voluntary Fund for Assistance.
- Balance of the Voluntary Fund for Assistance: EUR 1,362,849.76.

Status of Participation in the CWC

The OPCW States Parties already represent about 98% of the global population and landmass, as well as 98% of the worldwide chemical industry. The OPCW provides all States not Party to the CWC support in preparing to join the CWC and to effectively implement the global ban on chemical weapons. It is the fastest growing international disarmament organisation in history. The United Nations has called upon all States to join the CWC and to rid the world of the threat chemical weapons pose to international security.

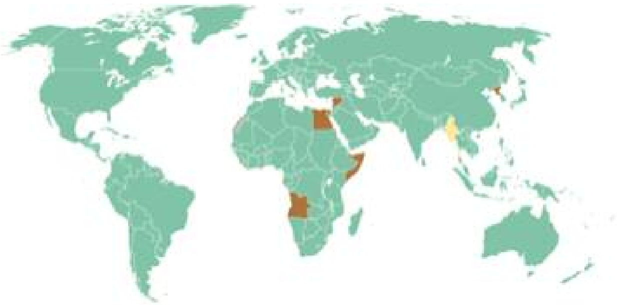
Signatory States which have not yet ratified the Chemical Weapons Convention

No.	State	Signature
1	Israel	13/01/1993
2	Myanmar	14/01/1993

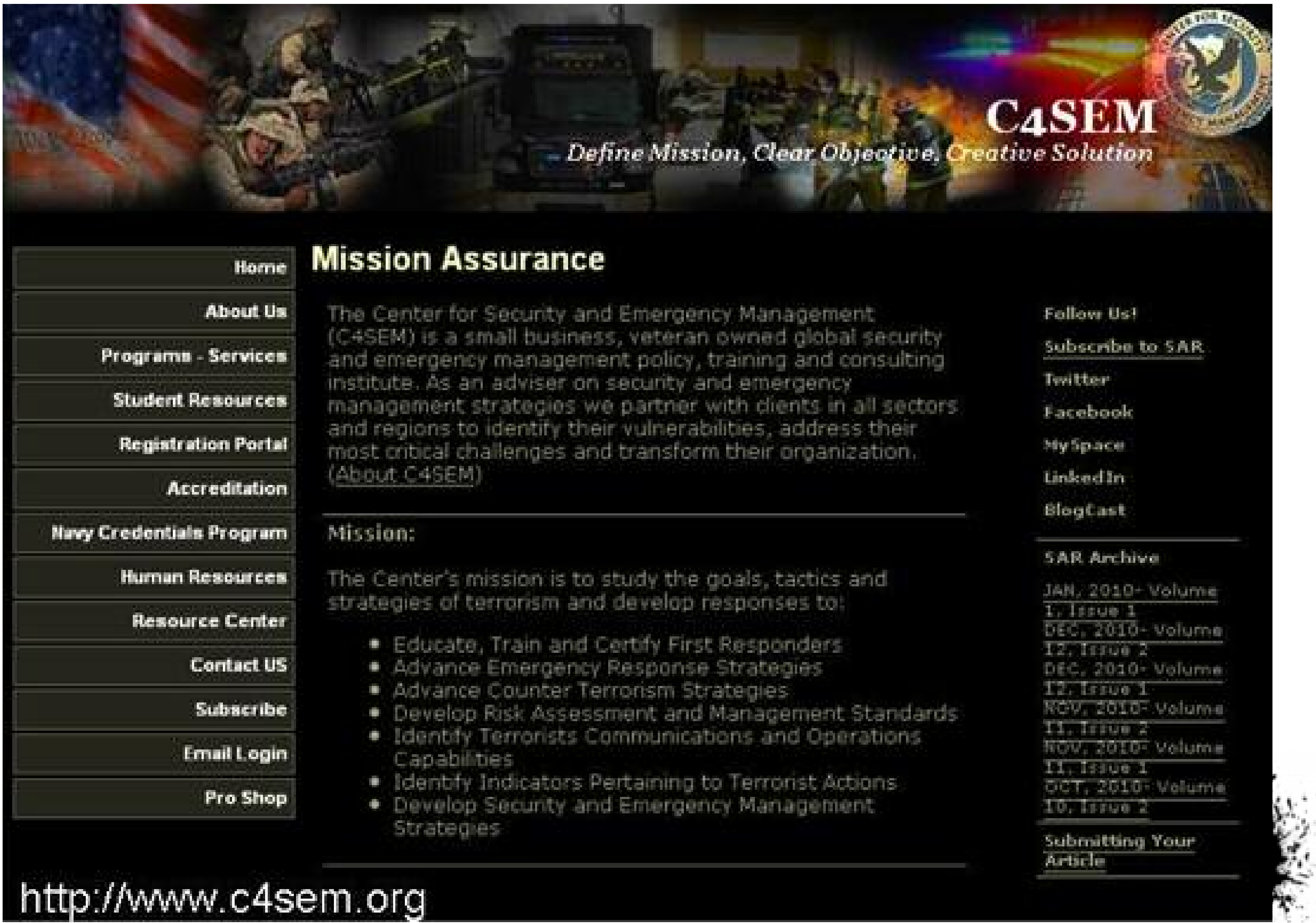
States that have neither signed nor acceded to the Chemical Weapons Convention

No.	State
1	Angola
2	Egypt
3	North Korea
4	Somalia
5	Syria

The map below shows States Parties (**green**), Signatory States (**yellow**) and Non-Signatory States (**red**).



Status of Participation in the Chemical Weapons Convention



Mission Assurance

The Center for Security and Emergency Management (C4SEM) is a small business, veteran owned global security and emergency management policy, training and consulting institute. As an adviser on security and emergency management strategies we partner with clients in all sectors and regions to identify their vulnerabilities, address their most critical challenges and transform their organization. (About C4SEM)

Mission:

The Center's mission is to study the goals, tactics and strategies of terrorism and develop responses to:

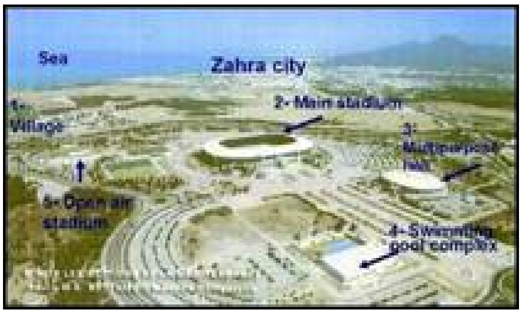
- Educate, Train and Certify First Responders
- Advance Emergency Response Strategies
- Advance Counter Terrorism Strategies
- Develop Risk Assessment and Management Standards
- Identify Terrorists Communications and Operations Capabilities
- Identify Indicators Pertaining to Terrorist Actions
- Develop Security and Emergency Management Strategies

http://www.c4sem.org

ASSISTEX 3 – The biggest international chemical exercise worldwide

By Ervin Farkas

The OPCW's third international Assistance and Protection Exercise (ASSISTEX 3), hosted by the Government of Tunisia, got underway Monday with the arrival of more than 400 specialists from 11 States Parties, the Technical Secretariat and the UN Office for the Coordination of Humanitarian Assistance (UN-OCHA) at a sprawling sports complex on the outskirts of Tunis where the exercise will take place. The scenario for the exercise will be a terrorist attack with chemical weapons against civilians during a sports event, combined with an investigation of alleged use (IAU). A State Party has requested assistance and protection from the OPCW against the threat of use of chemical weapons under Article X of the Chemical Weapons Convention. On Monday and Tuesday, specialized international teams arrive and deploy on the scene during the "threat phase", followed by two days of live exercise in response to an attack and investigation of alleged use on Wednesday and Thursday. The event will end on Friday with a VIP programme and closing ceremony. ASSISTEX 3 brings together national teams from the Czech Republic, Denmark, France, India, Italy, Spain, South Africa, Switzerland, Tunisia, Turkey and the United Kingdom, together with a regional team from the Caribbean and three sub-regional teams from North, West and East Africa. The combined international force includes specialists in all aspects of response and alleged use: reconnaissance, detection, decontamination, evacuation, medical support, sampling and analysis, search and rescue, and bomb disposal units. The joint operation is coordinated by a Local Emergency Management Authority (LEMA) staffed by Tunisian officials and an On-Site Operations Coordination Centre (OSOCC) joining the OPCW and UN-OCHA. During the first day of the threat phase on Monday, teams deployed and tested their equipment, including a field hospital and mobile laboratory. Command units were established to coordinate tasking; participants visited the various sites on location where the scenario will unfold to review the "injects", and local role players received instruction for the simulation activities. The exercise will be filmed by teams from Tunisian Television and the Vigili Fuoco (Fire Department) of Italy for training and promotional purposes. A large contingent of Tunisian and international journalists is expected for a special media program on Thursday.



ASSISTEX 3 Teams Complete Preparations

Preparations for the exercise were completed on Day 2 (Tuesday) with the assembly of all coordination units, national teams and equipment at the 7 of November Sport Complex outside of Tunis, together with final planning meetings to coordinate activities. During the initial 2-day preparatory "threat phase" of ASSISTEX 3, the OPCW Director-General has received a request for the OPCW to investigate a threat of use of chemical weapons and to assess the potential need for assistance and protection, and a mandate for such an operation has been prepared. Below is a selection of individuals representing various components of "Team ASSISTEX" and the tasks they and their teams will perform during the exercise on Wednesday and Thursday.

ERVIN FARKAS
ASSISTEX Directorate Staff, OPCW
"My job has been to prepare all operational field activities of the exercise, including writing the exercise script, scenario and injects, and to engage with the teams working together to prepare for a chemical weapons incident."

OLIVIER BRUYERE
Team Leader, UN Disaster Assessment and Coordination (UNDAC) /Head, On-Site Operational Command Center (OSOCC)
"UNDAC is a tool at the disposal of the host country and the UN family to coordinate the response to any kind of emergency, which tasks teams as an emergency unfolds and needs demand. In ASSISTEX I am performing as the head of OSOCC

JIYAU SINGH
Deputy Commander and Team Leader, India
"The India team is the largest contingent in ASSISTEX 3 and can provide a number of tasks in a chemical emergency – detection, decontamination, urban search and rescue, and evacuation, stabilization and pre-hospital care for casualties."

LADISLAV BELICKY
Mission Leader, OPCW
"As Mission Leader I coordinate the two main OPCW components of the exercise – assistance and response (ACAT) and the investigation of alleged use (IAU) – to ensure that necessary assistance against a chemical weapons attack is provided and that evidence of an attack is collected."

CRISTINA RODRIGUES
ACAT Team Leader, OPCW
"ACAT is the assistance, coordination and assessment team of OPCW. We liaise with LEMA, UN-OCHA and the national teams to ensure the delivery of assistance."

AYFE ROZ
Team Leader, Turkey
"We are a 5-person medical team with specialized training in national and CBRN (chemical, biological, radiological, nuclear) emergency response and working in Personal Protective Equipment. In this exercise we have a mobile medical unit and can perform pre-triage and emergency hospital care."

GIUSEPPE BENNARDO (left)
MARCO FREZZA (right)
Vigili del Fuoco, Italy
"The Italian team has a number of capacities. We can analyze air, water and soil samples with our mobile laboratory, decontaminate first responders, refill respirator tanks. We also have a special truck with an infrared sensor that can detect the presence of poison gas in the air up to a distance of 5 kilometres."

DANNY POIRET
Team Leader, East/South Africa Team
"We will be doing decontamination, search and rescue, first aid and evacuation, and backup for the investigation of alleged use. We've had specialized training as a group in these tasks in Uganda, Tanzania and Prague, with additional individual training in South Africa"

ASSISTEX 3 Live Exercise: Day 1

Based on intelligence reports, the "Republic of Daniria" suspects that it may be attacked with chemical weapons by an armed separatist movement in October, possibly during a major sports event. As a State Party of the OPCW, under Article X of the Chemical Weapons Convention Daniria requests the OPCW to provide assistance and protection against the threat of use of chemical weapons, and an investigation of alleged use. After considering the information provided by Daniria, the OPCW approves the request. The Director-General authorizes the dispatch to Daniria of a team from the Technical Secretariat to assess the threat, and to coordinate assistance and protection should it be needed. The OPCW also mobilizes specialized teams from other States Parties to provide assistance and protection support for the Danirian Government and an investigation of alleged use. On Wednesday morning, just as a sporting event was to begin at a stadium in Daniria, two vans exploded in the car park that released what appeared to be toxic chemicals. The prevailing winds carried the toxic vapor into a corner of the stadium, where within minutes pandemonium erupts. Spectators are exposed to the vapor and disabled, many of them with symptoms of concentrated exposure. Units of the Danirian government authority and international teams coordinated by the OPCW arrive on the scene. They undertake detection activities, search and rescue, evacuation of casualties, and bomb detection and disposal. Casualties are rushed to mobile medical units for pre-triage, stabilization and treatment. At the same time, evidence of suspected toxic chemicals is found in and around the sport stadium, where samples are collected and sent to a mobile laboratory for analysis.

ASSISTEX 3 Live Exercise Continues

On the second day of the live exercise, activities shifted locale to the nearby village of "Santar". Following the previous day's attack on the stadium, the local mayor has sent an urgent request for training of residents to protect themselves against a possible assault on the village with chemical weapons. Units of the ASSISTEX force are deployed to Santar and quickly instruct 20 villagers in the use of

Personal Protective Equipment (PPE). In due course, residents in the area discover two unexploded grenades and two suspicious packages that may be Improvised Explosive Devices (IEDs) at the gate to the village. The ASSISTEX command center is notified and deploys a bomb disposal team to the scene. They safely recover the grenades and one of the IEDs. On examining the second IED, the disposal expert suspects it may be rigged with a chemical weapons agent. A mobile x-ray 'gun' that can detect chemical agent from up to 30 meters is trained on the IED but finds only a conventional explosive, and the device is disposed of with a blast from a high-pressure water cannon. Around noon, Santar is struck with chemical weapons rockets. The ASSISTEX command post deploys all available national and international assets to the village. The trainees don their PPEs and search the village and surrounding area for casualties. With the assistance of international search-and-rescue teams, more than 80 casualties are brought to a mobile medical unit that has set up outside the 'hot zone' around the village. The casualties receive pre-triage to ascertain the severity and nature (chemical/non-chemical) of their injuries, are decontaminated, and then removed from the area for treatment at a mobile hospital according to their injuries. Meanwhile, an OPCW Investigation of Alleged Use (IUA) sampling team arrives and takes water samples from a well inside the hot zone. After external decontamination, the sample containers are transferred to an OPCW mobile laboratory for analysis to identify the chemicals. Under OPCW escort to maintain chain of custody, a split sample is then escorted by OPCW personnel to the airport and shipped to a pre-determined certified laboratory for confirmation of the results. At the same time that events are playing out at Santar, the ASSISTEX command post receives reports of more suspected IEDs that have been found in a sports hall near the stadium, scene of the previous day's attack. Urban search-and rescue (USAR) specialists arrive to evacuate casualties and mark the locations of the suspected IEDs. Bomb disposal experts are then called in defuse the devices. At 15:45 on Day 2, the Local Emergency Management Authority (LEMA) declares the situation under control and ASSISTEX operations are concluded.

OPCW Director-General Has High-Level Meetings and Closes ASSISTEX 3 Exercise in Tunisia

The OPCW Director General, Ambassador Ahmet Üzümcü, visited Tunis on 14 and 15 October 2010 where he met with Tunisian Government ministers and participated in the closing ceremony of the ASSISTEX 3 international assistance and protection exercise. At the sport complex in Rades where ASSISTEX 3 was staged, the Director-General reviewed a display of the equipment used by participating national teams together with a commercial exhibition of equipment for protection against chemical weapons. He then participated in the closing ceremony with H.E. Mrs Saida Chtioui, Tunisia's State Secretary for Foreign Affairs, and H.E. Mr Vaidotas Verba, Chairman of the Conference of the States Parties to the CWC. Director-General Üzümcü expressed his appreciation to the Tunisian authorities for hosting ASSISTEX 3, and to the other participating OPCW States Parties*, the regional teams from North, West and East Africa and the Caribbean, and the United Nations Office for the Co-ordination of Humanitarian Affairs (UN-OCHA), for their active participation. Noting that the threats associated with use of chemical weapons by non-state actors have created increased interest in the OPCW's coordination of emergency assistance to States Parties, he stressed that the Organisation must maintain a state of readiness to respond to requests for assistance in a timely and efficient manner, including provision of emergency assistance and coordination with various agencies in the field. The Director-General further noted that ASSISTEX 3 was the first such exercise held outside Europe, and for the first time that it combined a mock investigation of alleged use of chemical weapons with an assistance and protection exercise. He stated that ASSISTEX 3 had enabled the OPCW to test the scope of its cooperation and coordination with other organisations, local emergency management authorities and emergency response units, and that participating teams had the opportunity to test their own mandates and procedures. The Director-General said that the Technical Secretariat will carry out a comprehensive evaluation of ASSISTEX 3 and its performance, and based on the results achieved and the lessons learned, a follow-up plan will be drawn up and implemented in the coming months.

* Denmark, France, India, Italy, Libya, Spain, South Africa, Switzerland, Turkey, United Kingdom

ASSISTEX-3 and the mass media

FRENCH NEWSPAPER

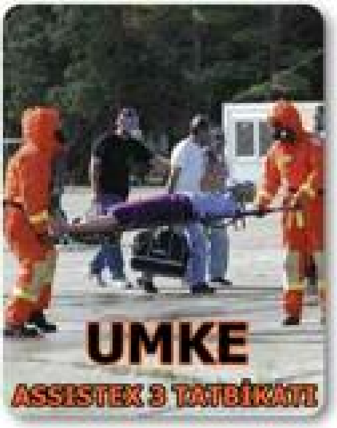
Tunis to host assistance exercise against use of chemical weapons

TUNISIAONLINENEWS- – From 11-15 October, 2010 the Organization for the Prohibition of Chemical Weapons (OPCW) will conduct its third exercise on the delivery of assistance and protection to states parties against the use of chemical weapons, in Tunis. The exercise, dubbed ASSISTEX 3, will be held at the 7 November Sports Complex at Rades, in Tunis, reported the Tunisian press agency on Wednesday. The exercise will focus on the OPCW's response to a request for assistance by a state party that has been threatened and attacked with chemical weapons. Participants will include specialized teams from Denmark, France, India, Italy, Libya, South Africa, Spain, Switzerland, Tunisia, Turkey and the United Kingdom, together with personnel from the OPCW Technical Secretariat in The Hague and the UN Office for the Coordination of Humanitarian Affairs. The program will include briefings, demonstrations, and a concluding press conference. The convention on the prohibition of chemical weapons came into force in 1997 and currently includes 188 member states, representing 98% of the world population and chemical industry.

ITALIAN NEWSPAPER

Chemical Weapons: ASSISTEX 3 Exercise Ends in Tunis

(ANSAmed) - TUNIS, OCTOBER 15 - The first to move among the wounded are the ''dirty men'' with breathing apparatus that nor only provide the lungs with oxygen but also inject oxygen into the suit that covers the every centimeter of skin, insulating the body: this is part of the ASSISTEX 3 simulation, the exercise against chemical weapons attacks that ended today in the Rades Stadium north of Tunis. This is the third exercise decided by the Organisation for the prohibition of chemical weapons (Organizzazione per la proibizione delle armi chimiche, OPAC), a body with offices in the Hague to which the United Nations assigned the implementation of the Paris Convention on the ban of chemical weapons that has been in force since April 1997 (CWC). The Convention was signed by 188 Countries that undertook to ban the production, develop-

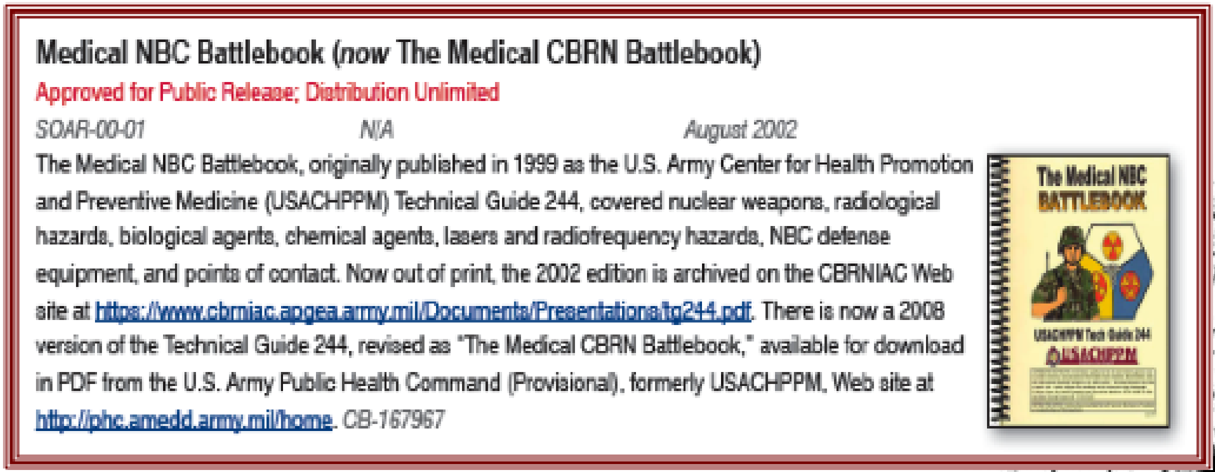


ment, storage and use of any chemical weapon and OPAC, which includes operational teams from 22 Countries, has the duty of intervening upon request by any Member State. ASSISTEX 3 in Tunis saw the involvement of more than 200 experts and observers from Algeria, Denmark, France, India, Libya, Spain, South Africa and Tunisia. Italy was present with 31 firemen, one of the largest fire fighting teams, led by Silvio Saffiotti, and ten vehicles equipped with cutting edge technology for detection, analysis, decontamination, reclamation and recharging of self protection devices. The exercise simulated in detail a chemical attack in the imaginary country of Daniria with men strewn on the ground acting as the wounded and the ''dirty men'' that first enter the ''cordoned'' area. Their task is to recover the wounded and to rapidly collect soil and air samples as well as any containers. The wounded and the champions are then handed over to the ''clean teams'' that lie outside the contaminated area. The wounded are transported to decontamination showers, and samples to analysis facilities. The life of the affected men depends on the speed of technicians in identifying the toxic agent, Sarin, Soman, Tabun, VX, or Ea 5774, and delivering the suitable antidote. (ANSAmed).

TUNISIAN NEWSPAPER
Third ASSISTEX 3 drill ends in Tunis

TUNISIAONLINENEWS- The third drill in assistance and protection against use of chemical weapons, "ASSISTEX 3," which started on October 11, ended on Friday, at the Radès November 7 Sports City. The closing day of the exercise was chaired by Secretary of State for Foreign Affairs in charge of American and Asian Saida Chtioui, with attendance of Mr. Ahmed Uzumcu, Director- General of the Organization for the Prohibition of Chemical Weapons (OPCW) and ambassador Vaildotas Verba, chairman of the Conference's member-states. The secretary of state stressed that the organization of this drill in Tunisia, as instructed by President Ben Ali, demonstrates Tunisia's unfailing attachment to the noble targets defined in the Convention of Prohibition of Chemical Weapons, given the country's conviction of the importance of solidarity and international co-operation and commitment to serve the causes of peace and security in the world. For his part, Mr. Ahmed Uzumcu, OPCW Director-General, underscored Tunisia's efforts to guarantee success of this drill, which was an occasion for the OPCW member countries to boost their capacities and develop their skills in the field of protection against likelihood of chemical attacks. On the fringes of this drill, an exhibition/display of protection equipments against chemical weapons was organized. (Source/TAP)

More on ASSISTEX-3 @ www.opcw.org



Medical NBC Battlebook (*now* The Medical CBRN Battlebook)

Approved for Public Release; Distribution Unlimited

SOAR-00-01 *N/A* *August 2002*

The Medical NBC Battlebook, originally published in 1999 as the U.S. Army Center for Health Promotion and Preventive Medicine (USACHPPM) Technical Guide 244, covered nuclear weapons, radiological hazards, biological agents, chemical agents, lasers and radiofrequency hazards, NBC defense equipment, and points of contact. Now out of print, the 2002 edition is archived on the CBRNIAC Web site at https://www.cbrniac.apgea.army.mil/Documents/Presentations/tg244.pdf. There is now a 2008 version of the Technical Guide 244, revised as "The Medical CBRN Battlebook," available for download in PDF from the U.S. Army Public Health Command (Provisional), formerly USACHPPM, Web site at http://phc.amedd.army.mil/home. *CB-167967*

POLICE
DHS
Do not remove
identiFINDER 2
0.094 µSv/h
0.000 cps
icx technologies
L
M
R

Pakistan floods released tons of toxic chemicals

Source: http://homelandsecuritynewswire.com/pakistan-floods-released-tons-toxic-chemicals

photo G Mendel

The floods in Pakistan earlier this year, in addition to forcing about 20 million people out of their homes, also released long-lived chemicals, known collectively as persistent organic pollutants (POPs); these include several banned pesticides and the insect repellent DDT; they are dispersed around the planet by atmospheric patterns, do not degrade naturally, and are linked to hormonal, developmental, and reproductive disorders, and increased risk of diabetes, cancer, and dementia. The floods that tore through Pakistan earlier this year, affecting twenty million people, released some 3,000 tons of dangerous chemicals into the environment. A report due to be published next year will warn that the event was not a one-off. Its findings were presented at the climate negotiations in Cancún, Mexico, earlier this week. The long-lived chemicals, known collectively as persistent organic pollutants (POPs), include several banned pesticides and the insect repellent DDT. They are dispersed around the planet by atmospheric patterns, do not degrade naturally, and are linked to hormonal, developmental, and reproductive disorders, and increased risk of diabetes, cancer, and dementia. Catherine Brahic reports that "Climate Change and POPs Inter-Linkages," published by the UN Environment Program, is the first study to look at how climate change will affect POPs, which are regulated under the UN Stockholm convention. It found that climate change increases the risks posed in several ways. Both measurements and models show that as evaporation increases with warmer temperatures, more of the chemicals are released from the land masses, rivers and lakes where they are stored. Once in the atmosphere, they can travel great distances. Likewise, glaciers lock away POPs, preventing them from causing more harm. Data shows, however, that as they are melting with global warming, their toxic load is being re-mobilized. Storms and extreme weather events like this year's floods in Pakistan are another factor in the release of POPs into the environment, when disasters release stockpiles stored in drums. Pakistan is a recent signatory or the Stockholm Convention and in 2009 it filed a preliminary audit of its POP stockpiles, stating that there were at least 6,000 tons of the chemicals locked up in stores around the country. According to Pakistan's audit, about half of the stores were in low-lying areas near bodies of water, including the areas that were flooded this year. Michael Stanley-Jones of UNEP yesterday told New Scientist that aerial surveys after the floods found that the facilities had been destroyed by the force of the water crashing through the flooded plains. Similar events took place after the Indian Ocean tsunami in 2004, said Donald Cooper, executive secretary of the Stockholm Convention, adding that more and more intense extreme weather events like this year's floods and fires put the hundreds of thousands of tons of stockpiled chemicals around the world at risk. "Throughout Asia and Africa there has been a large accumulation of old pesticides, many of which are POPs," says Cooper. In a bitter twist or irony, the pesticides were often sent by rich nations as aid, in response to a past food crisis. Excess pesticide could not be sent back and so was simply stored for an indefinite period.

IN A CHEMICAL NERVE AGENT ATTACK

Have No Regrets. Be Prepared.

By delivering the 2 recommended antidotes in an auto-injector, DuoDote® (atropine and pralidoxime chloride injection) offers the speed and simplicity to help you respond to poisoning by organophosphorous nerve agents or organophosphorous insecticides.[1-3]

To find out more about DuoDote® and for information on grant assistance, visit www.DuoDote.com or call 1-800-638-8093.

Indication

DuoDote® Auto-Injector (atropine and pralidoxime chloride injection) is indicated for the treatment of poisoning by organophosphorous nerve agents as well as organophosphorous insecticides.

DuoDote® Auto-Injector should be administered by emergency medical services personnel who have had adequate training in the recognition and treatment of nerve agent or insecticide intoxication. DuoDote® Auto-Injector is intended as an initial treatment of the symptoms of organophosphorous insecticide or nerve agent poisoning; definitive medical care should be sought immediately.

Important Safety Information

Individuals should not rely solely upon agents such as atropine and pralidoxime to provide complete protection from chemical nerve agents and insecticide poisoning. Primary protection against exposure to chemical nerve agents and insecticide poisoning is the wearing of protective garments including masks designed specifically for this use. Evacuation and decontamination procedures should be undertaken as soon as possible. Medical personnel assisting evacuated victims of nerve agent poisoning should avoid contaminating themselves by exposure to the victim's clothing.

In the presence of life-threatening poisoning by organophosphorous nerve agents or insecticides, there are no absolute contraindications to the use of DuoDote® Auto-Injector. When symptoms of poisoning are not severe, DuoDote® Auto-Injector should be used with extreme caution in people with heart disease, arrhythmias, recent myocardial infarction, severe narrow angle glaucoma, pyloric stenosis, prostatic hypertrophy, significant renal insufficiency, chronic pulmonary disease, or hypersensitivity to any component of the product. Elderly people and children may be more susceptible to the effects of atropine. DuoDote® Auto-Injector is Pregnancy Category C and should be used during pregnancy only if the potential benefit justifies the potential risk to the fetus. Safety and effectiveness in children have not been established.

Muscle tightness and sometimes pain may occur at the injection site.

The most common side effects of atropine can be attributed to its antimuscarinic action. Pralidoxime chloride can cause changes in vision, dizziness, headache, drowsiness, nausea, tachycardia, increased blood pressure, muscular weakness, dry mouth, emesis, rash, dry skin, hyperventilation, decreased renal function, excitement, manic behavior, and transient elevation of liver enzymes and creatine phosphokinase. When atropine and pralidoxime are used together, the signs of atropinization may occur earlier than might be expected when atropine is used alone.

DuoDote® AUTO-INJECTOR

(atropine and pralidoxime chloride injection)

READY TO RESPOND

Please see brief summary of full Prescribing Information on adjacent page.

References: 1. Agency for Toxic Substances and Disease Registry. Medical Management Guidelines (MMGs) for nerve agents: tabun (GA), sarin (GB), soman (GD), and VX. http://www.atsdr.cdc.gov/MHMI/mmg166.html. Updated August 22, 2008. Accessed May 20, 2010. **2.** DuoDote Auto-Injector [package insert]. Columbia, MD: Meridian Medical Technologies, Inc.; 2007. **3.** Robinson T, Clements BW, Bailey JA, Evans RG. Organophosphate antidote auto-injectors vs. traditional administration: a time motion study. J Emerg Med. 2009;37(2):139-143.

MERIDIAN MEDICAL TECHNOLOGIES™

Napolitano Urges Allies to Crack Down on Bomb-Making Material

Source:http://www.foxnews.com/politics/2011/01/05/napolitano-counterterrorism-focus-shipments-everyday-chemicals/#ixzz1AHZkSpXb

Homeland Security Secretary Janet Napolitano is warning America's allies in the fight against terrorism that they must expand the monitoring of the global supply chain to include everyday substances that can be used to make weapons. «It can be ... chemicals used in the manufacture of bombs, but you're also talking chemical, biological, potentially radiological (weapons),» she said, speaking exclusively to Fox News. «All the things that we need to be concerned about in today's threat environment.» It's an argument Napolitano is expected to be making quite a bit in the days to come. On Thursday, Napolitano and officials from the Department of Homeland Security and White House will be meeting here behind closed doors with the World Customs Organization, the only intergovernmental group devoted exclusively to customs matters. Napolitano will then wrap up her week-long, security-focused trip to Afghanistan, the Middle East and Europe with remarks at the European Policy Center, a Brussels-based think tank. Aides wouldn't offer details about what she will say, but one official said to expect a call for «expansion» of global efforts to monitor and secure potentially dangerous substances, particularly the 14 so-called «precursor chemicals» that are legal but causing so many problems in Afghanistan and elsewhere. According to a statement from the European Policy Center, Napolitano will «share her vision for securing the global supply chain through a layered security approach to identify, deter and disrupt threats in partnership with Europe and other international actors.» A year ago, the U.S. government and world partners, led by the World Customs Organization, launched an initiative called Global Shield, focusing on chemicals such as ammonium nitrate, which can be found in standard fertilizer and is used in more than 80 percent of the homemade bombs used by insurgents in Afghanistan. Napolitano started her overseas trip in Afghanistan, where dozens of officials from her department, particularly from Customs and Border Protection and the U.S. Border Patrol, are training Afghan security forces to conduct customs operations. Napolitano got a first-hand look at the Torkham border crossing along the Afghanistan-Pakistan border. She said her department «started» its efforts by addressing precursor chemicals «because that's such a top priority, keep the tools out of the hands of terrorists.» «But as you know from last October when we had the attempt to get bombs hidden in toner cartridges onto cargo planes, cargo itself can become a target,» she said. «What we're really talking about here is what's called the global supply chain, how you protect it from terrorist attack. ... Given the global nature of commerce, it's very important that that supply chain itself remains free from attack.» In the end, one Homeland Security official said, Napolitano is in Brussels to «build» and «bulk up» international efforts to track precursor chemicals and secure the global supply chain. «How can someone smuggle a radiological weapon filled with chemicals into the United States by exploiting the global supply chain?» the official said. «There are multiple points into that supply chain, so there are multiple ways to disrupt it.» The official said the U.S. government is trying to be «proactive,» employing «intelligence-based» methods, analysis of shipping data from around the world, and information-sharing.

«You get at it by forming partnerships, and you get at it by working with the community of nations,» Napolitano said.

EDITOR'S NOTE: On Jan 8th a mailing addressed to the nation's homeland security chief ignited with a similar flash of fire and smoke at a D.C. postal processing facility.

Navigating the CBRN landscape of 2010 and beyond: towards a new policy paradigm

The Hague Centre for Strategic Studies
Erik Frinking, Tim Sweijs, Teun van Dongen and Aksel Ethembabaoglu

This report has been commissioned by TNO.
Source: http://www.hcss.nl/en/news/1322/The-CBRN-landscape.html

In times of tightening security budgets, the way in which countries prepare for Chemical, Biological, Radiological and Nuclear (CBRN) incidents, deserves renewed scrutiny. The 'one percent doctrine' – prepare for the worst, even if the worst is highly unlikely – which is the current dominant paradigm, may have to be set aside in favour of a more realistic approach. This involves the prioritisation of capabilities against C, B, R, or N in the analysis, prevention and response (APR) phases. This will have to be done against the background of limited availability of data on the intentions and capabilities of actors to actually use CBRN weapons and uncertainty about scientific developments in the field of chemistry, biology and nanotechnology.

This report seeks to inform both policymakers and the CBRN industry by analysing the nature and size of present and future CBRN-threats as perceived by the policymaking and the expert community. It also compares policy approaches in six countries (Canada, France, Germany, the Netherlands, the United Kingdom (UK) and the United States (US)) and two international organisations (NATO and the EU).

Current CBRN-threats and hazards

An analysis of how current CBRN-threats and hazards are perceived by policymakers from the countries analysed shows the following:

- There is a consensus on the importance of CBRN-threats. All six countries list CBRN-terrorism or other CBRN-weapon use and the proliferation of CBRN-weapons among the most important security threats;
- The supporting analysis of these countries as well as NATO and the EU consider CBRN-incidents as necessarily catastrophic, high impact phenomena. They do not consider the possibility of smaller CBRN-incidents;
- The general perception is that state actors have the capacity to acquire CBRN but are restrained to deploy them. The opposite holds true for non-state actors. Only Al-Qaeda is considered a CBRN threat.

The Hague Centre for Strategic Studies
Navigating the CBRN landscape of 2010 and beyond: towards a new policy paradigm
The Hague Centre for Strategic Studies Nº 01 | 01 | 10

The expert community does not concur with these assessments. Most notably, this community disagrees with the probability of terrorist actors committing a CBRN attack (which it deems less probable). The experts also present a more in-depth understanding of the consequences of the release of CBRN agents with different delivery methods (impact).

Future CBRN threats and hazards

There is a consensus that in the next five to fifteen years, potential future CBRN threats and hazards depend on technological and geopolitical developments related to the proliferation and use of CBRN materials. With respect to science and technology, experts expect:

- An increasing convergence of chemistry and biology;
- Tremendous advances in understanding and manipulating genes, cells, and organisms;
- Developments in the field of nanotechnology that may revolutionise dispersal methods.

With respect to materials:

- An increasing availability of CBRN materials;
- The potential to engineer (CB) materials from scratch;
- A growth in the number of dual-use materials and technology that pose major challenges to non-proliferation regimes.

With respect to intentions:

- A persistent intention on the part of state actors to acquire (new types of) CBRN capabilities;
- A persistent intention on the part of non-state actors to acquire (new types of) CBRN capabilities and in some cases an explicit desire to use these capabilities.

With respect to capabilities:

- Significantly fewer hurdles to state actor CBRN acquisition as a result of knowledge diffusion and economic globalisation;
- Fewer hurdles to non-state actor CBRN acquisition, although these will continue to exist;
- The emergence of a distinction between future and traditional BCW, with the former the prerogative of state actors while the latter may be within the reach of both state and non-state actors.

Overall, experts agree that in the 21st century, CBRN materials may be utilised and deployed as weapons in novel ways, both in the military and civil domain.

The CBRN-policy benchmark

The CBRN-policy benchmark, comparing the six countries mentioned above, reveals how countries formulate and execute their respective CBRN policies.

Our analysis found that:

- Some countries deal with CBRN as a single policy issue in its own right; other countries approach CBRN as part of a larger security policy approach;
- CBRN crisis management has shifted from the military to the civil domain resulting in a duplication of efforts;
- While capabilities have been strategically identified along the analysis, prevention and response (APR) phases, few countries have dedicated CBRN strategies.

On the basis of the findings and conclusions of each of the chapters, the following **eleven observations** are made. These observations are intended to help policymakers and industry navigate the complex CBRN landscape of 2010 and beyond. They are formulated around the scope of risk consideration, the assessment of risks (including probabilities, impact, and vulnerability) and capability requirements.

Observation 1

The worst case-scenario approach, which is prevalent in CBRN assessment conducted by states, neglects attention to smaller or milder CBRN incidents.

Observation 2

The focus on CBRN as a whole ignores the distinct characteristics of each of these components.

Observation 3

While current proliferation prevention mechanisms seem to work, it is questionable whether they can keep pace with technological developments and remain future proof.

Observation 4

Focus on loss of life has dominated the impact discussion at the detriment of other potentially damaging impacts, ranging from political and social instability to economic and ecological costs.

Observation 5
Existing CBRN risk assessment capabilities within and outside governments are generally crude and lack a more calibrated analysis and an integrated understanding of the risk posed by CBRN incidents.

Observation 6
The current risk assessments approaches primarily focus on the threat and impact components of risk, and less so on vulnerability.

Observation 7
As with other investments in the field of security, a transparent method to evaluate budget allocation and investment in capabilities, against risk reduction and potential economic gain is lacking.

Observation 8
Risk reduction efforts do not focus sufficiently on getting more value for money.

Observation 9
The CBRN efforts by military and civilian actors are uncoordinated and overlap.

Observation 10
Responsibility for CBRN protection is partly shifting from the public to the private sector. But the associated knowledge flow (what to protect against, how to protect, how to respond?) is not always keeping up with this movement.

Observation 11
National security concerns prevent division of tasks across borders. This hampers a more efficient and effective CBRN policy.

RIEAS Research Institute for European and American Studies

Objective
The objective of the Research Institute for European and American Studies (RIEAS) is to promote the understanding of international affairs. Special attention is devoted to transatlantic relations, intelligence studies and terrorism, European integration, international security, Balkan and Mediterranean studies, Russian foreign policy as well as policy making on national and international markets.

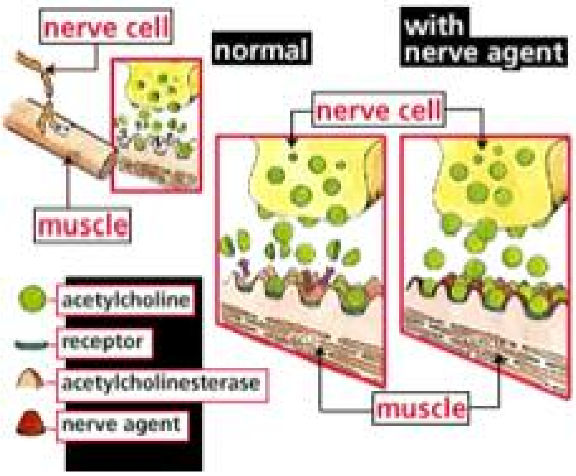
Activities
The Research Institute for European and American Studies seeks to achieve this objective through research, by publishing its research papers on international politics and intelligence studies, organizing seminars, as well as providing analyses via its web site. The Institute maintains a library and documentation center. RIEAS is an institute with an international focus. Young analysts, journalists, military personnel as well as academicians are frequently invited to give lectures and to take part in seminars. RIEAS maintains regular contact with other major research institutes throughout Europe and the United States and, together with similar institutes in Western Europe, Middle East, Russia and Southeast Asia.

Status
The Research Institute for European and American Studies is a non-profit research institute established under **Greek law (Greek Court registered no. 5427, April 6, 2006, Legal Document in Greek language)**. RIEAS's budget is generated by membership subscriptions, donations from individuals and foundations, as well as from various research projects. The Institute is autonomous organization. Its activities and views are independent of any public or private bodies, and the Institute is not allied to any political party, denominational group or ideological movement.

Protection Against Nerve Gas

Source: http://www.medicalnewstoday.com/articles/214657.php

Protection against nerve gas attack is a significant component of the defense system of many countries around the world. Nerve gases are used by armies and terrorist organizations, and constitute a threat to both the military and civilian populations, but existing drug solutions against them have limited efficiency. A multidisciplinary team of scientists at the Weizmann Institute of Science succeeded in developing an enzyme that breaks down such organophosphorus nerve agents efficiently before damage to nerves and muscles is caused. Their results have recently been published in the journal Nature Chemical Biology. Recent experiments performed in a U.S. military laboratory (USAMRICD) have shown that injecting a relatively small amount of this enzyme into animals provides protection against certain types of nerve agents, for which current treatments show limited efficacy. Nerve agents disrupt the chemical messages sent between nerve and muscle cells, causing loss of muscle control, and ultimately leading to death by suffocation. Nerve agents interfere with the activity of acetylcholinesterase, the enzyme responsible for the breakdown of the chemical messenger - acetylcholine. As a result, acetylcholine continues to exert its effect, resulting in constant muscle contraction throughout the body. Several drugs exist that are used to treat cases of nerve agent poisoning. Although these drugs are somewhat effective when exposed to small doses of the nerve agent, they do not provide protection against high-dose exposure; they are not effective against all types of nerve agents; or they cause serious side effects. Neither are they able to prevent nor repair cerebral and motor nerve damage caused by the nerve agent. An ideal solution to the problem is to use enzymes - proteins that speed up chemical reactions - to capture and break down the nerve agent before it gets the chance to bind to the acetylcholinesterase, thereby preventing damage. The main obstacle facing the realization of this idea, however, is that nerve agents are man-made materials and therefore, evolution has not developed natural enzymes that are able to carry out this task. Scientists worldwide have previously succeeded in identifying enzymes that are able to break down similar materials, but these enzymes were characterized by low efficiency. Large amounts of the enzyme were therefore required in order to break down the nerve agent, rendering their use impractical. This is where Prof. Dan Tawfik of the Weizmann Institute's Biological Chemistry Department enters the picture. Tawfik's group developed a special method to artificially induce «natural selection» of enzymes in a test tube, enabling them to engineer «tailor-made» enzymes. The method is based on introducing many mutations to an enzyme, and scanning the variety of mutated versions that were created in order to identify those that exhibit improved efficiency. These improved enzymes then repeatedly undergo further rounds of mutations and selection for higher efficiency. In previous studies, Tawfik showed that this method can improve the efficiency of enzymes by factors of hundreds and even thousands. For the current task, Tawfik selected an enzyme that has been extensively studied in his laboratory, known as PON1. The main role of this enzyme, found naturally in the human body, is to break down the products of oxidized fats that accumulate on blood vessel walls, thus preventing atherosclerosis. But PON1 seems to be a bit of a «moonlighter» as it has also been found to degrade compounds belonging to the family of nerve agents. However, because this activity has not fully evolved and developed



through natural selection, its efficiency in carrying out the task remains very low. But by using the directed evolution method, scientists hope that they will be able to evolve this random «moonlighting» activity into PON1's main «day job,» which would be carried out more quickly and efficiently than before. In the first phase, Tawfik and his team, including research fellow Dr. Moshe Goldsmith and postdoctoral student Dr. Rinkoo Devi Gupta, induced a number of mutations in PON1 - some random and others directed at key sites on the enzyme. To identify the most effective PON1 mutants, the scientists joined forces with Yacov Ashani of the Structural Biology Department. The method that the scientists developed closely mimics what happens in the body upon exposure to nerve agents: They put the acetylcholinesterase in a test tube together with a specific mutant PON1 enzyme that they wanted to test, and added a small amount of nerve agent to it. In cases where the acetylcholinesterase continued to function properly, it could be concluded that PON1 rapidly degraded the nerve agent before it was able to cause damage to the acetylcholinesterase. After several rounds of scanning, the scientists succeeded in indentifying active mutant enzymes, which are able to break down the nerve agents soman and cyclosarin effectively before any damage is caused to the acetylcholinesterase. These mutant enzymes have been structurally analyzed by a team of scientists from the Structural Biology Department, which included Profs. Joel Sussman and Israel Silman, and research student Moshe Ben-David. Further experiments have shown that when these enzymes were given as a preventative treatment before exposure, they afforded animals near-complete protection against these two types of nerve agents, even when exposed to relatively high levels. The scientists plan to further expand the scope and develop preventive treatment that provides protection against all types of existing nerve agents. They are also trying to develop enzymes with high enough efficiency to be able to very rapidly break down the nerve agent so they could be used to prevent the lethal effects of nerve agents by injection immediately after exposure.

U.S. urged to update chem-bio defense efforts

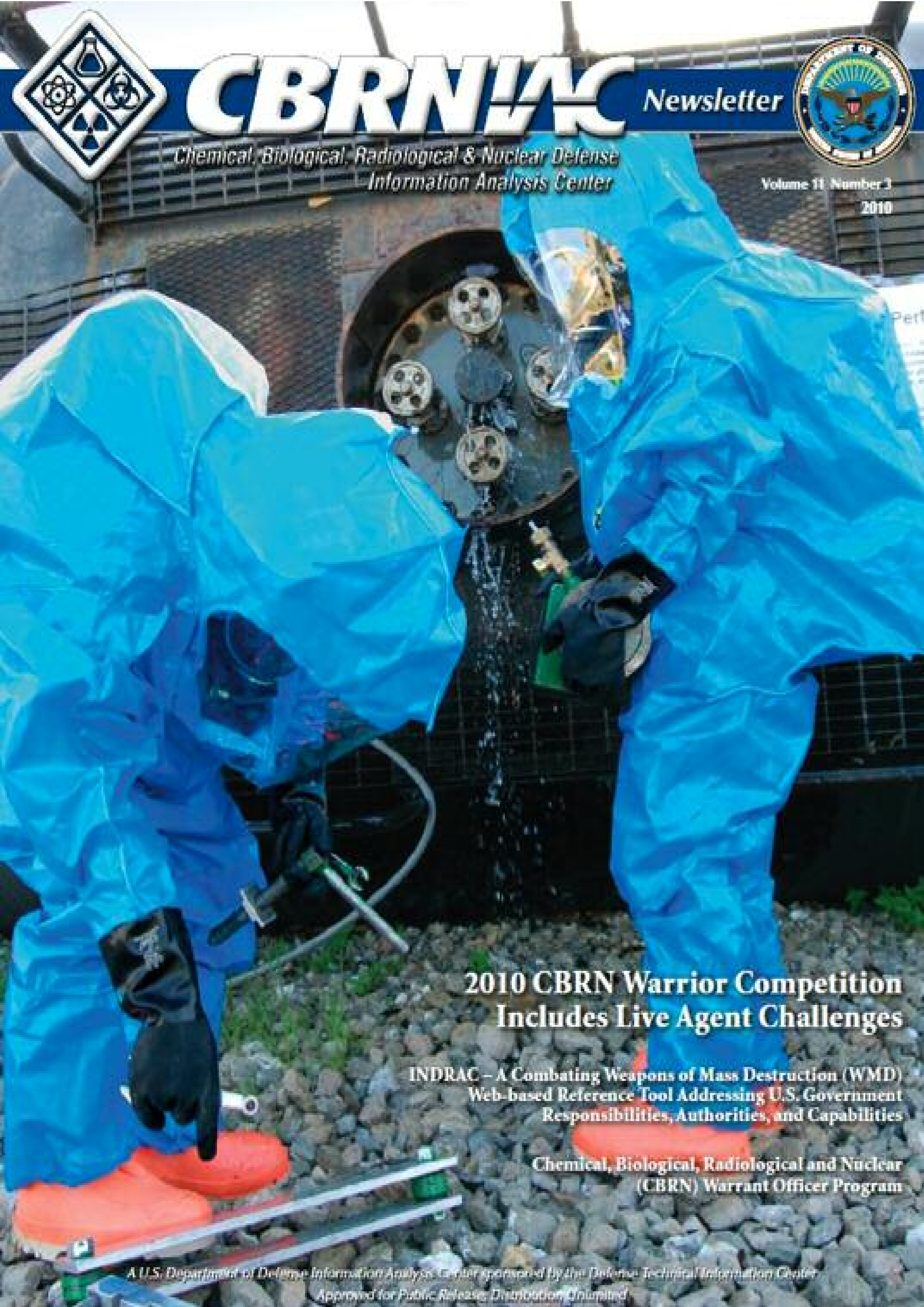
Source: http://homelandsecuritynewswire.com/us-urged-update-chem-bio-defense-efforts

A new report highlights one of the major problems in preparing defenses against chemical and biological (CB) agents: «Given the inherent secrecy with which states and other actors will conduct CB agent development, adversary programs could acquire new CB agents years before U.S. defense planners recognize those agents—- And, after the U.S. intelligence community recognizes those CB agents as threats, the United States will probably need many more years to establish a comprehensive defense against them. Such gaps in CB agent defense capabilities pose a potentially serious risk to U.S. military operations». The U.S. Defense Department should revamp its chemical- and biological-weapon defense efforts in a bid to discourage antagonists from developing new lethal agents or employing such materials in a devastating attack, according to a newly published RAND Corp. report. Global Security Newswire quotes the report to say that, "Given the inherent secrecy with which states and other actors will conduct CB agent development, adversary programs could acquire new CB agents years before U.S. defense planners recognize those agents…. And, after the U.S. intelligence community recognizes those CB agents as threats, the United States will probably need many more years to establish a comprehensive defense against them. Such gaps in CB agent defense capabilities pose a potentially serious risk to U.S. military operations." There are a number of "key challenges" in dealing with biological and chemical threats, the report states: identifying creation of new weapons materials, comprehending those dangers, the years or even decades needed for countermeasure development, and the "extended time periods" required for deploying those systems. Mustard agent existed for decades before scientists understood its harmful genetic effects, and U.S. medical preparations for a soman attack are unfinished more than a half a century after the nerve agent's potential became known, the document notes. Physical countermeasures including protective suits and breathing apparatus could in many cases offer "some level of defense" against a wide range of agents, the report states. "But what of new agents developed specifically to exploit limitations in the existing CB defenses? What if detection is the trigger for donning protective gear, and U.S. detectors are incapable of sensing new categories of agents? These concerns pose real challenges for a program that delays the development of an operational defense strategy until potential CB threat agents are validated and well characterized." Improving U.S. military and allied preparations for chemical or biological strike would necessitate "broadening and adjusting" Pentagon Chemical and Biological Defense Program policies for obtaining new equipment, the report later adds. Various international developments have increased the probability of governments or other organizations developing new chemical or biological warfare capabilities, it says. The Chemical Weapons Convention forbids the stockpiling of known chemical-weapon agents and their constituent materials, but "some actors might try to avoid short-term treaty censure by pursuing agents and precursors not explicitly identified by the CWC and take similar action with biological weapons," says the analysis. "The adverse economic and political repercussions of developing new CB agents will likely compel actors to conduct their CB programs covertly, posing a range of problems for the international community," it adds. Scientific capabilities around the world are "accelerating" and "dual-use" manufacturing sectors have proliferated, raising additional concerns about the increasing availability of weapon-usable material and expertise, says the document. A number of "small yet technically competent nations" might consider a chemical or biological deterrent a potential asset, and recent high-profile incidents such as the 2001 anthrax mailings have shown that such agents can serve as "weapons of intimidation," it adds. "Potential proliferators are aware that the use of [chemical-weapon] agents in the past (for example, Italy in the 1930s and Iraq in the 1980s) did not result in the kind of swift punishment that supports deterrence," the report's authors wrote. "In the coming decades, these factors will likely increase the probability that the United States will face 'unknown' CB agent threats and CB agent threats against which existing CB defenses are inadequate even for U.S. military personnel," they said. The "best approach" to the threat would involve dissuading enemies from preparing new biological or chemical weapons systems, broadly deterring the use of such materials, and pursuing "immediate deterrence of specific adversary CB attacks and the ability to defeat such attacks," according to RAND. Components of this strategy would include "proactive CB defensive [science and technology], vigorous and well-funded defensive system development, and strategic communications"; a "convincing information offensive" that would persuade foes that the United States and its allies are prepared to deal with any biological or chemical threat; and an expanded and updated Chemical and Biological Defense Program purchase emphasis. "Successful initiatives in dissuasion and deterrence will depend on CB defensive programs that appear dynamic, progressive, and integrated with other Defense Department and national-level efforts in counterproliferation," the report states.

CBRNIAC Newsletter

Chemical, Biological, Radiological & Nuclear Defense
Information Analysis Center

Volume 11 Number 3
2010



2010 CBRN Warrior Competition Includes Live Agent Challenges

INDRAC – A Combating Weapons of Mass Destruction (WMD) Web-based Reference Tool Addressing U.S. Government Responsibilities, Authorities, and Capabilities

Chemical, Biological, Radiological and Nuclear (CBRN) Warrant Officer Program

A U.S. Department of Defense Information Analysis Center sponsored by the Defense Technical Information Center

The CBRNIAC's Products and Services are at Your Fingertips!

Visit the CBRNIAC Online to access CBRN Defense and Homeland Security scientific and technical information!

Shop for CBRNIAC Information Products

Browse the entire Product Catalog or shop online for Critical Reviews and Technology Assessments, Databases and Databooks, Handbooks and Training Aids, and State-of-the-Art Reports.

Access CBRNIAC Newsletters

Read the latest CBRNIAC Newsletter, access the Newsletter Archives, sign up for a free subscription to the hardcopy version of the newsletter, submit an article for publication consideration or request commercial advertisement space.

Submit an Inquiry

Get up to 4 hours of free assistance in answering your CBRN-related technical questions. The CBRNIAC responds to questions from U.S. DoD, other U.S. government agencies, DoD and federal contractors, and state and local government agencies that fall within the CBRNIAC's technical scope.

Initiate a Technical Area Task or Subscription Account

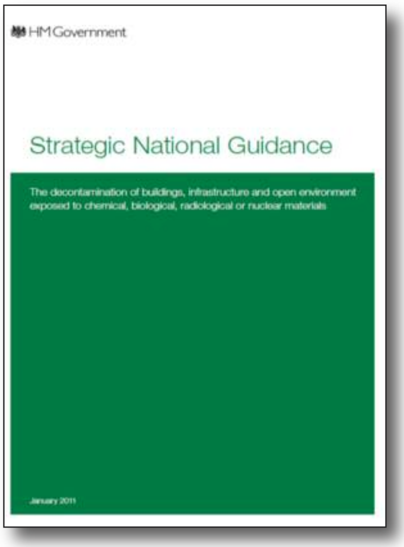
Technical Area Tasks (TATs) provide a pre-competed, convenient and responsive task-order contract vehicle for life-cycle coverage from basic research through fielding. Subscription accounts are "Mini-TATs." If you have an urgent requirement and need immediate support, a Subscription Account is a fast solution to shorter term needs.

http://www.cbrniac.apgea.army.mil/

U.K. Rolls Out New WMD Decontamination Protocols

Source: http://www.globalsecuritynewswire.org/gsn/nw_20110202_9676.php

The United Kingdom has issued new recommendations for the rehabilitation of contaminated buildings and other structures and outdoor areas following a WMD attack, the Center for Infectious Disease Research and Policy reported. The 50-page guidance paper prepared by the British Environment, Food and Rural Affairs Department amends 2004 recommendations for recovery operations following an unintended or deliberate chemical, biological, radiological or nuclear incident. The department said the recommendations cover a variety of entities, including private businesses and government organizations, and is intended to provide a beginning point for preparing for and responding to a crisis. The document addresses planning for coordination among various organizations and suggests strategies for establishing priorities when carrying out decontamination operations.



HM Government

Strategic National Guidance

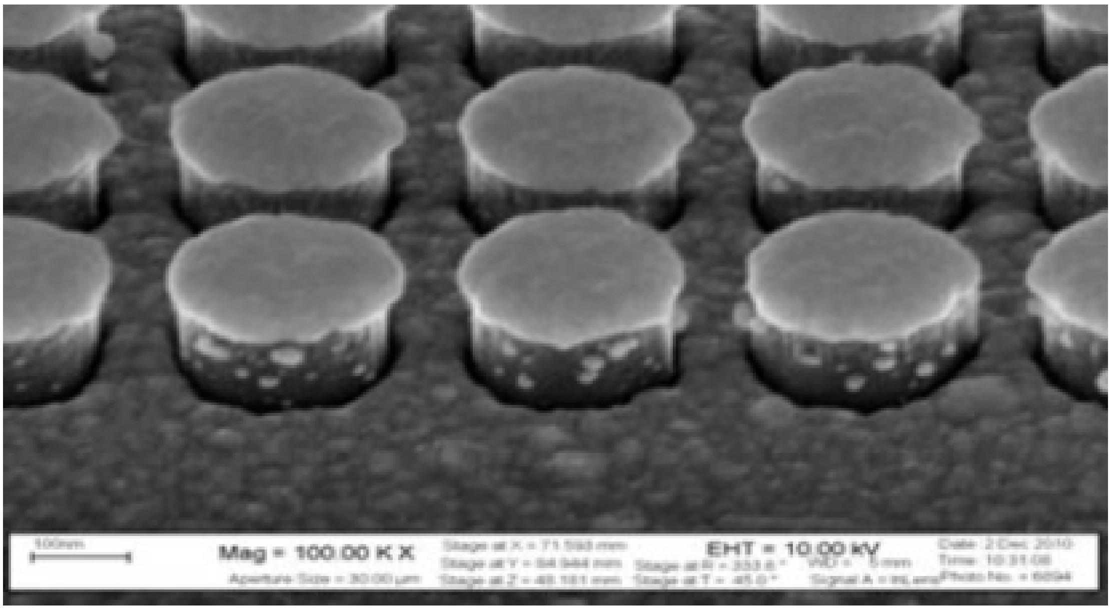
The decontamination of buildings, infrastructure and open environment exposed to chemical, biological, radiological or nuclear materials

January 2011

Warfighters Ready For Invisible Threats

Source: http://www.medicalnewstoday.com/articles/216289.php

In asymmetric warfare, early detection and identification of trace level chemical and biological agents and explosive compounds is critical to rapid reaction, response, and survivability. While there are many methods currently being used that can detect these threats, none allow for the unique fingerprinting of threat agents at trace levels. A research team, led by Drs. Joshua Caldwell and Orest Glembocki, scientists at the U.S. Naval Research Laboratory, Electronic Science and Technology Division, has overcome this limitation with surface enhanced Raman scattering (SERS) using optically stimulated plasmon oscillations in nanostructured substrates. Shown to provide enhancements of the Raman signal, large-area gold (Au) coated silicon (Si) nanopillar arrays are over 100 million times (108) more sensitive than Raman scattering sensing alone, while maintaining a very uniform response with less than 30 percent variability across the sensor area. «These arrays are over an order-of-magnitude more sensitive than the best reported SERS sensors in the lit



A 100,000 times magnified view of the gold coated, silicon nanopillars that make up the arrays used in the SERS measurements. Each array consists of 250,000 nanopillars with up to 400 arrays per wafer. Credit: U.S. Naval Research Laboratory

erature and the current state-of-the-art large-area commercial SERS sensors,» said Caldwell. «These arrays can be a key component of fully integrated, autonomously operating chemical sensors that detect, identify and report the presence of a threat at trace levels of exposure.» Raman devices use laser light to excite molecular vibrations, which in turn causes a shift in the energy of the scattered laser photons, up or down, creating a unique visual pattern. In the case of trace amounts of molecules in gases or liquids, detection through ordinary Raman scattering is virtually impossible. However, the Raman signal can be enhanced via the SERS effect using metal nanoparticles. Despite surface-enhanced Raman scattering being first observed in the late 1970s, efforts to provide reproducible SERS-based chemical sensors has been hindered by the inability to make large-area devices with a uniform SERS response. The ability to reproducibly pattern nanometer-sized particles in periodic arrays has finally allowed this requirement to be met. «While many tools are currently available to detect trace amounts of chemical warfare and biological agents and explosive compounds, a device using SERS can be used to identify these minute quantities of the chemicals of interest by providing a 'fingerprint' of the material, which all but eliminates the prevalence of false alarms,» says Glembocki. SERS offers several potential advantages over other spectroscopic techniques because of its measurement speed, high sensitivity, portability, and simple maneuverability. SERS can additionally be used to enhance existing Raman technologies, such as the hand held and standoff units that are already in use in field applications.

Multi-Role Respiratory Protective Equipment (RPE) System

Source: http://www.avon-protection.com/Protection%20US/Solutions%20by%20sector/viking-st53.htm

The ST53 TM combines Avon Protection Systems' FM53 mask with new and innovative modular breathing apparatus technology to provide positive pressure SCBA and PAPR capability. The ST53 TM system provides the operator with total flexibility to select the necessary level of protection quickly and efficiently whilst continuing to operate effectively at an incident. For the first time, the operational flexibility required by specialist users from their respiratory protection system is being offered in a purpose designed product. Depending on the threat or operational circumstances at the scene of an incident, ST53 TM can be configured to provide the ideal protection mode. Seamless transition between APR protection (negative pressure) and SCBA protection (positive pressure) ensures operatives can maximise their time on scene, whilst ensuring that the very highest levels of protection are available.

AVON PROTECTION

Features:

- The ST53 TM utilises the FM53 TM mask, designed specifically with military and law enforcement applications in mind.
- The FM53 TM system includes a unique close fitting filter design, giving the user greater visibility, improved weapon sighting and manoeuvrability.
- The ST53 TM backframe option includes a remote accessible, chest mounted pressure gauge for monitoring of pressure and a whistle for end of service alarm which has the option to be disabled if required.

- The ST53SD TM provides the option of either a remote whistle and pressure gauge or a single pressure gauge attached directly to the regulator body.

- The world's smallest, most compact chemically hardened demand valve provides constant positive pressure.
- Designed with stealth applications in mind including non reflective components and a warning whistle which can be silenced.
- For enhanced voice amplification, an optional Voice Projection Unit (VPU) with internal microphone can be connected via the Electronic Communication Port (ECP). The internal microphone may also be used for radio communications.
- The ST53 TM comes with a choice of 4.7 l – 9 l 300 bar lightweight carbon cylinders.

The ST53SD TM is available with either a 1 or 2 l 300 bar lightweight carbon wrapped 300 bar cylinder.

- Airline / decontamination attachments are available with the ST53 TM.
- Operator replaceable spare parts available, easy to maintain with access to key components.
- A wide range of fully compatible accessories such as hydration canteens, communication connections, vision correction system, clear, sunlight and laser outserts and a range of storage and carry bags.

WINTER
2010/11
£4.50/$8

The Circuit

The Magazine for Security Professionals

Back issues

Issue #9
Security Management

Issue #8
The Bodyguard Diary

Issue #7
Working Girl

Issue #6
Introduction to Close Quarter Pressure Points

Issue #5
A few industry do's & don'ts from across the pond

Issue #4
The Times They Are A Changing

Issue #3
Key Points to being a good bodyguard

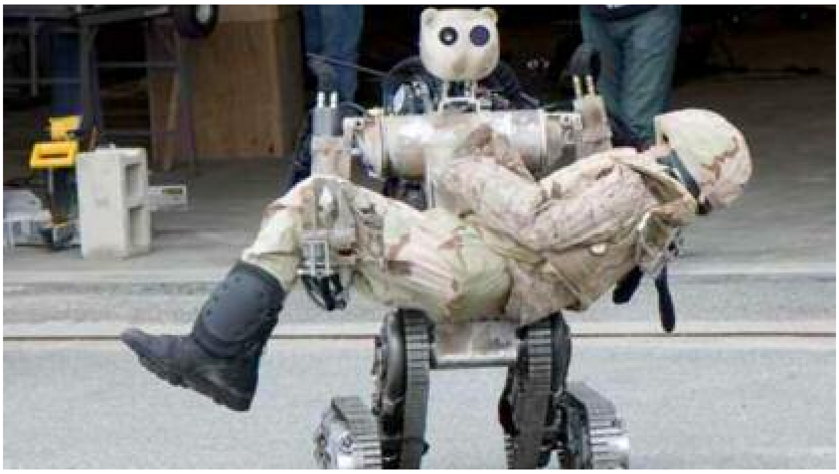
Issue #2
1st Aid For Close Protection

Issue #1
Interview with Elijah Shaw

A Quarterly publication from the British and North American Bodyguard Association

Battlefield Extraction-Assist Robot to ferry wounded to safety

Source: http://www.gizmag.com/battlefield-extraction-assist-robot/17059/

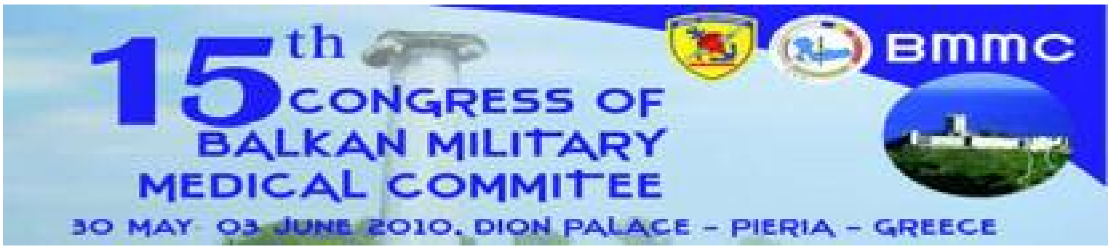


BEAR is an all-terrain, search-and-rescue humanoid robot that can lift and carry up to 500 pounds, yet can grasp fragile objects without damaging them (Image: TATRC)

The U.S. Army is currently testing a robot designed to locate, lift and carry wounded soldiers out of harm's way without risking additional lives. With feedback from its onboard sensors and cameras, the Battlefield Extraction-Assist Robot (BEAR) can be remotely controlled through the use of a special M-4 rifle grip controller or by hand gestures using an AnthroTronix iGlove motion glove. This equipment would allow a soldier to direct BEAR to a wounded soldier and transport them to safety where they can be assessed by a combat medic. Built by Vecna Robotics, BEAR maneuvers via two independent sets of tracked "legs" and is able to stand up and dynamically balance on the balls of its ankles, knees or hips while carrying a load. At full height BEAR stands 1.8 m (6 ft) tall, allowing it to look over walls or to lift its cargo onto a raised surface. To ensure it can handle a fully equipped soldier, BEAR's hydraulic arms are capable of carrying up to 500 pounds (227 kg), while its hands and fingers allow it to carry out fine motor tasks. It also has a "teddy bear" face that is designed to be reassuring. BEAR has been undergoing tests over the past year in simulations and live exercises by soldiers at the U.S. Army Infantry Center Maneuver Battle Lab at Fort Benning, Georgia. These tests are designed to provide BEAR's developers with feedback on the real-world operational capabilities and requirements for the robot. Anthronix, the makers of the iGlove, which is available commercially as the **AcceleGlove**, plans to develop a new glove for controlling the robot that will include more accelerometers and a digital compass to allow for greater control using only hand gestures – to instruct the robot to disable an improvised explosive device or travel exactly 500 meters east for example. The alternative method of remote control, a «Mounted Force Controller» which is mounted on the grip of an M-4 rifle, allows a user to control BEAR without having to put down their weapon. Currently all BEAR's actions are controlled by a human user but the developers are working to give BEAR more complicated semi-autonomous behaviors that will allow it to understand and carry out increasingly complicated commands. Vecna Robotics says BEAR could also be used for search and res

cue, handling hazardous materials, surveillance and reconnaissance, mine inspection, lifting hospital patients, or even warehouse automation. However, the battlefield is where we’re probably most likely to first see BEAR. “If robots could be used in the face of threats such as urban combat, booby-trapped IEDs, and chemical and biological weapons, it could save medics’ and fellow soldiers’ lives,» says Gary Gilbert of the U.S. Army Medical Research and Materiel Command’s Telemedicine and Advanced Technology Research Center (TATRC), which helped fund BEAR’s development.

EDITOR’S NOTE: BEAR might be a good alternative for extraction of CBRN contaminated casualties trapped in the “hot zone” following a real terrorist attack or an industrial accident.



EDITOR’S NOTE: Oral and poster presentations relevant to the thematology of the CBRNE-Terrorism Newsletter:

EVALUATING A NEWLY SYNTHESIZED OXIME CLINICALLY AND BIO-ANALYTICALLY IN ORGANOPHOSPHOROUS COMPOUND EXPOSURE

Authors: CPT. Zeki İlker KUNAK, MD. PhD[1]., , CPT. Nuri YILDIRAN, MD[2]., Tuna SUBASI, Chemıst[3]. LCDR Emin Özgür AKGÜL, MD[4]., CPT. Enis MACIT Pharm. PhD[5]., COL KENAR Levent MD. PhD[1]., LCDR Hakan YAREN, MD. PhD[1].

Institutions: (1) Gulhane Military Medical Academy, Dept. of Med. CBRN Def., Ankara, Turkey, (2) Gulhane Military Medical Academy, Dept. of Military Health Services., Ankara, (3) Turkey Mıddle East Technıcal Unıversıty, Faculty Of Chemistry, Ankara, Turkey, (4) Gulhane Military Medical Academy, Dept. of Med. Biochem., Ankara, Turkey, (5) Gulhane Military Medical Academy, Dept. of Toxicology, Ankara, Turkey

OBJECTIVE: In this study, it has been aimed to evaluate the oxime, named TS-131 besides atropin and obidoxime, whether it could be used as a wide spectrum enzyme reactivator and the therapeutic efficacy in organophosphorous compound exposure.

MATERIAL AND METHOD: Methyl paraoxon is a chemical which inhibits the cholinesterase enzyme irreversibly, similar with nerve agents. Anti-cholinergic agents (atropine) and enzyme re-activators (oximes) are used against organophosphorous cholinesterase inhibitors. Here, clinical effects and ability of reactivating the cholinesterase of both obidoxime and TS-131 – which we developed – are compared. Besides this we determined the plasma levels of both oxime by High Performance Liquid Chromatography, to evaluate the correlation with efficacy level. 70 male Sprague-Dawley have been used in the study. In order to compare the enzyme reactivation abilities, oximes have been administered 1 minute after exposure to methyl paraoxon. Cholin esterase activities of plasma and erythrocyte of the rats which have been exanguinated at the 30th m nute, have been measured via spectrometric method.

RESULTS: In terms of clinical therapy and enzyme reactivation, significant difference (p>0.05) between TS-131 and obidoxime have been found but it has been suggested that by increasing the dose, this difference might diminish especially in butyrilcholineesterase reactivation.

CONCLUSION: With this study, it has been suggested that, it is possible to use TS-131 for organophosphorous compound exposure but it will be proper to test TS-131 against other types of organophosphorous compounds with alternative dosages, determine the toxicity pharmacokinetic characteristics, proceed experiments on the distribution of the molecule in various tissues

BIOLOGICAL WARFARE AGENTS- EMERGENCY DETECTION AND MONITORING OF NATURAL FOCUS

Authors: Major MARINOV Krustyu MD PhD, GEORGIEVA Elena PhD, SAVOV Encho MD DNs

Institution: Military Medical Academy, Department of Military Epidemiology and Hygiene, Sofia, BULGARIA

Objective: The purpose of this presentation is to publish our experience, achievements and problems in identification of some bacterial species – agents of biological weapon. We report the results from our participation in international NATO exercises on sampling and identification of biological and chemical agents (SIBCA). Additionally, results from ten years monitoring of new natural focus of tularemia are reported.

Materials and Methods: Rapid methods for identification of etiological agents of anthrax, brucellosis, tularemia, plague and cholera were tested and used. Immunofluorescence methods and genetic methods- polymerase chain reaction were used. Isolation and characterization of tularemia strains from new focus of tularemia were performed by classical methods. Genotyping of the strains was performed by multilocus variable number tandem repeat analysis. Seroprevalence of F. tularensis among farm animals was investigated.

Results: The results from our participation in SIBCA exercises showed good practical readiness for participation in defense of Bulgarian army in case of biological attack. In study of tularaemia focus in an area where tularaemia had never been reported eight F. tularensis subsp. holarctica strains were isolated. The strains showed heterogeneity, based on acid production from glycerol and erythromycin susceptibility. Genotyping by analysis of seven loci containing variable-number tandem repeats showed four genotypes among eight strains.

PIRACY – TERRORISM OR CRIME

Authors: TONEV, Stoian; KOSTADINOV, Rostislav; KANEV, Kamen; ARSOV,Volodya

Institution: Medical Intelligence Ward, Chair Disaster Medicine and Toxicology, Military Medical Academy, Sofia, Republic of Bulgaria

A lot of articles have been published recently for the piracy, particularly around Somali coast. There are many authors describing Somali pirates as terrorists.

Aim: The aim of the article is to discuss the features of the modern piracy responding to the question about the pirates' nature – terrorists or criminals.

Material and Methods: In order to achieve the set goal pirates' activities are thoroughly analyzed. Descriptive and comparative methods were applied, along with deductive and cluster analyses.

Results: Somali pirates' activities are described and their features are highlighted. The results from analyzed in depth pirates objectives and methods are compared to the terrorists' aims and preferred mode of actions. Authors are considering the possible linkage between terrorists groups and pirates in Somalia as highly probable. On the other hand there are several and have to be noted distinguish dif ferences between Somali pirates and contemporary terrorist groups and organizations.

An attempt to find out the routes of piracy in the modern world is performed.

Conclusion: All obtained results coincide with the published analyses where contemporary piracy is described as criminal activity with probable link to terrorists' groups/organizations.

PREPAREDNESS FOR EMERGENCY RESPONSE AFTER EXPLOSIONS

Author: GALABOVA, A.; DRAGNEV V., MD,PhD

Institution: Disaster Medicine Scientific Research Laboratory, Military Medical Academy

Introduction: The moment of an explosion is unpredictable, owing to circumstances which can hardly be forseen, such as location and time of occurrence of accidents with explosive materials or terrorist acts. Therefore, it requires the organization and preparedness for the timely response of the emergency teams related to the problem.

Aim: The present material aims to outline the factors that affect the timely reaction of the forces involved in the response activities.

Material and methods: A literary reference was carried out concerning past explosions, problems were identified regarding the organization of the relief procedures.

Summary: Besides the typical for the explosions blast trauma, in this kind of incidents intoxications also occur due to the emitted toxic gases or chemical warfare agents use. The possibility a «domino effect» implies the creation of complicated emergency.

Conclusion: Blasts problems, as an integral part of the scientific discipline Disasters Medicine have their own specificity, which requires readiness and implementation of specific emergency measures to mitigate the consequences.

THE DISASTER TREATMENT PLANNER

Authors: Zvezdana Stojanovic MD; Col. Radomir Samardzic, MD, PhD; Zeljko Spiric MD, Ph.D, G. Mandic-Gajic, MD.Ph D.

Institution: Department of Psychiatry, Military Medical Academy, Belgrade

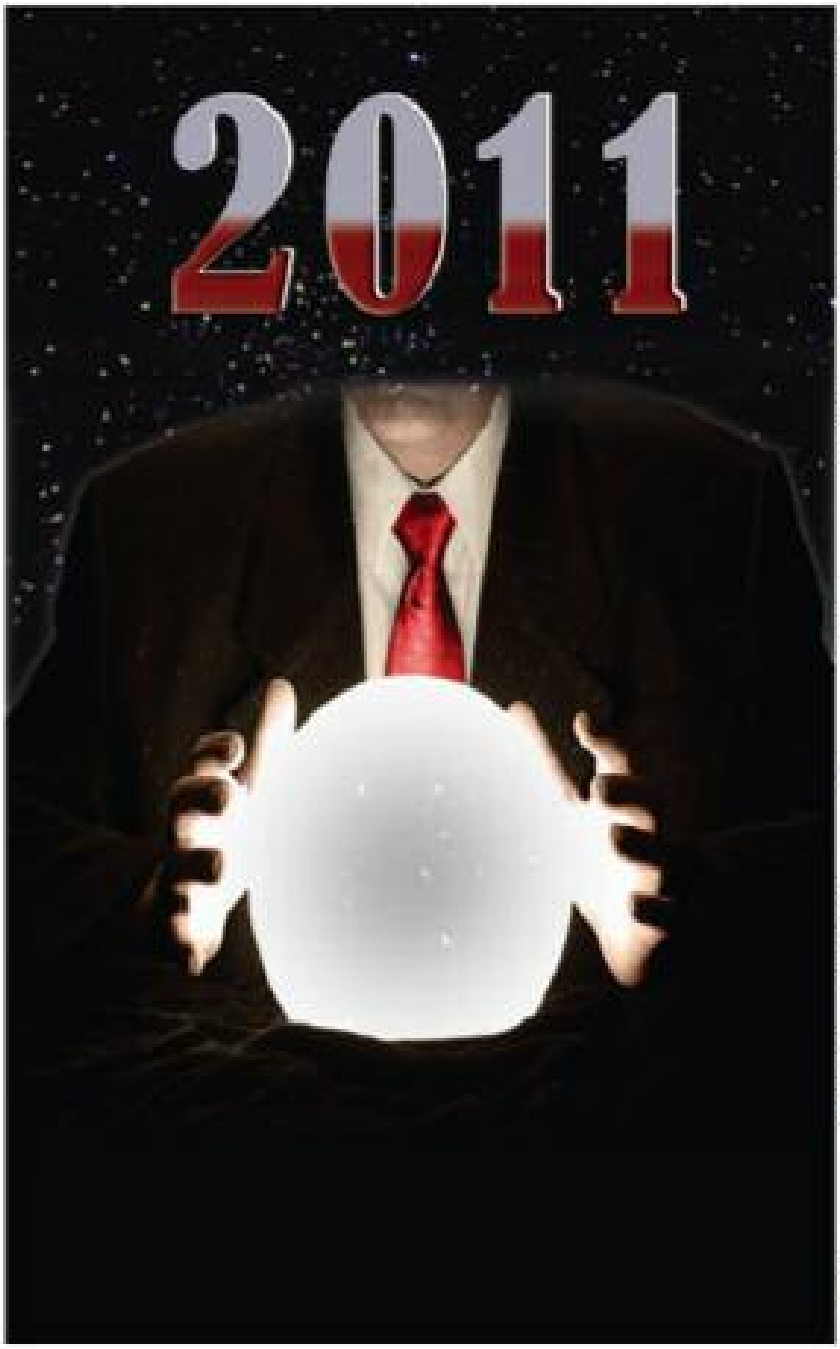
Purpose: People have become exposed to violent crises at an incidence rate that is alarmingly increasing. Individuals in crisis need specialized interventions that are unlike other forms of therapy. The treatment planner provides a framework to offer crisis intervention effectively, while incorporating the criteria necessary for managed care review and insurance reimbursement. The individual's strength and weaknesses, unique stressors, social network, family circumstances and symptom patterns must be considered for developing a treatment strategy. The aim of the disaster treatment plan is to consider a logical series of steps that include long-term goals, short-term objectives and therapeutic interventions.

Conclusion: The treatment planner for the disaster will promote effective, creative treatment planning starting with crisis intervention - a process that will ultimately benefit the client, clinician, and mental health community.

DomPrep Journal

US Annual $100 Volume 6 Issue 12, December 2010

FORECAST



Since 1998, Integrating Professional Communities of Homeland Security, Preparedness, Response & Recovery

Bio News

WikiLeaks reveals U.S. anxious over infrastructure vulnerability

Source: http://homelandsecuritynewswire.com/wikileaks-reveals-us-anxious-over-infrastructure-vulne-rability

Among the leaked documents released by WikiLeaks is a secret list of infrastructure-related facilities and topics, from pipelines to smallpox vaccine suppliers, whose loss or attack by terrorists could «critically impact» U.S. security in the view of the State Department; the February 2009 cable from the State Department requested overseas U.S. missions update a list of infrastructure and resources around the globe «whose loss could critically impact the public health, economic security and/or national and homeland security of the United States»; the list includes undersea cables, communications, ports, mineral resources, and firms of strategic importance in countries ranging from Austria to New Zealand. WikiLeaks has released a secret list of infrastructure-related facilities and topics, from pipelines to smallpox vaccine suppliers, whose loss or attack by terrorists could "critically impact" U.S. security in the view of the State Department. The February 2009 cable from the State Department requested overseas U.S. missions update a list of infrastructure and resources around the globe "whose loss could critically impact the public health, economic security and/or national and homeland security of the United States."

The cable asked diplomats to identify "systems and assets, whether physical or virtual, so vital to the United States the incapacitation or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." The cable is marked "secret state … noforn, not for internet distribution." "Noforn" means it should not be shown to foreign governments or other non-U.S. interests. AFP reports that based on responses from U.S. missions around the world, the Department of State prepared a list of critical infrastructure facilities, assets, and resources which are vital to U.S. national security and welfare. The list includes undersea cables, communications, ports, mineral resources, and firms of strategic importance in countries ranging from Austria to New Zealand. The cable said the State Department, in coordination with DHS, was seeking input from embassies on "critical infrastructure and key resources within their host countries which, if destroyed, would likely have an immediate and deleterious effect on the United States." It said diplomats were "not being asked to consult with host governments with respect to this request." The request came under the National Infrastructure Protection Plan, which aims to enhance protection of key resources "to prevent, deter, neutralize or mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate or exploit them; and to strengthen national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster or other emergency." The cable reveals a vast range of sites and firms seen as vital to national interests and security, ranging from major infrastructure such as the Panama canal and oil pipelines to Belgian medical firms and Italian and Australian companies which produce snake-bite treatments. In Europe, the Ludwigshafen plant of German chemical giant BASF was the "world's largest integrated chemical complex" while Siemens AG in Erlangen was responsible for "essentially irreplaceable production of key chemicals." The cable describes Russia's Nadym gas pipeline junction as "the most critical gas facility in the world."

In the Middle East, it notes that "by 2012 Qatar will be the largest source of imported LNG (liquefied natural gas)" to the United States. The hundreds of entries in the document leaked on Sunday also include mines and mineral resources in Africa and South America, undersea pipelines, cables, and ports in China and Japan, French medical and pharmaceutical companies and shipping terminals and crude oil refineries in the Middle East. In addition the list includes Danish and German suppliers of smallpox and rabies vaccines, British defense contractors and telecommunications facilities, chromite mines in India, and dams and hydro-electric projects in Canada which supply power to the United States. WikiLeaks created an international firestorm when it started releasing more than 250,000 classified State Department cables on 28 November, which have included embarrassing details of American diplomats' private assessments of foreign leaders.

""Targets for terror"

The Times reported reported the story with the headline "WikiLeaks lists 'targets for terror' against U.S."

"There are strong and valid reasons information is classified, including critical infrastructure and key resources that are vital to the national and economic security of any country," Crowley told he Times.

"Julian Assange (WikiLeaks's founder) may be directing his efforts at the United States but he is placing the interests of many countries and regions at risk. This is irresponsible," he added. The U.K. government also condemned the publication of the document. "The leaks and their publication are damaging to national security in the United States, Britain and elsewhere," a spokesman for the Prime Minister David Cameron said in a statement, according to NBC News. "It is vital that governments are able to operate on the basis of confidentiality of information." Sir Malcolm Rifkind, a British lawmaker who has served as both defense and foreign secretary, told the Times that the publication of the list was "further evidence that they (WikiLeaks) have been generally irresponsible," adding that it was "bordering on criminal." "This is the kind of information terrorists are interested in knowing," added Rifkind, who now serves as chairman of the British parliament's Intelligence and Security Committee.

An Evaluation of Bioregulators as Terrorism and Warfare Agents

*Slavko Bokan, **John G. Breen, *Zvonko Orehovec *MOD, Croatian Military Academy, Laboratory for NBC Protection, Ilica 256 b, HR-10000 Zagreb, Croatia ** Geneva, Switzerland

Source: http://www.asanltr.com/newsletter/02-3/articles/023c.htm

Introduction

Within neuroscience over the last twenty years there has been an explosion of knowledge about the receptor systems on nerve cells that are of critical importance in receiving the chemical transmitter substances released by other nerve cells. Bioregulators or modulators are biochemical compounds, such as peptides, that occur naturally in organisms. They are a potential new class of weapons that can damage the nervous system, alter moods, trigger psychological changes and even kill. These compounds can act as neurotransmitters and modify neural response. Bioregulators are closely related to substances normally found in the body that regulate normal biological processes. Their potential military or terrorism use is similar to that of toxins. Some examples of potential application of bioregulators are to cause pain, as an anesthetic and to influence blood pressure.

Together with increased research into toxins, the bioregulators have also been studied and synthesized. These substances can also be modified synthetically, whereupon they may obtain new properties. It is feasible to produce some of these compounds by chemical synthesis. It is apparent that the past decade has brought an enormous increase in knowledge about the pharmacology and structural biology of receptors.

In the last ten years considerable advances have taken place in this in vitro synthesis of peptides, and, already commercial production in large quantities of various pharmaceutical peptides are freely available. Synthetic derivates or slightly modified forms of these compounds can have drastically altered toxic effects and these could be important in the development of new agents. Advances in discovery of novel bioregulators, especially bioregulators for incapacitation, understanding of their mode of operation and synthetic routes for manufacture have been very rapid in recent time. Some of these compounds may be potent enough to be many hundreds of times more effective than the traditional chemical warfare agents. Some very important characteristics of new bioregulators that would offer significant military advantages are novel sites of toxic action; rapid and specific effects; penetration of protective filters and equipment and militarily effective physical incapacitation.

Peptide bioregulators are interesting regulatory molecules for many reasons. Their range of activity covers the entire living system, from mental processes (e.g. endorphins) to many aspects of health such as mood control, consciousness, temperature control, sleep, or emotions, exerting regulatory effects on the body.

This paper presents an evaluation of bioregulators according to criteria, which are used for evaluation of toxin warfare agents, and describes the main human bioregulators or modulators that can be used as terrorism delivery system or biological agents in hostile activities.

Materials and Methods

As the list of bioregulators will be hard to define, we propose two tables of bioregulators, with important criteria to enable decision to include these compounds from a list of bioregulators with potential as terrorism or biological warfare agents.

It is very hard to find in available literature all the data for all bioregulators, especially for the criterion: Agents known to have been developed, produced, stockpiled or used as weapons (in the tables - Weaponized). Therefore, we can not be 100% sure that data for this criterion are correct.

Many biological agents, in this case bioregulators, have the capacity to cause disease and potentially be used to threaten civilian populations. From a public health standpoint however, bioregulators which are less known, must be evaluated and prioritized in order to assure appropriate allocation of the limited funding and resources that are often found within public health systems.

Potential terrorism bioregulators with an expected mortality of >50% were rated higher (+++) than agents with lower expected mortalities (21-49% = ++, and <21% = +).

Bioregulators are rated higher (++) for morbidity if clinical disease requires hospitalization for treatment (including supportive care), and with lower rating (+) if outpatient treatment is possible for most cases.

We evaluated expected mortality in the same way as toxins: LD50 >50% were rated higher (+++) than agents with lower expected mortalities (21-49% = ++, and <21% = +).

Agents received (+) to (+++) for dissemination potential based on their environmental stability after release (+), their ease of production in large quantities (+) and distributed (+) as a agent in quantities that could effect large populations. High level of intoxication by a variety of routes - we rated according of the kind of exposure: per oral route (+), respiratory route (++), or both (+++).

Bioregulators also were ranked based on any special public health preparedness that might be required including: stockpiling of therapeutics (+), enhanced surveillance and education (+), improved laboratory diagnostics (+).

Public fear associated with an agent and the potential mass civil disruptions that may be associated with even a few cases of disease were also considered (+ to +++).

Results and Discussion

Our opinion is that if some bioregulator satisfies the bulk of the criteria, it should be recommended for inclusion in the list. Rankings of potential bioregulators according to important criteria are shown in the following Tables (1 and 2).

A. ENDORPHINS

Endorphins are small-chain peptides, which activate opiate receptors, producing feeling of wellbeing, tolerance to pain, etc. These compounds are hundreds or even thousands of times more potent than morphine on a molar basis. Because of this potency, their concentrations in vivo are low, and it has taken recent advances in experimental neuroscience to elucidate the chemistries of these hormones. The term opioid peptides are used for the endorphins. Proopiomelanocortin - POMC (pro-ACTH-Endorphin) is a glycosylated 31 kDa protein precursor posttranslational processing of which yields several neuroactive peptides upon specific cleavage and possibly a great number of as yet unidentified small peptides that may be pharmacologically active. Endorphins can further decompose to

Table 1.
Bioregulator assessment according to criteria for selecting bioregulators as warfare agents.

Criteria for Selection of Bioregulators as Terrorism Agents

1. High level of morbidity: higher rating (++) if clinical disease requires hospitalization for treatment including supportive care and lower rating (+) if outpatient treatment is possible for most cases.
2. High level of mortality or incapacity: agents with an expected mortality of =50% were rated higher (+++), and with lower expected mortalities (21-49%=++, and <21%=+).
3. Stability in the environment after release (+)
4. Ease of production and transportation (+)
5. High level of dissemination and contamination in quantities that could effect large populations especially by aerosol (+).
6. High toxicity or potency or low toxic dose: LD50 <0.000025 mg/kg (+++), LD50 from 0.000025 to 0.0025 mg/kg (++) and LD50 >0.0025 mg/kg (+).
7. High level of intoxication by variety route: per oral route (+), respiratory route (++), or both (+++).
8. Stockpiling of prophylactics and antidotal therapy (+)
9. Enhanced surveillance and education (+)
10. Difficult to diagnose or identify at the early stage or improved laboratory diagnostics (+).
11. Public perception: Public fear associated with an agent and the potential mass civil disruptions that may be associated with even a few cases of disease were also considered (+ to +++).

Table 2.
Bioregulator assessment according to criteria for selecting bioregulators as terrorism agents.

Criteria for Selection of Bioregulators as Warfare Agents

1. Agents known to have been developed, produced, stockpiled or used as weapons (+).
2. Likely methods and high level of dissemination or contamination a large area: by aerosol (+++) and sabotage (food and water supply) (++).
3. High toxicity or potency or low toxic dose: LD50 <0,000025 mg/kg (+++), LD50 from 0,000025 do 0,0025 mg/kg (++) and LD50 >0,0025 mg/kg (+).
4. High level of morbidity: higher rating (++) if clinical disease requires hospitalization for treatment including supportive care and lower rating (+) if outpatient treatment is possible for most cases.
5. High level of intoxication by variety route: per oral route (+), respiratory route (++), or both (+++).
6. High level of mortality or incapacity: agents with an expected mortality of =50% were rated higher (+++), and with lower expected mortalities (21-49%=++, and <21%=+).
7. No effective prophylaxis and therapy commonly available and widely in use (+). (cont. p. 18 - Bioregulators) (Bioregulators - from p. 17)
8. Stability in the environment (+).
9. Difficulty to diagnose/detect or identify at early stage (+).
10. Ease of production and transportation (+).

small fragments (oligomers) which are still active, and which pass the blood-brain barrier more readily. Their high activity and specificity make endorphins attractive compounds from a clinical view, but most are active only if injected into the blood (or the cerebrospinal fluid). This is because peptides are digested in the stomach, decomposed by proteolytic and other enzymes. Also, because of their size and structure, they have difficulty passing into the brain. Thus, despite the low oral to parenteral ratio of many morphine derivatives, they will probably not be replaced by small-chain peptides anytime soon. Dipeptidyl carboxypeptidase, enkephalinases, angiotensinases, and other enzymes accomplish enzymatic degradation of small-chain endorphins. POMC cleavage products include a large N-terminal fragment, which yields ã-MSH (melanocyte stimulating hormone-gamma) and possibly other unidentified cleavage products, ACTH (corticotropin, 39 amino acids), Lipotropin, á-MSH (melanocyte stimulating hormone-alpha; melanotropin; acetylated and amidated ACTH 1-13), â-MSH (melanocyte stimulating hormone-beta) and â-endorphin. Individual products of the POMC protein act on immune cells and to be produced by them, thus establishing close links between immune cells and the nervous system. Endorphin molecules have a separate nomenclature (á, â, ã) that denotes their stereochemistry. â-endorphin (and also á-endorphin and ã-endorphin derived from it) has been found to be produced also by macrophages and lymphocytes. â-endorphin appears to act differentially: its C-terminal moiety enhances T-cell proliferation, whereas this stimulatory effect can be prevented by peptides that possess the N-terminal enkephalin sequence. Human â-endorphin is the most potent of three stereoscopic variants, and has the same sequence as the C-terminal end of â-lipotropin. Endorphins enhance the natural cytotoxicity of lymphocytes and macrophages towards tumor cells, stimulate human peripheral blood mononuclear cell chemotaxis and inhibit production of T-cell chemotactic factors. Opiate receptors presynaptically inhibit transmission of excitatory pathways including acetylcholine, the catecholamines, serotonin, and substance P, a neuropeptide active in pain neurons. Endorphins may also be involved in glucose regulation.

B. SUBSTANCE P (SP)

Substance P (P=powder, the designation originating from early studies using powdered extracts of equine brain and intestines). It is known also as neurokinin-1 (NK1). It is a member of a family of proteins known as tachykinins. This neuropeptide was found in the gut as well as in the brain. It is responsible for a number of excitatory effects on both central and peripheral neurons. It contracts smooth muscle, constricts bronchioles and increases capillary permeability. When released from afferent nerves, it causes a neurogenic inflammatory response, including mast cell degranulation. Substance P, a polypeptide (molecular weight = 1,350 D) which is active in doses of less than one microgramme. Substance P causes a rapid loss of blood pressure, which may cause unconsciousness.

C. ENDOTHELINS (ET) OR (EDCF-ENDOTHELIUM-DERIVED CONTRACTING FACTOR)

Endothelins are a family of closely related peptides of 21 amino acids with two disulfide bonds. The four known species are isoforms encoded by four different genes. They are called ET-1 (endothelin-1), ET-2 (endothelin-2), ET-3 (endothelin-3) and VIC (vasoactive intestinal contractor). Endothelin is a highly potent vasoconstrictor peptide first isolated from porcine endothelial cell supernatant. Varying amounts of ET are also produced in other cell types such as smooth muscle, neuron, mesangium, melanocyte, parathyroid and amnion. Individual ET may posses separate physiological or pathophysiological roles in different target tissues. Secretion of ET is stimulated by epinephrine, angiotensin II, arginine vasopressin, transforming growth factor beta, thrombin, interleukin-1, and hypoxia. Endothelins act to stimulate contraction of many smooth muscle tissues including blood vessels, uterus, bladder, and intestine. ET-1 is the most potent vasoconstrictor peptide yet discovered. Numerous studies have implicated the endothelins in cardiovascular diseases such as hypertension, heart failure, and atherosclerosis. Endothelin levels are elevated in atherosclerosis, congestive cardiac failure and renal insufficiency. ET may play an important role in homeostatic hemodynamic balance. Endogenous endothelins and ET receptor subtypes are present in various endocrine organs. ET appears to act a modulator of secretion of prolactin, gonadotropins, GH and TSH. It is also may act as a neurotransmitter. Among this family of peptides ET-1 is the most studied compound. Therapeutic potential of endothelins has generated tremendous interest in numerous laboratories around the world. Structures of recently isolated snake venom sarafotoxins (Sarafotoxin S6a and S6b) bear striking resemblance to endothelins. They are carrying vasoconstrictor activity and potent coronary constrictor activity. They can cause heart arrest in several minutes with concentration of LD50 - 15 mg.kg-1.

D. BRADYKININ (KININ-9, KALLIDIN)

Bradykinin is the final product of the kinin system and is split from a serum á-2-globulin precursor by the kallikreins and also by trypsin or plasmin. Bradykinin reduces blood pressure by dilating blood vessels. In bronchial smooth muscles and also in the intestines and the uterus bradykinin leads to muscle contraction. Bradykinin is also one the most potent known substances inducing pain. BK causes hypotension, contracts smooth muscles and increases vascular permeability. It also plays a role in pain pathways and inflammation. BK antagonists are used for treating inflammations, pain, rheumatic arthritis, osteoarthritis, pancreatitis, rhnitis, asthma and gout. Bradykinin has a powerful influence in stimulating smooth muscle contraction, inducing hypotension, increasing blood flow and permeability of capillaries.

E. VASOPRESSIN (VP)

This protein is called also antidiuretic hormone (ADH), adiuretin, vasotocin, pituitrin P and pitressin. It is a cyclic nonapeptide synthesized in the hypothalamus and stored in the posterior lobe of the pituitary from which it is released into the circulation as necessary. Functions of VP include stimulation of ATCH release, improvement of the memory and learning capacity, reduction of the pressure in the pulmonary arteries and reduction of renin and ACE activity. Vasopressin regulates osmotic pressure in body fluids via a specific vasopressor receptor (V1). It has direct antidiuretic activity in the kidney, mediated by the antidiuretic receptor V2, and promotes readsorption of water in the distal convoluted tubules of the kidney. It also causes vasoconstriction in peripheral small blood vessels by stimulating smooth muscle cells in the cell walls to contract.

F. ANGIOTENSINS

Angiotensin is a decapeptide originally found to be produced by kidney derived renin from an á-2 hepatic globulin. It is mainly known for its potent pharmacological activities. Angiotensin elevates blood pressure through its direct vasoconstrictor, sympathomimetic, and (through release of aldosterone) sodium-retaining activities. Angiotensins are formed in biological fluids by the enzymatic cleavage of proteins. The speciesspecific enzyme renin, which can be generated by kallikrein from inactive prorenin, is responsible for the formation of angiotensin I (AT I) from globulin angiotensinogen (ATG). AT I that has no effect on the blood pressure, is split by the membrane bound angiotensin-converting enzyme (ACE) to form angiotensin II (AT II). Angiotensin II is a very potent vasoconstrictor substance and acts directly on the adrenal gland to stimulate the release of aldosterone. The inhibition of ACE results in a double hypotensive effect because both the formation of blood pressure raising AT II as well as the degradation of the blood pressure lowering kinin is inhibited. AT II agonists are used for treatment of shock and collapse in which a normal blood pressure could be restored as quickly as possible, while ACE inhibitors and AT II antagonists are applied as antihypertensive agents for treatment of hypertension.

G. ENKEPHALINS

These compounds comprise the basis for the body's own pain fighting mechanisms. The enkephalins are found in many areas of the body. Changes in these compounds and their metabolism have been associated with different headache disorders. The two 5-peptide enkephalins have been identified. One terminates in a leucine, and is known as Leu-enkephalin; the other terminates in a methionine, and is called Met-enkephalin. The enkephalins are relatively weak analgesics, which activate all opioid receptors, but appear to have the highest affinity for the d receptor. Apart from nervous tissue, enkephalins have been identified in many other organ systems, including the gut, sympathetic nervous system, and adrenal glands. In the CNS, enkephalins have been found in many areas but predominantly those associated with nociception (e.g. PAG and dorsal horn). Their pre-cursor molecule is proenkephalin and they are rapidly degraded by enkephalinase. Wondering why the human brain should have receptor sites for alkaloids from the opium poppy led to the discovery of a family of natural painkillers, the endorphins (from endogenous morphines). These substances are oligopeptides, containing from 5 to 30 amino acids.

H. SOMATOSTATIN (SRIF)

Somatostatin, known also as somatotropin release inhibiting hormone (SIH) , is a peptide of 14 amino acids found in the hypothalamus and central and peripheral nervous system. Angiopeptin is a stable analog of somatostatin. Somatostatin (SRIF) is formed as prepro-SRIF. The main product of gene expression is pro-SRIF- (1-64), which is processed at the C-terminus to form SRIF-28 and SRIF-14. SRIFand SRIF like substance have been found in hypothalamus, central and peripheral nervous system as well as gastrointestinal tract. The main biological effect of SRIF is to inhibit the release of growth hormone, TSH, prolactin, CRH, insulin, glucagon, VIP, secretin, pancreatic polypeptide, gastrin releasing peptide, gastrin, CCK and motilin. A possible role for somatostatin in affective disorders is suggested by its low concentration in cerebrospinal fluid of patients with depression. Somatostatin in the brain might be involved in therapeutic effects of some of antidepressant drugs.

I. BOMBESIN (BN)

Bombesin is a tetrapeptide found in skins of Bombina and Bombina variegate. It distributes in the central nervous system, the gastrointestinal tract as well as the peripheral tissues. Bombesin and Bombesin-like factors show a wide spectrum of biological activities. These include regulation of the contraction of smooth muscle cells, induction of the secretion of neuropeptides and hormones. Bombesin increases the plasma levels of gastrin, CCK, glucagon, insulin, pancreatic peptide, VIP and many other gastrointestinal peptides. The C-terminal nonapeptide of bombesin has the minimum length with the maximum effect. Bombesin is used as a diagnostic aid in the gastrin stimulation test. Bombesin originally isolated from the skins of the amphibians Bombina bombina and Boombina variegata variegata, is a potent stimulant of gastric acid secretion and shown the strong biologically active in central nervous system.

J. NEUROTENISN

Neurotenisn is a 13 amino acid peptide isolated from bovine hypothalamus. It causes hypotension in the rat and its smooth muscle actions include relaxation of the rat duodenum and contraction of guinea pig ileum and rat uterus. Neurotensin may also act as a CNS neurotransmitter. Neurotensin is involved with memory function, and that in brains of Alzheimer's disease patients there are deficits in this peptide in certain regions involved with memory function. This peptide may also be involved in the pathophysiology of Parkinson's disease and schizophrenia.

K. OXYTOCIN

The posterior pituitary has two hormones, ADH (antidiuretic hormone, vaspopressin) and oxytocin which are medically important. Both of these hormones are small peptides containg nine (9) amino acids each. They are synthesized in the hypothalamus (supraoptic nucleous for ADH and paraventricular nucleus for oxytocin). Oxytocin stimulates contraction of uterine smooth muscle. It is secreted during labor to effect delivery of the fetus. Oxytocin also stimulates contraction of smooth muscle in the mammary glands (myoepithelial cells). Oxytocin causes smooth muscle contraction in the alveoli (small chambers) and larger sinuses of the mammary glands to make readily available milk, whose production has been induced by prolactin and estrogen, to the suckling infant. Oxytocin causes milk ejection, which is necessary for adequate lactation, but not milk production. Prolactin controls milk production in conjunction with estrogen.

L.THYROTROPIN – THYROLIBERIN TSH (THYROID STIMULATING HORMONE)

A glycoprotein hormone consisting of two protein chains, one of which is identical with a subunit of Luteinizing hormone. Thyrotropin is produced in the anterior pituitary in response to thyrotropin releasing hormone (thyroliberin; thyrotropic hormone releasing factor or TRF). Thyrotropin stimulates the thyroid gland to secrete thyroid hormones such as thyroxin and triiodothyronin. These two hormones inhibit the secretion of TRF and thyrotropin. Thyrotropin stimulates secretion of prolactin and acts as a neurotransmitter in the central nervous system. Apart from its wellknown physiological role thyrotropin appears to be involved in the modulation of immune responses within the neuroimmune network. Thyrotropin enhances proliferation of lymphocytes stimulated by suboptimal concentrations of IL2 and enhances IL2-induced NK-cell activity. TSH also enhances production of superoxide anions by stimulated macrophages.

M. HRF (HISTAMINE-RELEASING FACTORS)

This is a general term used for factors that induce the release of histamines from basophils and mast cells when stimulated with antigens or mitogens. HRIF (Histamine release inhibitory factor). This poorly characterized factor is a specific antagonist of histamine-releasing factors. It is produced by peripheral blood mononuclear cells (B-cells, T-cells, monocytes) upon stimulation with histamine or mitogens such as Con A. It inhibits HRF-induced histamine release from basophils and mast cells. One particular factor with HRIF activity is IL8 .

CTAP-3 Beta-Thromboglobulin (Beta-TG)

CTAP-3 (connective tissue activating protein-3) or beta-thromboglobulin is a protein of 8.85 kDa. Beta-thromboglobulin is stored in the Alpha-granules of platelets and released in large amounts after platelet activation. Beta-thromboglobulin is a strong chemoattractant for fibroblasts and is weakly chemotactic for neutrophils. It stimulates mitogenesis, extracellular matrix synthesis, glucose metabolism, and plasminogen activator synthesis in human fibroblast cultures. Beta-thromboglobulin, its precursor, and its cleavage products influence the functional activities of neutrophilic granulocytes. Beta-thromboglobulin affects the maturation of human megakaryocytes and thus could play a role in the physiological regulation of platelet production by megakaryocytes.

N. AND O. NEUROKININ A (NKA) (SUBSTANCE K), NEUROKININ B (NKB) (NEUROMEDIN K)

Neurokinins are found centrally in the spinal cord and in the sensorial nuclei of the brain stem and peripherally in the ends of the sensorial fibers. Neurokinins include Substance P (SP), neurokinin A (NKA), and neurokinin B (NKB). Similar compounds, which occur in cold-blooded animals, are called tachykinins. So far, three different receptors have been found for the neurokinins: NK1 for SP, NK2 for NKA, NK3 for NKB. Neurokinins play various roles in the regulation of cardiovascular system, pain pathway and inflammatory reaction. Neurokinin A and B belong to the tachykinin family. They are a more potent bronchio-constrictor than substance P and may regulate neutrophil recruitment in the lower respiratory tract. They arise from larger precursor molecules and exhibit functions such as vasodilatation, hypotension, extravascular smooth muscle contraction, salivation and increase of capillary permiability

P. NEUROPEPTIDE Y (NPY)

Neuropeptide Y (NPY) is present in the brain and in the peripheral nervous system along with other neurotransmitters. It has structural homology with pancreatic polypeptide (PP) and peptide YY (PYY). Its functions may include neurotransmission, neuromodulation, vasoconstriction, regulation of blood pressure, and appetite. Our opinion is that if some bioregulator satisfies the bulk of the criteria, it should be recommended for inclusion in the list. As the list of bioregulators will be hard to define generally and for purposes of the future negotiations of the States Parties of BTWC, this paper proposes two tables of enlisted bioregulators with important criteria on the basis of which a decision can be made to include in or exclude from a list of the molecular agents (bioregulators).

Conclusions

All of that shows that it is very hard to make a final decision on criteria and the final list of the molecular agents (bioregulators) for the needs of future Protocol to the BTWC based on these criteria. Because of all of that, this paper proposes that list and criteria for bioregulators be well studied and that an opinion by scientists and experts be obtained, because the list should be scientifically based. Although many bioregulators can be used to cause illness, they can truly threaten civilian populations on a large scale. If released upon a civilian population, these agents would pose the most significant challenge for public health and medical responses. Although many biological agents such as bioregulators can be used to cause illness, there are only a few that can truly threaten civilian populations on a large scale. If released upon a civilian population, these agents would pose the most significant challenge for public health and medical responses. The above criteria for ranking potential bioregulators and listing of them of greatest public health concern could be used for determination of priority biological threat agents for national public health preparedness efforts for bioterrorism. Having a defined method for evaluating biological threat agents allows for a more objective evaluation of newly emerging potential threat agents, as well as continued re-evaluation of established threat agents. Using this prioritization method can help focus public health activities related to bioterrorism detection and response and assist with the allocation of limited public health resources.

It is very hard to make a final decision on criteria and the final list of the molecular agents (bioregulators) as terrorism and warfare agents. We propose that the list and criteria for bioregulators be well studied and that opinions by scientists and experts be obtained. The list should be scientifically based. Although many bioregulators can be used to cause illness, they can truly threaten civilian populations on a large scale. If released upon a civilian population, these agents would pose a significant challenge for public health and medical responses.

Chemical
Hazard
Menu
CHEMPRO 100i
ENVIRONICS

Home Labs on the Rise for the Fun of Science

Source: http://www.nytimes.com/2010/12/16/technology/personaltech/16basics.html?_r=1

An infrared thermometer from Extech that can also measure electrical properties.

One day Kathy Ceceri noticed a tick on her arm and started to worry that it was the kind that carried Lyme disease. So she went to her home lab, put the tiny arachnid under her microscope, which is connected to her computer through a U.S.B. cable, and studied the image.

"It was," she said. "Then of course I Googled what to do when you've been bitten by a deer tick." Ms. Ceceri's microscope, a Digital Blue QX5, is one of several pieces of scientific equipment that make up her home lab, which she has set up on her dining room table in Schuylerville, N.Y. Home labs like hers are becoming more feasible as the scientific devices that stock them become more computerized, cheaper and easier to use. Ms. Ceceri has several microscopes and a telescope. Other home laboratories have tools like infrared thermometers, which can be used in the kitchen, and kits to analyze DNA at home. Many of these tools work closely with home computers and come with software that enhances their power. Others mix low-cost computers into the hardware to deliver more precise control. Some people who set up home laboratories are serious hobbyists in search of better tools; others are home-schooling parents equipping their children; and others are just curious.

Ms. Ceceri, a writer, seems to fall into all three camps because she teaches her sons Anthony, 15, and John, 18, at home, and then she writes about some of their discoveries for a number of blogs like geekdad.com, geekmom.com and homebiology.blogspot.com. "This year we're doing integrated science," she said of her home science curriculum. "Anything we were looking at, we put under the microscope." She explained that she and her children raised triops, tiny crustaceans, and examined the eggs under the microscope. "We took a really nice video of the paramecium and nematodes swimming around just holding a digital camera up to a microscope," she said. Brian Haddock, a software developer from south of Fort Worth, who also writes about science topics on his blog, Reeko's Mad Scientist Lab, particularly enjoys using a microscope with a computer. "Those U.S.B. microscopes are pretty cool," he said. "They don't magnify as much as one of those optical scopes would, but you can look at it on your computer screen. It's got a big picture on your screen that's easier to see instead of those little tiny images you squint at." "Personally, I like the Carson zPix," he said. The growth in home labs is helped by manufacturers who are building tools at affordable prices. ThinkGeek.com, an online store that sells items for home laboratories, among other things, offers three models of microscopes at various prices, said Scott Smith, a co-founder of the site. Prices begin at $99, with models that offer 20x to 200x digital enlargements of whatever is being examined. The store's high-end model costs $349, and it delivers what

The Moticam 1000, a digital camera, fits over the eyepiece of a microscope for capturing images.

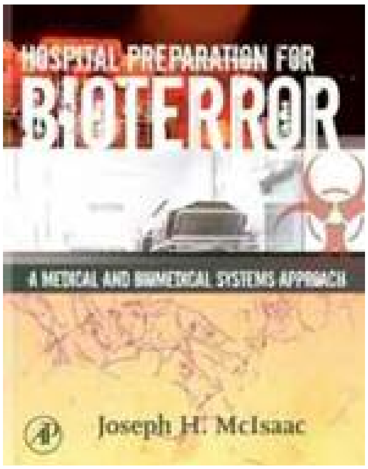
Mr. Smith characterized as sharper, better quality images for both hobbyists and businesses like jewelry shops. Adding a computer interface to a telescope makes it possible to collect more detail than might appear to the eye looking through the optics. The computer can collect multiple images over time and combine the results, enhancing the appearance of the faintest items. “It isn’t just about capturing video or still images. It actually allows you to stack a whole bunch of still images to get those really beautiful, spectacular pictures of the night sky,” explained Timothy Burns, the director of marketing at Edmund Scientific, the scientific supplier, which stocks a wide range of telescopes for the casual and professional scientist. “It gets the really deep color,” he said. “You could probably get a pretty cool still picture of the moon, but if you’re looking at a deep space object like a nebula, it brings out the colors and the definition of the whole star field.” The telescopes come with computerized controls, which Mr. Burns said makes them easier for children to control. The computer helps find particular objects in the sea of billions of stars. Edmund Scientific also supplies a digital camera, the Moticam 1000, which fits over the eyepiece of many standard telescopes and microscopes to capture images. Home scientists who want to study animals may be interested in a digital camera that can be activated by motion sensors. Cabela’s, the outdoor recreation merchant, stocks dozens of models at prices that begin just under $100 and rise to above $500. The cameras can take pictures during the day or even at night, adding time stamps. There is no requirement that the photographer return to hunt the animals. Infrared thermometers, which range from $20 to more than $100, are another tool home scientists can enjoy. These thermometers measure the temperature of objects without touching them, by reading the energy of the infrared light given off by the object. Cooks might use one of these to measure the temperature of a pan; I have used mine to look for poorly insulated sections of walls and to estimate the performance of my heating system by taking the temperature of the water returning from the heating loops. John Baichtal, a contributing writer for Make magazine, said he liked the Extech EX210 Multimeter, an infrared thermometer with the ability to measure voltage, resistance and other properties of electricity for just under $70. “It would be helpful for homeowners,” he said. “Let’s say there’s something that you can’t reach. A little laser pointer helps you aim accurately.” The tool is also ideal for helping children understand the flow of heat. Many exterior walls, for instance, have hot and cold spots that correspond to the amount of insulation, and the infrared thermometer helps spot energy leaks in the winter. Not everyone is content to fill their labs with centuries-old technology. Samara Rubenstein, the manager of the Sackler Educational Laboratory for Comparative Genomics and Human Origins at the American Museum of Natural History, said home scientists could extract their DNA by rinsing their mouth with salt water, breaking apart the sloughed-off cheek cells with dish detergent, and then rinsing out the DNA with rubbing alcohol. “It’s really cool,” she said. Other experiments for home labs can be found at Ology, a corner of the museum’s Web site. After the DNA is extracted, more options are becoming available for identifying the organism using a technique known as PCR, or polymerase chain reaction. A new project, OpenPCR, is designing new home tools for DNA analysis. Tito Jankowski, who founded the project with Josh Perfetto, said the kit would give anyone the chance to analyze DNA. Mr. Jankowski said one possible experiment for home scientists would be to test for their reactions to certain food. Only some people, for instance, taste the bitterness in brussels sprouts, a trait that has been linked to a part of our genome that the kit can identify. Eri Gentry, an entrepreneur in San Francisco, said she had already tested herself for this gene, using a $200 kit from Carolina Biological Supply, which sells to school science labs. “Some of these things you do not because it’s the quickest way to do it, but because you learn a lot,” she said.

Hospital Preparation for Bioterror: A Medical and Biomedical Systems Approach (Biomedical Engineering)

Joseph H. McIsaac III (Author - 2009)
Source: LinkedIn – Medical/Hospital CBRNE Defence Group

Hospital Preparation for Bioterror provides an extremely timely guide to improving the readiness of hospitals or healthcare organizations to manage mass casualties as a result of bioterrorism, biological warfare, and natural disasters. Contributions from leading law enforcement agencies, hospital administrators, clinical engineers, surgeons and terror-prevention professionals provide the most comprehensive, well-rounded source for this valuable information. Chapters on logistics and protecting the infrastructure help personnel distinguish the specific risks and vulnerabilities of each unique institution and assists in identifying specific solutions for disaster and bioterrorism preparedness.

- Principles and techniques discussed are applicable to all disasters, both large and small, not just bioterrorism
- Technical aspects such as hospital power and telecommunications are covered, in addition to patient care, response to mass casualties, large-scale drills, and surge capacity.
- Organized along functional lines, patient flow, medical specialty, and infrastructure
- A complimentary website with supplementary materials, check-lists, and references enhances the text and provides additional resources for preparedness.



Genetically Modified Mosquitos

Source: http://www.globalresearch.ca/index.php?context=va&aid=22385

While “scientists” have been genetically modifying insects for years, only in the last few have they begun to openly discuss releasing them into the environment. As always, the fact that public discussion has just now begun to take place on the issue means that the project has already been initiated. This much has been borne out by the facts in that the release of the insects has already been announced.

Under the guise of eradicating Dengue fever, GM mosquitoes were released into the environment in the Cayman Islands in 2009. Dengue fever is a mosquito-borne, virus-based disease that has largely been non-existent in North America for several decades. Dengue fever can morph into a much more dangerous form of the illness known as Dengue Hemorrhagic fever. Symptoms of Dengue fever are high fever, headache, pain behind the eyes, easy bruising, joint, muscle, bone pain, rash, and bleeding from the gums. There is no known cure or treatment for Dengue fever besides adequate rest and drinking plenty of water.

Generally speaking, it is one specific type of mosquito, Aedes aegypti, which transmits the virus.

The publicly given method for using these GM mosquitoes in the eradication of Dengue fever was that the genetically modified mosquitoes were “engineered with an extra gene, or inserted bacterium, or have had a gene altered so that either their offspring are sterile and unable to spread dengue, or simply die.” More specifically, the male GM mosquitoes are supposed to mate with natural females which produce larvae that die unless tetracycline, an antibiotic, is present. Without the antibiotic, an enzyme accumulates to a level that is toxic enough to kill the larvae.

It is important to note that these GM mosquitoes, known as OX513A, necessarily have to be of the Aedis aegypti type in order to achieve the goals publicly stated by the developers. Therefore, the millions of male mosquitoes that were released into the open-air environment in 2009, and again in 2010, were all of the dengue fever carrying type. The OX513A mosquitoes were developed by a British biotechnology company named Oxitec and their subsequent release was overseen by the Mosquito Research and Control Unit (MRCU) in the Cayman Islands, a British overseas territory. Although Oxitec Limited was the developer who engaged in most of the groundwork for the GM insects, the project was not theirs alone. The Bill and Melinda Gates Foundation, the World Health Organization, The PEW Charitable Trusts, and government agencies in the United States, England, Malaysia, and others were all involved in the development and promotion of the GM mosquitoes.

What has been quite suspicious, however, is the fact that Dengue fever, which has been nonexistent in North America for decades, has recently surfaced in Florida. Initially, the fever was found in 2009, but by 2010 the cases had vastly increased. In July 2010, a CDC study was released to very little media attention indicating that about 10 percent of the population of Key West had been infected with Dengue fever. This had doubled from 2009 where 5 percent had been infected. One might wonder what caused a virus that had been almost entirely eradicated to suddenly reappear with such vigor. That is, one might wonder if the answer weren't so blatantly obvious. Of course, official reports do not address whether or not the Dengue fever is connected to the millions of mosquitoes capable of carrying the fever which were released just miles away in the Cayman Islands.

While Dengue fever had been eradicated in terms of naturally occurring outbreaks in the United States, cases that were research-related and laboratory-generated have occurred in the country for many years. This is because Dengue fever has been of particular interest to the United States government, US Army, and CIA since at least the middle part of the 20th century. There is a great deal of evidence suggesting that the biochemical research facilities at Fort Detrick were conducting tests on Dengue fever as a bio-weapon as far back as 1942. It is generally known that in the 1950s the CIA partnered with Ft. Detrick to study Dengue fever and other exotic diseases for use as biological weapons.

It is also interesting to note that, according to CIA documents as well as a 1975 congressional committee, the three locations of Key West, Panama City, and Avon Park (and two other locations in central Florida) were testing sites for Dengue fever research. As is generally the case, the experiments in Avon Park were concentrated in low-income neighborhoods, in areas that were predominantly black with newly constructed housing projects. According to H.P. Albarelli Jr. and Zoe Martell of Truthout, CIA documents related to the MK/NAOMI program revealed that the agency was using the Aegis aegypti type of mosquito in these experiments as well. In one of these experiments, 600,000 mosquitoes were released over Avon Park and in another 150,000 insects were released in specially designed paper bags that were designed to open up when they hit the ground. Truthout interviewed residents (or test subjects) of Avon Park still living in the area who related that there were at least 6 or 7 deaths resulting from the experiments. As quoted by Truthout, one resident said, "Nobody knew about what had gone on here for years, maybe over 20 years, but in looking back it explained why a bunch of healthy people got sick quick and died at the time of those experiments." Truthout goes on to point out that around the same time of the Avon Park experiments "there were at least two cases of Dengue fever reported among civilian researchers at Fort Detrick in Maryland." In 1978, a Pentagon document titled, "Biological Warfare: Secret Testing & Volunteers" revealed that similar experiments were conducted in Key West by the Army Chemical Corps and Special Operations and Projects Divisions at Fort Detrick.

Like the current situation, U.S. government agencies teamed with NGOs, academia, and other organizations to conduct mosquito-related projects. Operation Bellweather, a

1959 experiment consisting of over 50 field tests, was conducted over several states including Georgia, Maryland, Utah, and Arizona, and Florida. Operation Bellweather was coordinated with the Rockefeller Institute in New York; the facility that actually bred the mosquitoes. What's more, the experiment was aided by the Armour Research Foundation, the Battelle Memorial Institute, Ben Venue Labs, Inc., the University of Florida, Florida State University, and the Lovell Chemical Company.

The military and CIA connections to Dengue fever outbreaks do not end with these experiments, however. It is widely believed that the 1981 outbreak in Cuba was a result of CIA and U.S. military covert biological attacks. This outbreak occurred essentially out of nowhere and resulted in over one hundred thousand cases of infection. Albarelli and Martell write:

> *American researcher William H. Schaap, an editor of Covert Action magazine, claims the Cuba Dengue outbreak was the result of CIA activities. Former Fort Detrick researchers, all of whom refused to have their names used for this article, say they performed 'advance work' on the Cuba outbreak and that it was 'man made.'*

In 1982 the CIA was accused by the Soviet media of sending operatives into Pakistan and Afghanistan for the purposes of creating a Dengue epidemic. Likewise, in 1985 and 1986, authorities in Nicaragua made similar claims against the CIA, also suggesting that they were attempting to start a Dengue outbreak.

While the CIA has characteristically denied involvement in all of these instances, army researchers have admitted to having worked intensely with "arthropod vectors for offensive biological warfare objectives" and that such work was conducted at Fort Detrick in the 1980s. Not only that, but researchers have also admitted that large mosquito colonies, which were infected with both yellow fever and Dengue fever, were being maintained at the Frederick, Maryland facility.

There is also evidence of experimentation with federal prisoners without their knowledge. As Truthout reports:

> *Several redacted Camp Detrick and Edgewood Arsenal reports indicate that experiments were conducted on state and federal prisoners who were unwittingly exposed to Dengue fever, as well as other viruses, some possibly lethal.*

With all of the evidence that CIA and military tests have been conducted regarding Dengue fever, there is ample reason to be concerned when one sees a connection like the recent release of mosquitoes and the subsequent outbreak of Dengue fever in Florida, a traditional testing site for these organizations. The response to the Dengue outbreak should also be questioned as aerial spraying campaigns were intensified. While these sprayings were claimed to be for the eradication of the Dengue-carrying mosquitoes, the number of people who contracted the illness actually rose.

Another questionable incident related to mosquito-borne Dengue fever and the sudden outbreak occurred on November 15, 2010. A University of South Florida molecular biologist apparently committed suicide by drinking cyanide at a Temple Terrace hotel. Dr. Chauhan, had studied mosquitoes and disease transmission at the University of Notre Dame. While ordinarily this would not be cause for concern, when one considers the level of interest maintained in mosquito-borne illnesses by both the military and intelligence agencies, the death of Dr. Chauhan might well be something that should be investigated further. Until her death, she was a post-doctoral researcher in the Global Health department in the College of Public Health. Those who knew her described her as both very bright and very enthusiastic. Maybe this is a coincidence, but regardless, it is one that should be looked at closely.

Unfortunately, the issue of GM insects being released into the wild does not end with increasing Dengue fever and malaria. In 2009, The Bill and Melinda Gates Foundation awarded $100,000 each to researchers in 22 countries in order to develop mosquitoes that would act as "flying syringes." Essentially, the mosquitoes would be genetically engineered to deliver vaccines with each bite.

The money was distributed to a wide variety of academic institutions, non-profit organizations, government agencies, and private companies. The funding was part of what was termed in an AFP article "the first round of funding for the Gates Foundation's 'Grand Challenges Explorations,' a five-year 100-million-dollar initiative to 'promote innovative ideas in global health.'" The basic premise behind the flying mosquito vaccines is that an insect will be genetically modified to produce antibodies to a certain disease in their saliva, which is then transmitted to the individual when the mosquito bites them.

There is a host of problems with this method that range from the moral to the scientific. First, the presence of antibodies does not necessarily mean immunity, and the transfer of them does not in any way provide immunization to the subject being injected with them. The science related to antibodies and immunity is still largely unsettled. Vaccines, themselves, are completely ineffective and have never been proven effective by a study that was not connected to a drug company or a pharmaceutical company.[1] They are, essentially, faith-based medicine.

Even more frightening is the potential of releasing genetically modified mosquitoes that contain actual diseases in their systems to purposely cause a human pandemic. Those who have weakened immune systems would be at the highest risk, but this would no doubt include everyone else as well since they would also be infected with the viruses when bitten. Person-to-person spreading would take over where the mosquitoes left off. Add to this the potential for simultaneous pandemics (if different versions of the insects were used simultaneously) and one has the recipe for genocide on a mass scale. Unfortunately, this is the scenario that many have envisioned for some time.

Nevertheless, although Gates has invested so much money, and so many hardworking individuals and prestigious universities have invested so much time and effort, the general consensus of the media is that the flying syringes will never take flight. This is because, as Science NOW reports,

> *The concept of a 'flying vaccinator' transgenic mosquito is not likely to be a practicable method of disease control, because 'flying vaccinator' is an unacceptable way to deliver vaccine without issues of dosage and informed consent against current vaccine programs. These difficulties are more complicated by the issues of public acceptance to release of transgenic mosquitoes.*

However, it is quite difficult to believe that the Gates Foundation distributed such a vast amount of money to researchers without first questioning whether or not their efforts were feasible for future use. It is likewise very hard to believe that once these issues were considered, that the Gates Foundation would simply throw away money on a project that was doomed to failure. In fact, anyone who actually believes this is unfortunately very naïve. Clearly, we are being conditioned to accept and expect these organisms to be released on the public on some future date. What the context will be, however, is anyone's guess.

Notes:

[1] Flu and Flu Vaccines: What's Coming Through That Needle. Dr. Sherri Tenpenny.

Brandon Turbeville is an author out of Mullins, South Carolina. He has a Bachelor's Degree from Francis Marion University where he earned the Pee Dee Electric Scholar's Award as an undergraduate. He has had numerous articles published dealing with a wide variety of subjects including health, economics, and civil liberties. He is also the author of Codex Alimentarius - The End of Health Freedom smiths medical

bringing technology to life

Mechanical Ventilation

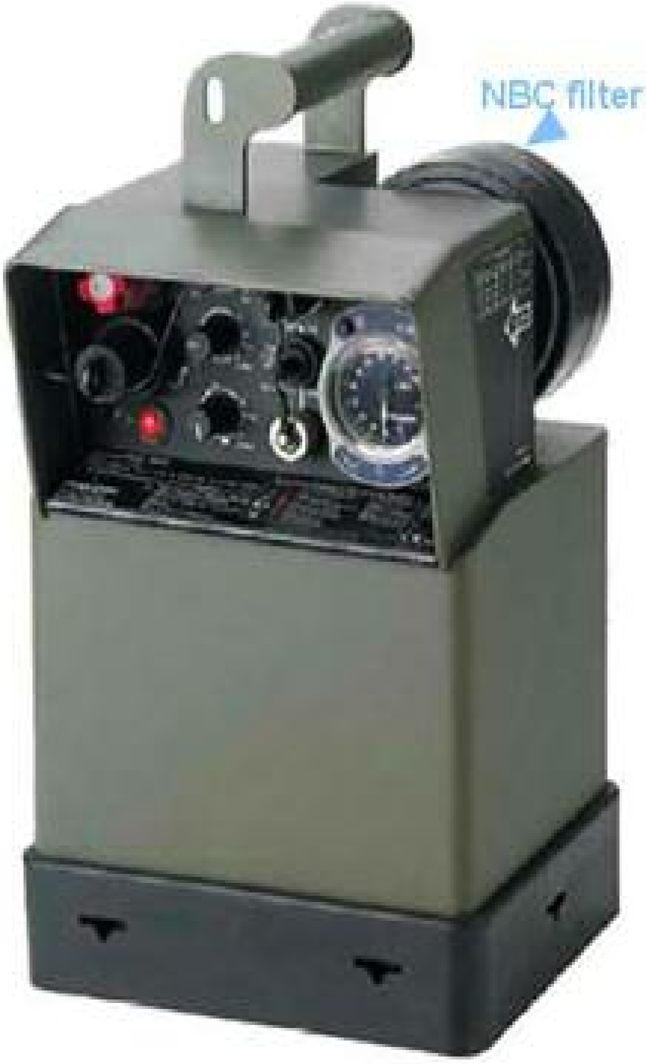
Pneupac® compPAC™

Pneupac

The compPAC ventilator has the unique ability to provide life support to patients in contaminated zones where oxygen supply is limited. In such situations the internal battery can power the integrated compressor providing ventilatory support for up to 4 hours.

The compPAC is equipped with a military style filter cannister, which combined with its rugged design and versatile power options makes it the leader in ventilation in difficult environments.

Currently compPAC is in service with military forces around the world and is part of disaster contingency plans for civil toxic release.



Product Features

- Versatile options for driving the ventilator
- Versatile options for powering the internal compressor
- Air mix facility
- Oxygen enrichment facility
- Separate controls for minute volume and frequency
- Integrated pressure monitoring/alarm system
- Relief pressure control with audible alarm
- Military style filter cannister
- Rugged and extremely durable
- Control panel light
- Low gas supply indicator

Contact Smiths Medical

Information for customer services and product information

Smiths Medical's aims to build a rewarding relationship with all our customers and we are continually working on ways of improving our products and services to support your needs.

Smiths Medical International Ltd (EMEA)

1500 Eureka Park, Lower Pemberton, Ashford, Kent, TN25 4BF, UK
Tel: +44 (0)1923 241411 - **Fax:** +44 (0)1233 722153
UKCS@smiths-medical.com
ics@smiths-medical.com
Click for customer service details

Smiths Medical North America

5200 Upper Metro Place, Suite 200, Dublin, OH 43017, U.S.A
Tel: +1 800 258 5361 / +1 614 210 7300 - **Fax:** +1 614 889 2651
info.asd@smiths-medical.com

Ready or Not 2010

Protecting the Public's Health from Disease, Disasters, and Bioterrorism
Source: http://healthyamericans.org/reports/bioterror10/

In the eighth annual Ready or Not? Protecting the Public from Diseases, Disasters, and Bioterrorism report, 14 states scored nine or higher on 10 key indicators of public health preparedness. Three states (Arkansas, North Dakota, and Washington State) scored 10 out of 10. Another 25 states and Washington, D.C. scored in the 7 to 8 range. No state scored lower than a five.

The scores reflect nearly ten years of progress to improve how the nation prevents, identifies, and contains new disease outbreaks and bioterrorism threats and responds to the aftermath of natural disasters in the wake of the September 11, 2001 and anthrax tragedies. In addition, the real-world experience responding to the H1N1 flu pandemic - supported by emergency supplemental funding - also helped bring preparedness to the next level.

However, the Ready or Not? report, released today by the Trust for America's Health (TFAH) and the Robert Wood Johnson Foundation, notes that the almost decade of gains is in real jeopardy due to severe budget cuts by federal, state, and local governments. The economic recession has led to cuts in public health staffing and eroded the basic capabilities of state and local health departments, which are needed to successfully respond to crises. Thirty-three states and Washington, D.C. cut public health funding from fiscal years (FY) 2008-09 to 2009-10, with 18 of these states cutting funding for the second year in a row. The report also notes that just eight states raised funding for two or more consecutive years. The Center on Budget and Policy Priorities has found that states have experienced overall budgetary shortfalls of $425 billion since FY 2009.

In addition to state cuts, federal support for public health preparedness has been cut by 27 percent since FY 2005 (adjusted for inflation). Local public health departments report losing 23,000 jobs - totaling 15 percent of the local public health workforce - since January 2008. The impact of the recession was not as drastically felt by the public health workforce until more recently because supplemental funds received to support the H1N1 pandemic flu response and from the American Recovery and Reinvestment Act have almost entirely been used.

Ready or Not? provides the public and policymakers with an independent analysis of the progress and vulnerabilities in the nation's public health preparedness. Some key findings include:

- Seven states cannot currently share data electronically with health care providers;
- 10 states do not have an electronic syndromic surveillance system that can report and exchange information to rapidly detect disease outbreaks;
- Half of states do not mandate all licensed child care facilities have a multi-hazard written evacuation and relocation plan;
- Only four states report not having enough staffing capacity to work five, 12-hour days for six to eight weeks in response to an infectious disease outbreak, such as novel influenza A H1N1; and
- Only one state decreased their Laboratory Response Network for Chemical Threats (LRN-C) chemical capability from August 10, 2009 to August 9, 2010.

The report also looked at findings from a recently released report from the U.S. Centers for Disease Control and Prevention

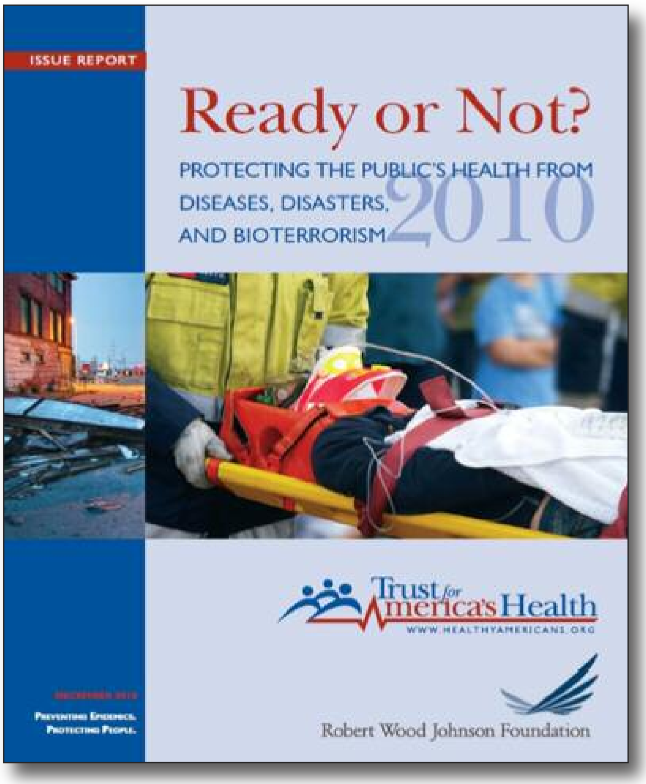
(CDC) based on activities in 2007-08 that focus on emergency operations and food outbreak identification.

- Only two states reported that pre-identified staff were not able to acknowledge notification of emergency exercises or incidents within 60 minutes a minimum of two times, the target established by the CDC;
- Six states did not activate their emergency operations center (EOC) a minimum of two times, the target established by the CDC;
- Only two states did not develop at least two After Action Report/Improvement Plans (AAR/IPs) after exercises or real incidents in 2007-08; and
- 21 states were not able to rapidly identify disease-causing E.coli O157:H7 and submit the lab results in 90 percent of cases within four days.

According to the report, while states have made progress, there are still a series of major ongoing gaps in preparedness, including in basic infrastructure and funding, biosurveillance, maintaining an adequate and expertly trained workforce, developing and manufacturing vaccines and medicines, surge capacity for providing care in major emergencies, and helping communities cope with and recover from emergencies.

Ready or Not? provides a series of recommendations that address the ongoing major gaps in emergency health preparedness, including:

- Gaps in Funding and Infrastructure: The resources required to truly modernize public heath systems must be made available to bring public health into 21st century and improve preparedness;
- A Surveillance Gap: The United States lacks an integrated, national approach to biosurveillance, and there are major variations in how quickly states collect and report data which hamper bioterrorism and disease outbreak response capabilities;
- A Workforce Gap: The United States has 50,000 fewer public health workers than it did 20 years ago - and one-third of current workers are eligible to retire within five years. Policies must be supported that ensure there are a sufficient number of adequately trained public health experts - including epidemiologists, physicians, nurses, and other workers - to respond to all threats to the public's health;
- Gaps in Vaccine and Pharmaceutical Research, Development, and Manufacturing: The United States must improve the research and development of vaccines and medications;
- A Surge Capacity Gap: In the event of a major disease outbreak or attack, the public health and health care systems would be severely overstretched. Policymakers must address the ability of the health care system to quickly expand beyond normal services during a major emergency;
- Gaps in Community Resiliency Support: The United States must close the existing day-to-day gaps in public health departments which make it difficult to identify and service the most vulnerable Americans, who often need the most help during emergencies.


ISSUE REPORT

Ready or Not?

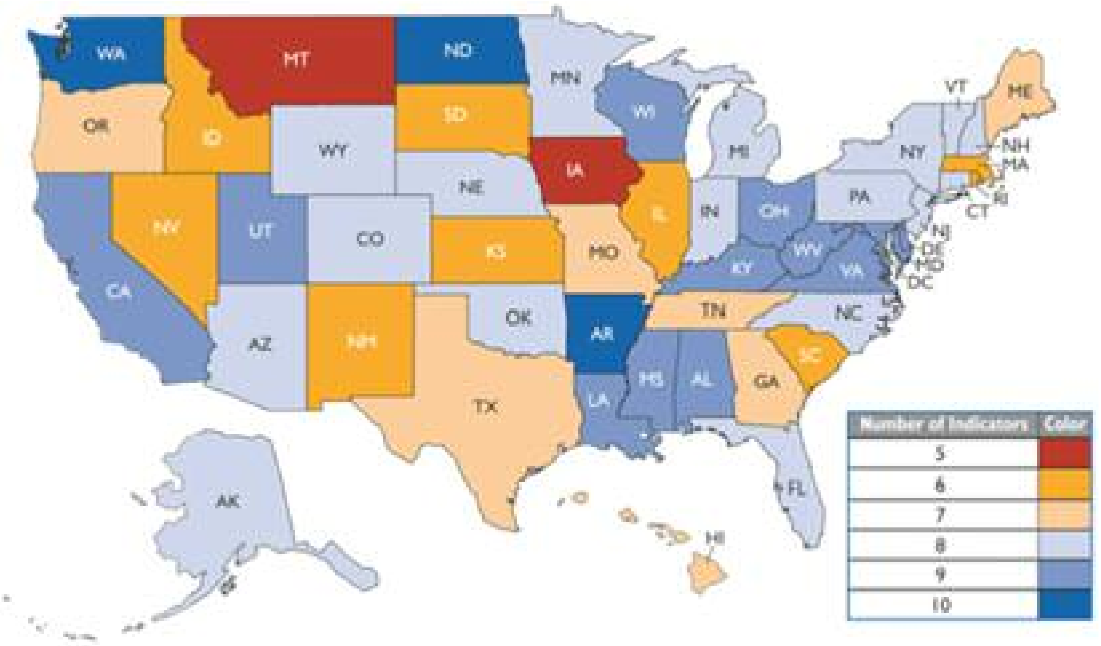
PROTECTING THE PUBLIC'S HEALTH FROM DISEASES, DISASTERS, AND BIOTERRORISM 2010

Trust for America's Health
WWW.HEALTHYAMERICANS.ORG

DECEMBER 2010

Preventing Epidemics. Protecting People.

Robert Wood Johnson Foundation



Click on a state below to access state-specific information and scores:

10	9	8	7	6	5
Arkansas	Alabama	Alaska	D.C.		
North Dakota	California	Arizona	Georgia		
Washington	Kentucky	Colorado	Hawaii		
	Louisiana	Connecticut	Maine		
	Maryland	Delaware	Missouri		
	Mississippi	Florida	Oregon		
	Ohio	Indiana	Tennessee		
	Utah	Michigan	T		
	Virginia	Minnesota			
	West Virginia	Nebraska			
	Wisconsin	New Hampshire			
		New Jersey			
		New York			
		North Carolina			
		Oklahoma			
		Pennsylvania			
		Vermont			
		Wyoming			

Download the full report at:
http://healthyamericans.org/assets/files/TFAH2010ReadyorNot%20FINAL.pdf

WikiLeaks cable shows US fears bioweapons can be stolen from Indian labs

Source:http://www.thetelegram.com/News/Canada%20-%20World/Arts/1969-12-31/article-2051569/ WikiLeaks-cable-shows-US-fears-bioweapons-can-be-stolen-from-Indian-labs/1

U.S. officials fear lax security at Indian laboratories could make the facilities targets for terrorists seeking biological weapons to launch attacks across the globe, according to comments in a leaked U.S. diplomatic cable made public Friday. The cable was part of a trove of documents sent from the U.S. Embassy in New Delhi that was obtained by the website WikiLeaks and published Friday by the British newspaper The Guardian. The cables also dealt with accusations of Indian torture in Kashmir, India's complaints about Pakistan's handling of the Mumbai terror attacks, and the concerns of Rahul Gandhi — seen as India's prime-minister-in-waiting — that Hindu extremists posed a greater danger to India than Islamist militants. One of the cables from June 2006 raised concerns that terrorist groups could take advantage of weak security at Indian laboratories to steal «bacteria, parasites, viruses or toxins.»

«Terrorists planning attacks anywhere in the world could use India's advanced biotechnology industry and large biomedical research community as potential sources of biological agents,» read the cable, marked «confidential.» ''Given the strong air connections Delhi shares with the rest of the world and the vulnerabilities that might be exploited at airports, a witting or unwitting person could easily take hazardous materials into or out of the country.» «Getting into a facility to obtain lethal bioagents is not very difficult here,» one expert, whose name was redacted from the cable, told U.S. diplomats. A second expert said that academic research facilities maintain only very loose security procedures. «**The harsh reality is that you can bribe a guard with a pack of cigarettes to get inside**,» the expert was quoted as saying. One source told the diplomats that India's thousands of biological scientists also might be recruited, either out of ideological sympathies or for money.

An Indian government official, who spoke only on condition of anonymity because he was not authorized to publicly address the issue, dismissed the concerns as «far-fetched and fanciful.» However, Suman Sahai, a biotechnology expert, told The Associated Press that security remains very poor at biotech firms four years after the cable was written. The regulatory system is porous, employees are easily influenced and those leaving public laboratories to work for private companies often steal seeds, genetic material and other sensitive property before they head out the door, she said. While India has not been the target of a biological attack, it has suffered devastating conventional terror strikes, including a 2001 attack on its parliament and the 2008 attack by 10 Pakistan-based militants who laid siege to the city of Mumbai for 60 hours.

Indian officials made it clear that they were focusing more on a possible nuclear or chemical attack — presumably from longtime rival Pakistan — than a biological one, which they considered unlikely to happen, the cable read. India's surveillance system and its public health system were ill-prepared for the possibility of such an attack, the cable said. While many countries are poorly prepared for a bioterror attack, the cable said, «few live in the kind of dangerous neighbourhood that India does, where terrorism, lax security, petty corruption, high population density, weak public health and agricultural infrastructures, and a booming and sophisticated biotech industry coexist.»

Another cable released Friday revealed the extent of India's frustration with rival Pakistan, where it says the Mumbai plot was hatched and received army support. Earlier this year, India's Home Minister Palaniappan Chidambaram told visiting FBI Director Robert Mueller that Pakistan had «done damn near nothing» to prosecute the Mumbai suspects, according a cable. While Pakistan has arrested seven people in connection with the attacks, those trials have not yet properly begun. Instead of pursuing militants, Pakistan's military is «hypnotically obsessed» with India's military, Indian Foreign Secretary Nirupama Rao was quoted as saying. She added that peace talks would remain on hold until Pakistan did more to dismantle terrorist networks that target India.

The cables also discussed a confidential 2005 briefing by the International Committee of the Red Cross that accused India of the widespread use of torture in Kashmir, where the Indian government confronts a raging separatist insurgency. The Red Cross said it had interviewed 1,491 detainees in Kashmir between 2002 and 2004 and found that many had been beaten, hung from the ceiling, put in stress positions, sexually abused or tortured with electricity, water or a round metal object called «the roller» used to crush a person's thighs, the cable said. The agency had raised the issues with India for a decade and the continuation of the practice led the agency to believe the government condoned the torture, it said.

On Friday, ICRC spokesman Christian Cardon said in Geneva that the briefing referred to in the cable did take place, but declined comment on what was said during it. In response to the accusation, Indian Foreign Ministry spokesman Vishnu Prakash said Friday: «India is an open and democratic nation which adheres to the rule of law. If and when an aberration occurs, it is promptly and firmly dealt with.»

The cables also revealed that Rahul Gandhi, a top official in the ruling Congress Party, warned in 2009 that homegrown Hindu extremist groups could pose a greater threat than established Islamist militant groups, such as Pakistan-based Lashkar-e-Taiba, which has been blamed for the Mumbai attacks. Gandhi appeared to be referring to the danger of a flare up in Hindu-Muslim communal violence caused by some of the more extreme leaders of the opposition Bharatiya Janata Party, according to the cable, which was written by Ambassador Timothy Roemer.

'Al-Qaida planned to poison US hotel buffets, salad bars'

Source: http://www.jpost.com/International/Article.aspx?ID=200377&R=R1

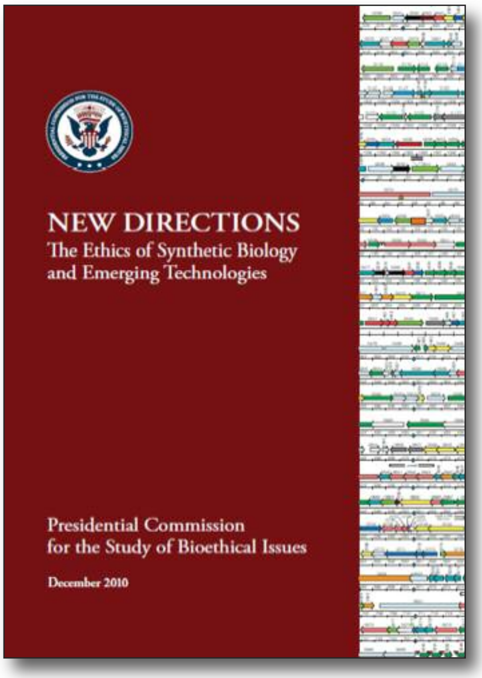
The US Department of Homeland Security discovered an al-Qaida plot to poison buffets and salad bars at American hotels and restaurants over a single weekend, CBS reported on Monday. A Homeland Security source called the threat «credible,» and Department of Agriculture and FDA officials reportedly briefed security officers from the hotel and restaurant industries. The same al-Qaida-affiliated terror group that attempted to bomb cargo planes in October was reportedly behind the plan to slip two poisons, ricin and cyanide, into salad bars and buffets. The poison attacks are part of what al-Qaida in the Arabian Peninsula called «**Operation Hemorrhage**,» which consists of «attacking the enemy with smaller but more frequent operations» to «add a heavy economic burden to an already faltering economy.» October's attacks on UPS planes headed for the US were also part of the operation. The terror group's websites feature manuals and videos explaining how to make both poisons. Dr. Susan Ford, a professor of pharmaceutical sciences, told CBS that such an attack «would look very much like food poisoning.»

but only 250 mg of sodium cyanide is a «fatal dose.» Department of Security spokesman Sean Smith said to CBS: «We are not going to comment on reports of specific terrorist planning. However, the counterterrorism and homeland security communities have engaged in extensive efforts for many years to guard against all types of terrorist attacks, including unconventional attacks using chemical, biological, radiological, and nuclear materials. Indeed, Al-Qaida has publicly stated its intention to try to carry out unconventional attacks for well over a decade, and AQAP propaganda in the past year has made similar reference. «Finally, we get reports about the different kinds of attacks terrorists would like to carry out that frequently are beyond their assessed capability.»

Limited Risks from Synthetic Genomics

Source:http://www.hstoday.us/focused-topics/surveillance-protection/single-article-page/limited-risks-from-synthetic-genomics-report-concluded.html

While counterterrorism authorities have expressed worry over the potential terrorist threat from the use of synthetic genomics as a means to create deadly infectious diseases – even "designer" and hybrid viruses the report of the Presidential Commission for the Study of Bioethical Issues, Ethics of Synthetic Biology and Emerging Technologies, concluded that synthetic biology poses only "limited risks."



NEW DIRECTIONS
The Ethics of Synthetic Biology and Emerging Technologies

Presidential Commission for the Study of Bioethical Issues

December 2010

"Future developments may raise further objections, but the Commission found no reason to endorse additional federal regulations or a moratorium on work in this field at this time," the Commission concluded. "Instead, the Commission urges monitoring and dialogue between the private and public sectors to achieve open communication and cooperation."

"Concerns about dual use or intentional misuse of synthetic biology to do harm are among the most prominent critiques of this emerging technology," the Commission's report stated, noting that "one of the most widely voiced risks attributed to synthetic biology is that it may be used, in the wrong hands, to intentionally create harmful organisms for bioterrorism. Recent examples of virus reconstruction using traditional recombinant DNA techniques fuel these concerns. These examples include the laboratory creation of infectious polio virus, the mycoplasma genome, and the 1918 strain of influenza virus.»

Continuing, the Commission's report stated that what's "frequently lost in these discussions about synthetic biology risks is recognition that DNA alone is not sufficient to create an independently functioning biological entity, such as a disease-causing virus that could spread. Despite the relative ease of access to known DNA sequences through public databases like GenBank60 (an annotated collection of all publicly available genetic sequences), and equivalent databases across the globe, most experts in the scientific community agree that mere knowledge of a viral genome is far from sufficient to be able to reconstitute it or create a disease-forming pathogen."

Rather, one must have an appropriate host and conditions for a virus to grow," the Commission concluded, saying "few individuals or groups today have the financial means or the technical skills to accomplish such ends, even when scientifically feasible. As the many technical challenges in synthetic biology affirm, it is not yet possible to craft functioning biological organisms from synthesized genomic material alone."

Other authorities, however, especially those involved in weapons of mass destruction counterterrorism, nevertheless remain alarmed about the possibility that rogue state-sponsored terrorists and terrorist organizations with the monetary resources and jihadist converted members with the appropriate skills could find ways to manipulate synthetic genomics to carry out deadly pathenogenic terrorist attacks.

The Commission recommended "that the government, through a coordinated process or body within the Executive Office of the President, lead an ongoing review of developments, risks, opportunities, and oversight as this field grows."

The Commission pointed out that the "Variola Amendment" to the Intelligence Reform and Terrorism Prevention Act of 2004 made it criminal to produce, engineer, or synthesize the variola virus. The "variola virus" was in turn defined to include "any derivative of the variola major virus that contains more than 85 percent of the gene sequence of the variola major virus or the variola minor virus."

But the Commission said, "the broad definition of 'variola virus' made it unclear what was actually covered by the statute, and a strict interpretation of the definition would have potentially, and inadvertently, criminalized beneficial research such as production of the smallpox vaccine."

Continuing, the Commission found that while "synthetic biology offers extraordinary promise to create new products for clea energy, pollution control, and medicine, to revolutionize chemical production and manufacturing, and to create new economic opportunities," it noted that "with this promise comes a duty to attend carefully to potential risks, be responsible stewards, and consider thoughtfully the implications for humans, other species, nature, and the environment."

The Commission said "this review should be in consultation with relevant scientific, academic, international, and public communities, and whenever possible its results should be made public. We also recommend that reasonable risk assessment should precede any field release of synthetic organisms. We suggest support for public engagement, education, and dialogue to ensure public trust and avoid unnecessary limitations on science and social progress."

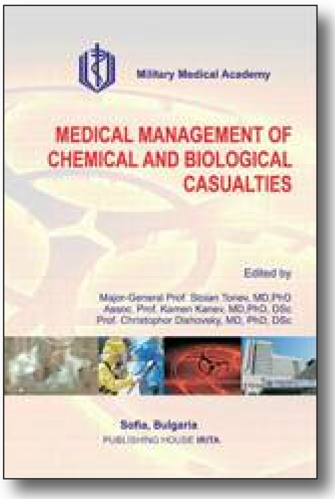
Full report at: http://www.bioethics.gov/documents/synthetic-biology/PCSBI-Synthetic-Biology-Report-12-16-10.pdf

Medical management of Chemical and Biological Casualties

Source:: Tonev, S.; Kanev, K.; Dishovsky, C (2009), «Medical Management of Chemical and Biological Casualties», as published in JMedCBR 8, 18 February 2010, http://www.jmedcbr.org/ issue_0801/Dishovsky/Dishovsky.html. Published with permission of Prof. Dishovsky. First published in August 2009 by Publishing House IRITA, Publishing House IRITA, ISBN 978-954-9993-91-2

Synopsis

This book includes reports that were presented at the Symposium «Medical Management of Chemical and Biological Casualties». The Symposium, which was held in Military Medical Academy, Sofia, Bulgaria from 27 to 28 April 2009, with international participation, was organized by the Military Medical Academy - Sofia, Bulgarian Toxicological Society, Bulgarian Association Of Clinical Toxicology, National Center of Infectious and Parasitic Diseases, and the Union of Scientists in Bulgaria -Medical Sciences Section. The goal of this symposium was to assess scientific concepts and practical ways to manage chemical and biological casualties. This book also includes the results of both theoretical and practical research for countering chemical and biological terrorism presented during the symposium.



The main topics of the presentations were:

1. New approaches in organization of emergency response;
2. Characterization and mechanisms of action of chemical and biological agents;
3. Pre-treatment and prophylactics of chemical and biological agents injuries;
4. Diagnosis of exposure to chemical and biological agents;
5. Therapy of chemical and biological agents casualties;
6. Some aspects of national and global defense against chemical and biological terrorism;
7. Threats of terroristic attacks with chemical and biological agents;
8. New approaches in counteraction to chemical and biological terrorism

Different trends and interactions between government agencies, the role of Military Medical Academy in emergency response in Bulgaria and medical support in case of chemical and biological threat are discussed. The problems are analyzed from an interdisciplinary perspective. This book will be interesting and useful for medical and other university students, medical doctors, specialists in the field of personal and social safety, environmental protection experts, chemists, biologists, and specialists of the military and governmental anti-terrorist or counter-terrorism departments.

Medical research is part of the military's combat mission, too

By David Brown - Washington Post Staff Writer
Source: http://www.washingtonpost.com/wp-dyn/content/article/2010/12/30/AR201012300 4610.html

On most days of his six-month deployment, surgeon David H. Zonies was lucky just to get outside and see the sun. Often, his only break from work was 30 minutes on the treadmill in the physical therapy department.

Every day, a half-dozen casualties arrived at the Joint Theater Hospital here, nearly all needing surgery in the next 24 hours, many missing limbs, a few barely clinging to life. The 36-year-old Air Force major was the «trauma czar.» His job was to coordinate the patients' care and operate on about a third of them.

At the end of October, however, Zonies took two days away from the job. He exchanged blue scrubs for a brown flight suit, flew to Kandahar Airfield 350 miles to the southwest and presented two papers at a medical conference.

One described bringing dialysis to the war theater, and the other was about a new lab test for measuring the strength of blood clots. Thirty people from four hospitals in Afghanistan watched his PowerPoint presentations and asked him questions. Then he flew back to work.

Zonies' big outing - and the willingness of the Air Force to let him take it - says a lot about how important medical research is to the American military, even during one of the most intense periods of a nine-year war.

The armed services are dedicated to saving every life, limb and eye of battle-wounded service members in Afghanistan and Iraq. The task requires not only skill and energy, but also the capacity to learn from failure and broadcast success.

Military medicine has made consistency and self-scrutiny part of the mission. It takes to heart the quality-assurance mantra «If you can't measure it, you can't change it.» It values publication in peer-reviewed journals as much as does the faculty of Harvard Medical School.

«Among the big challenges in medicine is taking up new stuff that works and letting go of the things that don't. My sense is that the military kind of has a handle on both,» said Carolyn Clancy, director of the Agency for Healthcare Research and Quality, the federal agency assigned to finding ways to better apply existing medical knowledge.

Historically, civilian medicine has had a poor handle on those challenges.

In a famous study published in the 1990s, a group of Harvard researchers measured how long it took for knowledge to turn into action in medicine. They performed a «cumulative meta-analysis» - essentially a running score card - of the results of clinical trials testing new heart attack treatments. They compared when there was enough information to say something worked, and when doctors started putting the treatments into practice.

They found that clot-dissolving thrombolytic drugs weren't widely recommended

until 13 years after it was clear they saved lives. For the use of aspirin in acute heart attacks, the lag was 10 years.

In the armed services, new approaches are viewed with more urgency.

«There is a push for people to get feedback quickly. It can't just be when somebody gets around to looking at the data,» said Cmdr. Lisa Osborne, a 42-year-old Navy nurse anesthetist who is coordinating in-theater research in Afghanistan. «There's an expectation to ensure that 'lessons learned' are actually changing practice.»

The upshot is that military medicine in many ways is a model for civilian medicine. It's also a testing ground, although not in the way many people might think.

War zone discoveries

Randomized controlled trials are the gold standard for trying out new treatments. But with few exceptions, such studies are never done with soldiers. The existence of rank and the chaos of the battlefield make getting «informed consent» for clinical experiments essentially impossible.

Nevertheless, war has been an incubator for medical progress as far back as the time of the Roman legions. From a flood of mayhem and disease, new insights emerge. Andrew N. Pollak, a surgeon at the University of Maryland's R Adams Cowley Shock Trauma Center in Baltimore and president-elect of the Orthopaedic Trauma Association, sees that happening now.

The Shock Trauma Center gets about 30 limb-threatening leg injuries a year. Doctors at the Walter Reed Army Medical Center get about 30 a month. Insights at the military hospital are causing orthopedists everywhere to question how they treat violent leg fractures. Pollak is helping design a randomized trial that will test two different strategies this year.

«What the war has done is focus our questions better,» he said.

The insights available from combat in Iraq and Afghanistan have been especially obvious because of the length of those conflicts, said John B. Holcomb, a surgeon who retired in 2008 after 23 years in the Army and is now a professor at the University of Texas Health Science Center in Houston.

«At the beginning of a war, the flow of knowledge is from the civilian world into the military,» he said. «After a couple of years, it is from the military to the civilian.»

Trauma database

A trauma registry is the data backbone of state and regional trauma systems in the United States. But at the time of the Sept. 11, 2001 attacks, the Department of Defense didn't have one.

It does now.

The Joint Theater Trauma Registry is the record of injuries sustained, treatment given, surgery performed, transfusions and antibiotics prescribed, complications sustained and, most important, health outcomes in 40,000 casualties from the Iraq and Afghanistan wars. The data are so important that troops are deployed just to capture it.

At Bagram this past fall, Maj. Camille Walker and Maj. Harriett Johnson, Air Force nurses, spent their days in a windowless room at the hospital transcribing data from paper patient records into computer files. Each morning, one of them would go on ward rounds and take notes.

«We need to get every CT scan, diagnostic test and procedure code, and we try to do it in real time,» Walker said during a break from the arduous work.

The registry is a data mine that, excavated properly, can yield nuggets of insight.

Consider «abdominal compartment syndrome,» a rare condition most often seen in burn patients, in which internal organs swell and essentially choke each other.

The registry allowed doctors to correlate the syndrome with the amount of IV fluid given. Guidelines for fluid resuscitation of burn victims were rewritten and the problem «went to zero overnight,» said Col. Brian J. Eastridge, an Army surgeon who helps run the registry.

In another particularly useful insight, military surgeons studying registry records determined that the mortality of patients needing «massive transfusions» (10 or more pints of blood in a day) could be reduced from 33 percent to less than 20 percent if they received whole blood, not just red blood cells and an occasional unit of plasma.

«We modified our transfusion guidelines over a year ago as a result of this,» said Lynette Scherer, the 43-year-old chief of trauma at the University of California in Davis, who visited Bagram in October as part of an American College of Surgeons delegation. «It has made a difference for patients I take care of in Sacramento.»

A broad variety of studies

There are 96 military «research activities» underway or being planned in Iraq and Afghanistan.

Before any begin, an eight-person Joint Combat Casualty Research Team addresses two key questions: Does this study have to be done here? Is it feasible? If the answers are yes, the team helps researchers fine-tune their study design and sometimes helps collect data. A «human protections administrator» audits the activities, which are first approved by ethics panels in the United States.

The topics are wide-ranging. A big one now is pre-hospital care.

Medics are trained to do many things for wounded soldiers, both on the ground and en route to the hospital. But how many of the lifesaving interventions get done, whether they were done right, and whether they made a difference are questions that largely go unanswered.

«The question we have to be constantly reevaluating is: Are we teaching them the right skills?,» said Army Lt. Col. Robert Eckart, a 39-year-old cardiologist who heads the joint research team. An equally relevant question is who should be doing what.

Most medevac helicopters carry only a medic or corpsman to attend to the wounded. The Army, however, is starting to rotate critical-care nurses onto helicopters, too. The British armed forces send physicians into the field to assist medics. These varied practices are creating a natural experiment that may shed light on which strategy works best.

«I think a lot of people would like to know that,» said Osborne, the Navy anesthetist on the joint research team.

There are studies on the frontline treatment of traumatic brain injury and on whether heart problems can be adequately addressed without evacuating patients to Germany. There's a study to determine whether muscle-building powders, which troops take like vitamins, affect their livers. One project seeks to learn whether playing with dogs eases combat stress.

As of this week, 586 articles arising from the experiences of the Iraq and Afghanistan wars have appeared in peer-reviewed scientific journals.

There will be more.

Pandemic H1N1 Influenza Vaccine Effective in 2009-10 Flu Season

Source: http://www.sciencedaily.com/releases/2011/01/110111171839.htm

One dose of the pandemic flu vaccines used in seven European countries conferred good protection against pandemic H1N1 influenza in the 2009-10 season, especially in people aged less than 65 years and in those without any chronic diseases. These findings from a study funded by the European Centre for Disease Prevention and Control (ECDC) and coordinated by EpiConcept, Paris, France, published in this week's PLoS Medicine, give an indication of the vaccine effectiveness for the influenza A (H1N1) 2009 strain included in the 2010-11 seasonal vaccines.

The authors conducted a multi-centre case-control study based on practitioner surveillance networks from seven countries — France, Hungary, Ireland, Italy, Romania, Portugal and Spain. Patients consulting a participating practitioner for influenza-like-illness had a nasal or throat swab taken within eight days of symptom onset. Individuals were considered vaccinated if they had received a dose of the vaccine more than 14 days before the date of onset of influenza like illness and unvaccinated if they were not vaccinated at all or if the vaccine was given less than 15 days before the onset of symptoms.

The authors analysed pandemic influenza vaccination effectiveness in those vaccinated less than 8 days, those vaccinated between, and including, 8 and 14 days and those vaccinated more than 14 days before onset of symptoms compared to those who had never been vaccinated. The authors then used statistical models to measure the effectiveness of pandemic influenza vaccine according to three age groups (< 15, 15-64, and 65+ years of age) and the presence of chronic diseases. These results obtained during the late phase of the pandemic suggest good protection with the pandemic H1N1 vaccine (vaccine effectiveness estimates between 65% and 100%). The findings also suggest that the 2009-10 seasonal influenza vaccine (as opposed to the pandemic H1N1 vaccine) did not protect against pandemic H1N1 influenza illness.

The authors said: «The late availability of the pandemic vaccine and subsequent limited coverage with this vaccine hampered our ability to study vaccine benefits during the outbreak period.» They added: «Future studies should include estimation of effectiveness of the new trivalent vaccine in the 2010-2011 season, when vaccination will occur before the influenza season starts.»

Bruno C. Ciancio, senior influenza expert from ECDC — who conceived the idea of a European network to measure influenza vaccine effectiveness and collaborated to design the study- stressed: «This study showed the added value of collaboration at European level as concerns vaccine evaluation. In addition, the results obtained are especially important for European countries this season, considering that the predominant influenza strain currently circulating across Europe is influenza A (H1N1).”

Food Bioterrorism Examined For Dissertation By K-State Doctoral Graduate

Source: http://www.medicalnewstoday.com/articles/212843.php

According to recent news reports, the next venue for a terror threat may involve the use of bio-agents to contaminate the food supplies of U.S. hotels and restaurants. Dave Olds, a December 2010 doctoral graduate in hotel, restaurant, institution management and dietetics from Kansas State University, conducted his dissertation on food security and bioterrorism. His dissertation, «Food Defense Management Practices In Private Country

Clubs,» examined current safety precautions used by country club restaurants to protect food and beverages, as well as how often those practices were put into effect. «I identified country clubs because they typically have an exclusive population. They are places often visited by affluent and influential people and their families, and sometimes even government officials,» Olds said. Other national studies on this venue have not been done, Olds said. The idea came from a former K-State study that investigated food bioterrorism in schools and hospitals. To gather data, Olds, a former chef, surveyed country club managers nationally. In the Midwest he toured the facilities of 25 country clubs and visited with club managers. «I found that intentional contamination of food isn't perceived to be a very common occurrence by club managers. In fact, most couldn't recollect an incident happening,» Olds said. «However, it's one of the oldest forms of terrorism, as there are recorded incidents of this happening in Roman history.» Olds found that 21 of the 25 club managers said they didn't think bioterrorism was a risk at their country clubs. Intentional food contamination can come from two groups: those working inside an operation and those working outside an operation. According to Olds, club managers felt that disgruntled employees were more likely than non-employees to intentionally contaminate food. An incident of this nature occurred in 2009 at a Kansas City restaurant, rather than a country club, when it was discovered that a former employee had mixed pesticide into salsa, Olds said. «One of the quotes in a recent news report on food contamination by Al Qaeda in the Arabian Peninsula said that this is a difficult topic to debate without alarming the public. I think that's very true,» Olds said. «It's really tricky because you want to educate employees and the board of directors, but you don't want to appear to be causing undo panic or even giving people ideas.»

Plague And Bacterial Pneumonias: New Discovery Could Lead To Vaccines

Source: http://www.medicalnewstoday.com/articles/214792.php

There is an ongoing battle in the «war on terror» that remains mostly unseen to the public - a race between scientists working to develop a vaccine to protect against plague and the terrorists who seek to use plague as a weapon. «Governments remain concerned that bioweapons of aerosolized Yersinia pestis, the bacteria that causes plague, could kill thousands,» said Stephen Smiley, a leading plague researcher and Trudeau Institute faculty member. The anthrax scare that followed the terror attacks of September 11, 2001, made the threat of bioterrorism real and led to a surge in federal funding into research aimed at heading off such threats. According to Dr. Smiley, there is no licensed plague vaccine in the United States. Together with postdoctoral associate Jr-Shiuan Lin, he is working to develop a vaccine that will protect members of the armed services and public from a «plague bomb.» Yersinia pestis is arguably the most deadly bacteria known to man. Plague infections of the lung, known as pneumonic plague, are extremely lethal. The bacteria, which grow both inside and outside the cells of the lung, usually lead to death within a week of infection. Most of the plague vaccine candidates that have been studied aim to stimulate B cells to produce plague-fighting antibodies. However, animal studies suggest that antibodies may not be enough to protect humans from pneumonic plague. The Smiley laboratory has shown that T cells can also fight plague. The lab previously demonstrated that a single immunization with an experimental vaccine stimulates the production of T cells that provide partial protection against pneumonic plague. New data, reported in the current issue of The Journal of Immunology, show that a second immunization, or booster, improves the protection provided by T cells. «It is particularly exciting that the boost seems to improve protection by increasing a newly described type of T cell, which we call a Th1

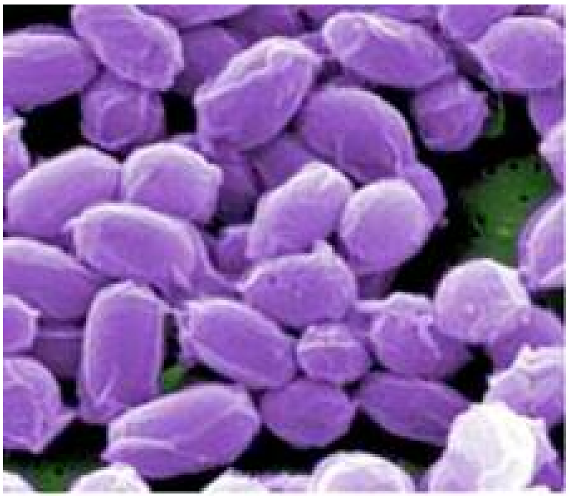
17 cell,» said Dr. Smiley. These cells have characteristics of both Th1 cells, which defend against intracellular bacteria, and Th17 cells, which specialize at killing extracellular threats. This research is focused primarily on thwarting the use of plague as a bioweapon. However, small, natural outbreaks of plague continue to this day. A plague vaccine will protect against both naturally occurring outbreaks and those that have been manufactured. Additionally, Dr. Smiley believes these Th1-17 cells may be important in fighting other kinds of pneumonia: «Bacterial pneumonia is one of the most common causes of death in hospitals and, like plague, many of these pneumonias are caused by bacteria that grow both inside and outside the cells of our bodies.» Dr. Smiley's studies are funded by the Trudeau Institute and grants from the National Institutes of Health. The Trudeau Institute is an independent, not-for-profit, biomedical research organization, whose scientific mission is to make breakthrough discoveries leading to improved human health. Trudeau researchers are identifying the basic mechanisms used by the immune system to combat viruses like influenza, mycobacteria, such as tuberculosis, parasites and cancer, so that better vaccines and therapies can be developed for fighting deadly disease. The research is supported by government grants and philanthropic contributions.

US-backed bio-weapons lab irks Kazakh opposition

Source: http://www.spacewar.com/reports/US-backed_bio-weapons_lab_irks_Kazakh_opposition_999 .html

The Kazakh opposition voiced alarm Tuesday over comments by the US ambassador revealing that the United States intended to help the republic build a «dangerous biological pathogens» facility in its largest city Almaty. The comments by outgoing US Ambassador Richard Hoagland were made at an official reception last week and then published on the embassy website. Hoagland praised the two countries' cooperation on efforts to prevent the spread of weapons of mass destruction, including nuclear weapons. «Just very recently, Kazakhstan and the United States, with the assistance of the Russian Federation, Ukraine, and the United Kingdom, fully secured for the next half century ... enough highly enriched uranium and plutonium to make 775 nuclear weapons,» Hoagland said. He then added: «And today, we are closely engaged with Kazakhstan to construct a world-class facility in Almaty to secure dangerous biological pathogens.» The US embassy was unable to provide further details about the site when contacted by telephone Tuesday. Hoagland's remarks have been picked up by the opposition, with leaders of the Azat National Social Democratic party writing to Prime Minister Karim Massimov with a request for further details about any agreement. «Why has Kazakhstan been selected for the creation of such a dangerous storage site, which is especially located in a highly-seismic zone of the republic's largest city?,» asked the letter. It also demanded to know why the opposition had learned about it from US officials rather than the republic's government. With a population of nearly 1.5 million people, Almaty served as the Central Asian republic's capital until 1997 and remains both its financial centre and largest city. The Kazakh state committee for health and dis

Nura
Kulik
Uzunagach
Kopa
Otar
Chilik
Otegen Batyr
Yeygen'yevka
Samsy
imeni Panfilova
Talgar
Yesik
Ul'ken Sulutor
Uzunagach Fabrichnyy
Kaskelen
Almaty (Alma-Ata)
Pik Talgar
4951
Zhanatalan
Chilik
Zhalan
Ak-Tüz
Kemin
nok
Kungei Alatau
Anan'ev
geti
Bordu
Balykchy (Ysyk-Köl)
Chong-Sary-Oy
Chok-Tal
Cholpon-Ata
Tup
Przheval'sk Pristany
Ysyk-Köl



ease control said in a statement issued to AFP that the centre would «develop and test new diagnostic methods and further identify, study and store (bacterial) strains.» It added that similar «reference laboratories» had already been built in the United States, Canada, Ukraine and Georgia. Three other facilities already store such bacterial strains in Almaty, the Kazakh committee said. Kazakhstan hosted several secret military programmes in the Soviet era, with a biological weapons centre built on the Aral Sea island of Vozrozhdeniye. Semipalatinsk in the northeast of the country was also the Soviet Union's primary nuclear weapons test site.

Tracking the progress of H1N1 swine flu

Source: http://www.ecdc.europa.eu/en/Pages/home.aspx

Seasonal influenza 2010–2011 in Europe (EU/EEA countries)
January 2011

The 2010/11 seasonal influenza epidemics in Europe are dominated so far by the A(H1N1)2009 viruses which emerged in the 2009 pandemic, although these are now considered seasonal viruses. There are also some B viruses circulating. Both are causing some severe disease and premature deaths but the preliminary data indicate that 90% of the fatalities are due to A(H1N1)2009

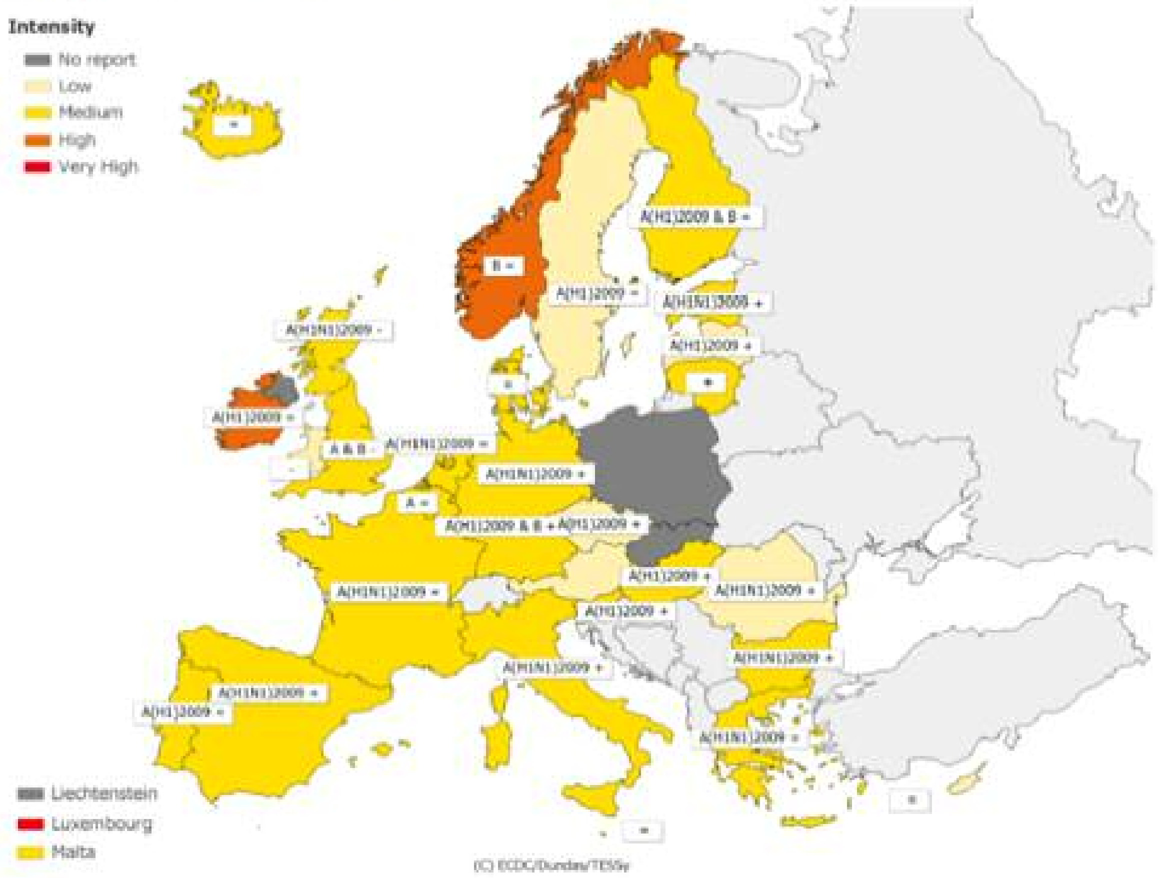
This is the first European influenza season after the 2009 pandemic. Many of the features and required countermeasures are the same as for the previous seasonal influenzas (which ran until the 2008/09 season). However, there are important differences which Europe needs to take into consideration, notably the type of people who are most affected and experiencing severe disease.

In the first affected country (the United Kingdom) there have been higher numbers of people seeking care than on average with seasonal influenza. Also, the number of people with severe disease has been considerably higher than during the pandemic with at its peak 1.4 persons/105 population requiring higher level (intensive) hospital care at one time. The reason for the latter finding is unclear. Part of the reason for the increased demand in primary care has been persons seeking immunisation or treatment as information on the severe cases became apparent to the public. These phenomena have also been observed in other countries in Western Europe, albeit at lower levels.

A broad pattern of west to east progression of influenza epidemics is underway, such as has been seen in previous years. Hence the experience of the Western countries can inform those further to the east of the European Union. All these considerations constitute the justification for this Interim ECDC Risk Assessment, which will be updated at intervals.

Those mostly reported as experiencing severe disease or dying prematurely are those adults below the age of 65 years and children in the clinical risk groups. These constitute over 80% of cases reported. Severe disease also affects some pregnant women. There are also some previously entirely healthy people.

Map 1: Intensity for week 2/2011



(C) ECDC/Dundas/TESSy

* A type/subtype is reported as dominant when > 40 % of all samples are positive for the type/subtype.

Legend:

Low	No influenza activity or influenza at baseline levels
Medium	Usual levels of influenza activity
High	Higher than usual levels of influenza activity
Very high	Particularly severe levels of influenza activity

-	Decreasing clinical activity
+	Increasing clinical activity
=	Stable clinical activity
A	Type A
A & B	Type A and B
A(H1)2009	Type A, Subtype (H1)2009
A(H1)2009 & B	Type B and Type A, Subtype (H1)2009
A(H1N1) 2009	Type A, Subtype (H1N1)2009
B	Type B

who account for 20% of the deaths in the UK, and higher percentages requiring higher-level (intensive) hospital care in France. As in the pandemic, there have been some older people experiencing severe disease but reported cases have been low in numbers.

Numbers of severely ill cases requiring care are now declining in the UK but they are rising in other countries. It cannot be anticipated whether those countries will experience the same rates as the UK.

The circulating viruses have not as yet changed or mutated, and it is expected that the seasonal vaccines will be effective in preventing disease. ECDC-coordinated studies in the pandemic found up to 80% effectiveness for vaccines containing A(H1N1)2009. Other observational studies have confirmed this. Indeed there are encouraging data suggesting that significant protection develops within a week of immunisation. Data on the early deaths in the UK indicate that the vaccines in use are also effective in preventing influenza-related deaths.

Recent surveys of pandemic and seasonal vaccine coverage by Member States indicate that there are many people in the clinical risk groups in Europe who remain unvaccinated, either with the pandemic vaccine or the 2010 seasonal vaccine.

In the UK, there is a rise in laboratory reports of two or more severe invasive bacterial diseases; pneumococcal disease and group A streptococcal disease has been observed. Rates of invasive streptococcal disease rose to 0.33/105 population in December 2010 compared to 0.19/105 in an average year. To date, this has not been reported elsewhere in Europe. It is unclear whether this rise is associated with the influenza epidemics and contributing to the high numbers of severe cases in the UK, but that is a possibility.

The scientific evidence to date provides justification for the following countermeasures already adopted by some countries in addition to the usual influenza personal protective measures (early self isolation, respiratory hygiene and hand-washing):

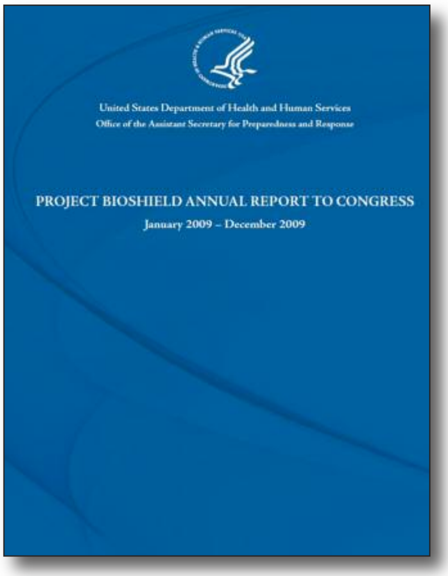
- Continued vaccination of all those recommended for vaccination following national guidelines but especially clinical risk groups, including pregnant women, especially as it seems that the vaccine provides some protection even just a week after injection. However, there may be vaccine availability, logistical and administrative issues that will make this difficult in some settings.
- Use of antiviral treatment in those presenting with severe influenza-like illness, pending virological confirmation, and in those with risk factors with milder disease.
- Alerting higher level healthcare services of potential increased numbers of influenza patients this winter, potentially already in the next few weeks.
- Advising clinicians to be vigilant to the possibility of severe illness due to bacterial co-infection with influenza, including invasive group A streptococcal, pneumococcal and meningococcal infection, and to be aware of the possibility of such bacterial co-infection in people with flu-like illness.
- Use or creation of clinical networks for surveillance, evaluation and sharing of clinical experience.

This is an interim risk assessment and will be up-dated at intervals as more data and analyses emerge.

BioShield projects sees vaccine, treatments successes

Source: http://homelandsecuritynewswire.com/bioshield-projects-sees-vaccine-treatments-successes

Efforts on behalf of the U.S. Department Health and Human Services to ensure that the United States has medical countermeasures (MCMs) available for responding to a chemical, biological, radiological, or nuclear (CBRN) event have been successful in developing the first human vaccine for avian flu, as well as delivering treatments for anthrax (vaccines and therapeutics), radiation exposure, and botulism to the Strategic National Stockpile (SNS) . As required by congress, the latest annual report on Project BioShield has been published by the U. S. Department of Health and Human Services (HHS), Office of the Assistant Secretary for Preparedness and Response. The report covers activities and efforts to diversify the medical countermeasures (MCM) enterprise from January 2009-December 2009. Efforts on behalf of the HHS to ensure that the country has medical countermeasures (MCMs) available for responding to a chemical, biological, radiological, or nuclear (CBRN) event have been successful in developing the first human vaccine for avian flu, as well as delivering treatments for anthrax (vaccines and



United States Department of Health and Human Services
Office of the Assistant Secretary for Preparedness and Response

PROJECT BIOSHIELD ANNUAL REPORT TO CONGRESS
January 2009 – December 2009

therapeutics), radiation exposure, and botulism to the Strategic National Stockpile (SNS). R&D efforts for a smallpox vaccine and additional countermeasures for the SNS are underway.

Despite advances made since the program's inception in 2004, Project BioShield still needs "adaptable distribution plans in place to deliver countermeasures to every American quickly," according to Nicole Lurie, MD, assistant secretary for preparedness and response, HHS. Throughout 2009, antitoxins to anthrax and botulinum were delivered to the SNS through existing contracts administered by the Biomedical Advanced Research and Development Authority (BARDA), a department within HHS. In March 2009 a solicitation was successfully issued to support the procurement of 1.7 million treatment courses of smallpox antiviral drugs. The project has run into considerable difficulty in developing and procuring a next generation anthrax vaccine. BioShield officials are hoping that the termination of a solicitation in December 2009 to support late-stage development of 20 million doses of vaccine will result in a more mature and reliable product being developed. The annual report describes streamlining procedures in awarding grants, contracts, and cooperative agreements in developing countermeasures. Section Four of the Project BioShield Act allows the Secretary of HHS to declare the use of unapproved products (also known as Emergency Use Authorization [EUA]) in an event determined to be an emergency by DHS or Defense. EUA has been used by the FDA in response to the 2009 H1N1 flu virus. In the event that an emergency is declared by the HHS secretary, the FDA commissioner must consult with the National Institutes of Health (NIH) and the Centers for Disease Control and Prevention (CDC) to ascertain the correct plan of action. Of the $5.6 billion in the Special Reserve Fund for Project BioShield, $2.4 billion remains as of December 2009. Contracts awarded using the Special Reserve Fund are primarily of the fixed priced variety. BARDA has awarded 9 contracts for development and acquisition of CBRN medical countermeasures valued at over $2 billion, and has successfully stockpiled seventeen medical products against six CBRN threats.

The 2009 report details the status of several acquisition contracts, its recipients, total funding, and reasons specific authority use and terminated contracts.

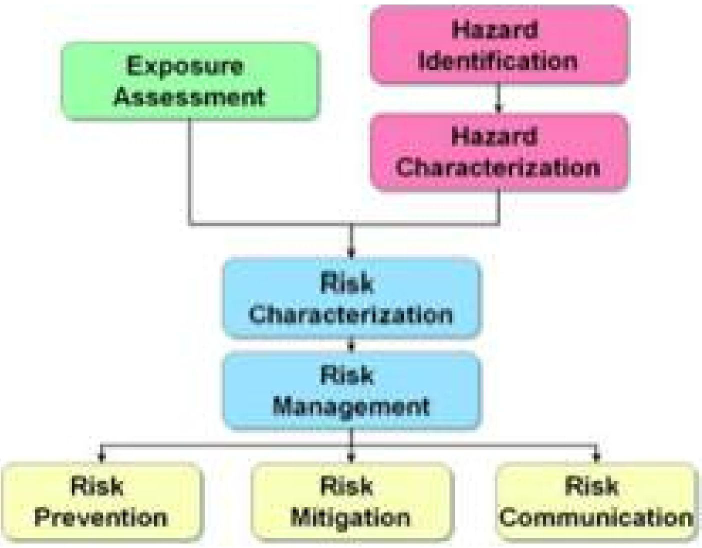
- Human Genome Sciences (HGS) was awarded $326 to develop Raxibacumab (an antitoxin used to treat Anthrax)
- Cangene was awarded $558 million to develop and procure Anthrax Immune Globulin (AIG, an antitoxin also used to treat Anthrax) as well as Botulinum Antitoxin (hBAT) therapeutic. The deliveries of treatments as specified by the contracts are still ongoing.
- Emergent, a global biopharmaceutical company focused on the development, manufacturing, and commercialization of vaccines and antibody therapies (formerly BioPort), received $691 million to procure 28.75 million doses of AVA (BioThrax, Anthrax vaccine absorbed).
- A $2 million contract for rPA (Recombinant Protective Antigen), an Anthrax vaccine treatment, was terminated between VaxGen in December of 2006 for failing to meet contract requirements. This termination of this contract was thought to have been a premature decision according to top scientists in the field. On 28 July 2010, VaxGen completed a merger transaction with diaDexus, Inc., a diagnostics company that focuses on the development and commercialization of patent-protected in vitro diagnostic products.

- Denmark-based Bavarian Nordic, an industrial biotechnology company that develops and produces vaccines for the treatment and prevention of life-threatening diseases, was awarded $505 million for their Imvamune (MVA, Modified Vaccinia Ankara) Smallpox vaccine. 1.15 million doses of the 10 million doses contract have been delivered as of 2009.
- Based in the greater St. Louis area, Fleming, a pharmaceutical company that specializes in the discovery, development, and manufacture of innovative prescription and over-the-counter (OTC) therapies, was awarded $18 million for providing 4.8 million bottles of Potassium Iodide (Thyroshield), a pediatric treatment.
- Illinois-based Akorn was awarded $22 million for close to 500,000 doses of IV Calcium/Zinc DTPA (Diethylene triamine pentaacetic acid), a treatment for internalized radionuclides.

How Safe Is Nano? Nanotoxicology: An interdisciplinary challenge

Source: http://www.nanowerk.com/news/newsid=19905.php

The rapid development of nanotechnology has increased fears about the health risks of nano-objects. Are these fears justified? Do we need a new discipline, nanotoxicology, to evaluate the risks? Harald F. Krug and Peter Wick of the Swiss Federal Laboratories for Materials Science and Technology discuss these questions in the journal Angewandte Chemie. “Research into the safety of nanotechnology combines biology, chemistry, and physics with workplace hygiene, materials science, and engineering to create a truly interdisciplinary research field,” explain Krug and Wick. “There are several factors to take into account in the interaction of nano-objects with organisms,” they add. The term nanotoxicology is fully justified. “Nanoscale particles can enter into cells by other means of transport than larger particles.” Another critical feature is the large surface area of nano-objects relative to their volume. If a similar amount of substance is absorbed, an organism comes into contact with a significantly larger number of molecules with nanoparticles than with larger particles. Dose–effect relationships cannot therefore be assumed to be the same. Furthermore, chemical and physical effects that do not occur with larger particles may arise. “Whether the larger or smaller particle is more toxic in any given case cannot be predicted,” according to the authors. “Clearly, the type of chemical compound involved and its conformation in a specific case can also not be ignored.” Carbon in the form of diamond nanoparticles is harmless, whereas in the form of nanotubes—depending on length and degree of aggregation—it may cause health problems. It is also thus impossible to avoid considering each nanomaterial in turn. For a risk assessment, it is also necessary to keep in mind what dosage would be considered realistic and that not every observed biological effect automatically equates to a health risk



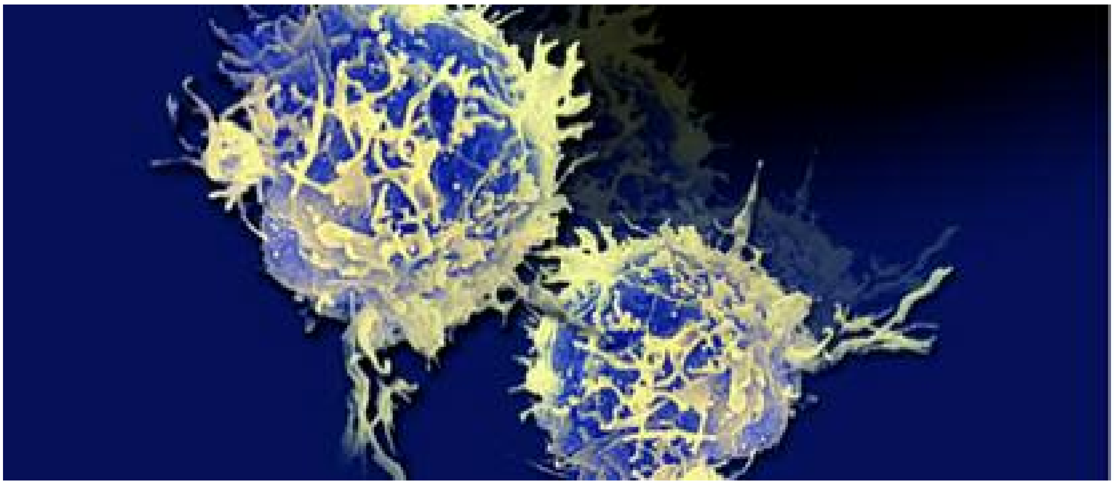
Krug and Wick indicate that a large amount of data about the biological effects of nanomaterials is available, but not all studies are reliable. Sometimes it is not possible to reproduce the specific material tested or the conditions. "By pointing out methodological inadequacies and making concrete recommendations for avoiding them, we are hoping to contribute to a lasting improvement in the data," state Krug and Wick.

More information: Harald F. Krug, Nanotoxicology: An Interdisciplinary Challenge, Angewandte Chemie International Edition, Permalink to the article: http://dx.doi.org/ … ie.201001037

T cells offer new promise for vaccines for plague and bacterial pneumonias

Source: http://homelandsecuritynewswire.com/t-cells-offer-new-promise-vaccines-plague-and-bacterial-pneumonias

There is currently no licensed plague vaccine in the United States, which is too bad because Yersinia pestis is arguably the most deadly bacteria known to man; most of the plague vaccine candidates that have been studied aim to stimulate B cells to produce plague-fighting antibodies, but animal studies suggest that antibodies may not be enough to protect humans from pneumonic plague; new studies show that T cells can also fight plague — and may be better candidates with which to develop a plague vaccine. There is an ongoing battle in the war on terror that remains mostly unseen to the public — a race between scientists working to develop a vaccine to protect against plague and the terrorists who seek to use plague as a weapon. "Governments remain concerned that bioweapons of aerosolized Yersinia pestis, the bacteria that causes plague, could kill thousands," says Stephen Smiley, a leading plague researcher and Trudeau Institute faculty member. The anthrax scare that followed the terror attacks of 9/11 made the threat of bioterrorism real and led to a surge in federal funding into research aimed at heading off such threats. According to Smiley, there is no licensed plague vaccine in the United States. Infection Control Today reports that together with postdoctoral associate Jr-Shiuan Lin, he is working to develop a vaccine that will protect members of the armed services and public from a "plague bomb." Yersinia pestis is arguably the most deadly bacteria known to man. Plague infections of the lung, known as pneumonic plague, are extremely lethal. The bacteria, which grow both inside and outside the cells of the lung, usually lead to death within a week of infection. Most of the plague vaccine candidates that have been studied aim to stimulate B cells to produce plague-fighting antibodies. Animal studies suggest, however



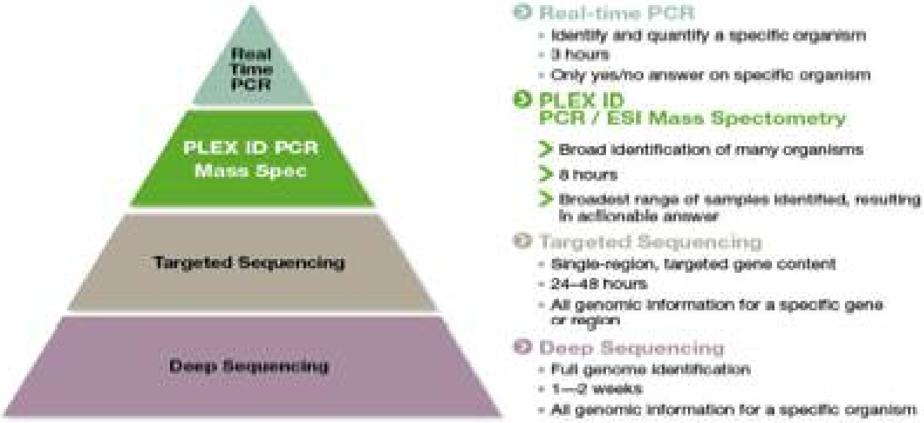
that antibodies may not be enough to protect humans from pneumonic plague. The Smiley laboratory has shown that T cells can also fight plague. The lab previously demonstrated that a single immunization with an experimental vaccine stimulates the production of T cells that provide partial protection against pneumonic plague. New data, reported in the current issue of the Journal of Immunology, show that a second immunization, or booster, improves the protection provided by T cells. "It is particularly exciting that the boost seems to improve protection by increasing a newly described type of T cell, which we call a Th1-17 cell," says Smiley. These cells have characteristics of both Th1 cells, which defend against intracellular bacteria, and Th17 cells, which specialize at killing extracellular threats. This research is focused primarily on thwarting the use of plague as a bioweapon. Small, natural outbreaks of plague, however, continue to this day. A plague vaccine will protect against both naturally occurring outbreaks and those that have been manufactured.

Additionally, Smiley believes these Th1-17 cells may be important in fighting other kinds of pneumonia: "Bacterial pneumonia is one of the most common causes of death in hospitals and, like plague, many of these pneumonias are caused by bacteria that grow both inside and outside the cells of our bodies." Smiley's studies are funded by the Trudeau Institute and grants from the National Institutes of Health.

New pathogen detector

Source: http://www.polijam.com/index.php?option=com_content&view=article&id=55740:abbott-unveils-new-pathogen-detector&catid=55:business&Itemid=54

A new assay system that can accurately detect **17 different bio-threat pathogens** has been introduced by Abbott, an Illinois pharmaceutical company. «While public health officials concerned with bioterrorism and emerging infectious diseases are detecting known, conventional infectious agents, it's becoming very clear there is a need for broader detection and characterization of pathogens for bio-defense,» said David Ecker, divisional vice president and general manager, of Abbott's Ibis Biosciences subsidiary. "The PLEX-ID system's new bio-threat assay will serve that need by identifying and quantifying, for non-diagnostic purposes, a broad set of pathogens including bacteria and families of viruses in humans and animals.» Abbott unveiled its PLEX-ID system at the American Society for Microbiology Conference on Biodefense and Emerging Diseases in Washington.The company said the PLEX-ID Bio-threat Assay permits analysis of direct specimens, such as blood, water, food and air filter samples, and provides results in less than eight hours. Among different bio-agents targeted in the new test are Bacillus anthracis, E. coli, salmonella, Ebola virus and avian influenza viruses.


Real Time PCR
PLEX ID PCR Mass Spec
Targeted Sequencing
Deep Sequencing
Real-time PCR
Identify and quantify a specific organism
3 hours
Only yes/no answer on specific organism
PLEX ID
PCR / ESI Mass Spectometry
Broad identification of many organisms
8 hours
Broadest range of samples identified, resulting in actionable answer
Targeted Sequencing
Single-region, targeted gene content
24–48 hours
All genomic information for a specific gene or region
Deep Sequencing
Full genome identification
1—2 weeks
All genomic information for a specific organism

CHEM-BIO DEFENSE

Quarterly

Vol. 7 No. 2

One Mission, One Team

Army orders radios for bio-threat system

Source: http://www.upi.com/Business_News/Security-Industry/2011/02/10/Army-orders-radios-for-bio-threat-system/UPI-86981297347557/#ixzz1DfPrzPtq

Harris Corp. of New York is providing the U.S. Army with high-frequency radios for use with a biological threat detection system under a $9 million order. Under the order, Harris will supply Falcon II 400-watt AN/PRC-150(C) HF systems for the Army's Joint Biological Point Detection System, which is designed to detect and identify biological warfare agents. The AN/PRC-150(C) automatically communicates alerts to headquarters over HF radio links when biological agents are detected, the company said. «Harris is the market leader in tactical, high-frequency radio communications,» said Brendan O'Connell, president, Department of Defense business, Harris RF Communications. «We have supported the integration of our radio systems into many types of customer programs. «In this instance, the Army is taking advantage of the secure data transmission capabilities of the AN/PRC-150 to give U.S. forces the maximum amount of time to respond to potentially significant threats.» The AN/PRC-150(C) is an NSA Type-1 certified HF radio system. Widely deployed, the AN/PRC-150(C) provides continuous coverage in the 1.6-to-60 MHz frequency range, delivering secure voice and data communications even in the harshest conditions.

Tool developed to monitor pandemic threats

Source: http://homelandsecuritynewswire.com/tool-developed-monitor-pandemic-threats

An Emerging Pandemic Threats (EPT) tool, known as «Predict,» will enable scientists and the public to track outbreaks of communicable animal diseases; Predict will monitor data from 50,000 Web sites with information from World Health Organization (WHO) alerts, online discussions by experts, wildlife trade reports, and local news. Created with a grant from the United States Agency for International Development (USAID), an Emerging Pandemic Threats (EPT) tool, known as "Predict," will enable scientists and the public to track outbreaks of communicable animal diseases. The goal of the program is to preempt or combat, at their source, newly emerging diseases of animal origin that could threaten human health. The tool is being produced by experts on human and animal diseases from a consortium that first came together in 2009 during the pandemic of H1N1 swine flu. The experts have focused their attention on animal diseases that infect humans, such as the virus that caused the outbreak of SARS and the viruses (Ebola in cluded) that are believed to have originated in bats. Predict will monitor data from 50,000 Web sites with information from World Health Organization (WHO) alerts, online discussions by experts, wildlife trade reports, and local news. Damien Joly, an associate director of wildlife health monitoring for the Wildlife Conservation Society, said "We strongly believe in public access to the data we collect. It doesn't do public health much good to collect data and let it sit while it awaits publication." The EPT program is being managed by USAID with technical support from the U.S. Centers for Disease Control and Prevention and the United States Department of Agriculture.

Terror attack fears over London virus superlab

Source: http://homelandsecuritynewswire.com/terror-attack-fears-over-london-virus-superlab

Experts express concern over the 600 million Pound virus «superlab» planned for St. Pancras, London; the 14-story, maximum security site containing viruses including malaria, tuberculosis, bird and swine flu, cancer cells, and HIV would need to be «bullet-proof» to withstand not only an earthquake, a bomb, or fire — there are also worries that Tube trains running through King's Cross and Euston stations could ruin delicate and expensive laboratory equipment.

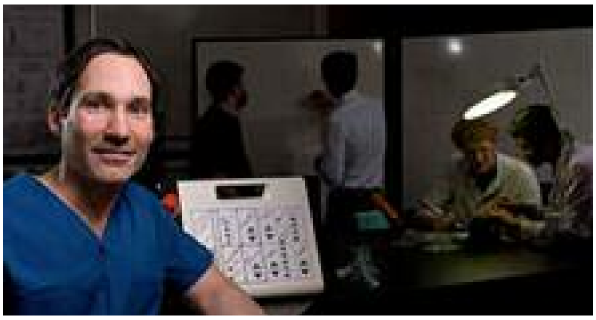
Artist rendering of London's planned virus superlab // Source: thisislondon.co.uk

One of Britain's leading bio-scientists yesterday voiced fears over the safety of a £600 million virus "super-lab" planned for St. Pancras, London. Professor Guy Dodson, who has worked at Oxford University, warned that the 14-storey, maximum security site containing viruses including malaria, tuberculosis, bird and swine flu, cancer cells, and HIV would need to be "bullet-proof." He told the Evening Standard: The issues are if you have an earthquake, some idiot lets a bomb off or there's a fire at St Pancras International. These are extreme examples but you don't want that building to suffer a serious knockabout when you've got this material in there. The unspoken concern is terrorism because it's a natural target. We need to know the capacity they have for dealing with the unexpected. The biochemist's fears echo those of some of the thousands living nearby. The U.K. Center for Medical Research and Innovation will have several underground laboratories. Professor Dodson is also concerned that vibrations from Tube trains running through King's Cross and Euston could ruin delicate and expensive laboratory equipment. In written evidence to a Commons Science and Technology select committee inquiry, he wrote: "I fear that the £600 million funding will not be sufficient to meet the uncertainties in building and equipping the laboratories." The consortium behind the project includes the Medical Research Council, Cancer Research U.K., and the Wellcome Trust. The Evening Standard reports that the center, which has won planning permission from Camden council and been approved by London Mayor Boris Johnson, said bio-security will be among the tightest in Britain. A UKCMRI spokesman said: "A number of submissions have been made. We look forward to discussing with MPs the development of this world-leading institute which represents a superb investment in the battle to improve the health of people across the capital and country."

Researchers Develop Low-cost Medical Ventilators for Global Disasters

By Stanford University Medical Center

Source: http://med.stanford.edu/ism/2011/february/ventilator-0214.html



After learning that his hospital would be short ventilators in the event of an influenza pandemic, Matthew Callaghan sketched out concepts for a less inexpensive ventilator on a napkin at a lunchtime meeting with a fellow physician. Matthew Callaghan, MD, had an epiphany about medical device design during a pandemic planning meeting, when his hospital was drafting a worst-case scenario protocol to decide which types of patients would receive life support from the hospital's limited number of breathing ventilators. "The physicians assumed that we'd have to ration the ventilators, and that if we put the criteria on paper, we wouldn't feel bad about the life-or-death decisions we were making," said Callaghan. "All of a sudden, I realized that the task force wasn't addressing the root problem. So I asked, 'Why not design a cheaper ventilator so rationing isn't necessary?'" So Callaghan started to think about why ventilators, which primarily move air in and out of impaired lungs, cost upwards of $40,000, and why no one had designed a low-end model that could be stockpiled for large-scale disasters. Fortunately, the fact that he was a surgical resident at UC-San Francisco at the time wasn't a mental barrier for Callaghan, who has degrees in product design and biology from Carnegie Mellon, a medical degree from State University of New York, a medical fellowship from New York University and now a postdoctoral position in Stanford University's biodesign program. In addition, his kindergarten report card probably said, "He colors outside of the lines." He began by inviting a physician friend to lunch, and they began sketching some ideas on a napkin. After learning that the United States would be short about 700,000 ventilators during a moderate-to-severe influenza pandemic, they realized that they might be able to build a business around their ideas. Three years later, Callaghan's team is close to commercially launching a low-cost ventilator, called OneBreath, which will be the first device specifically designed to address the global shortage of emergency The OneBreath ventilator went from napkin sketch to finished product with the help of Stanford Biodesign, a training incubator in medical technology that brings together multidisciplinary teams of medical, engineering, law and business school students to address unmet medical needs with innovative approaches. This program, which was founded 10 years ago, has jump-started a number of successful innovations, including a new approach to minimally invasive spine surgery (Simpirica Spine); a more cost-effective way to diagnose heart rhythm abnormalities (iRhythm); and a device to accelerate healing of skin ulcers (Spiracur). Stanford Biodesign recently established joint programs in India and Singapore to specifically help accelerate medical solutions for underserved populations. The Stanford Biodesign credo is that medical innovation can be taught, and all design teams learn a systematic approach to needs finding, invention and implementation. Before biodesign fellows even get close to building a prototype, they spend three months on clinical observation, asking questions, identifying needs, analyzing markets and brainstorming concepts. Along the way, they also learn about managing intellectual property, the regulatory process and medical reimbursements, applying this knowledge to their specific projects. Pictured: From left: Larry Miller, Matthew Callaghan, William Bishop, Frederick Winston and Dhruv Boddupolli show an early prototype of the OneBreath ventilator that they have developed. Their device, which is at least a year away from roll-out, is projected to be sold at a

From left: Larry Miller, Matthew Callaghan, William Bishop, Frederick Winston and Dhruv Boddupolli show an early prototype of the OneBreath ventilator that they have developed. Their device, which is at least a year away from roll-out, is projected to be sold at a fraction of the cost of a typical hospital ventilator.

fraction of the cost of a typical hospital ventilator. “We say that a well-characterized need is the DNA of a good invention. It’s a lot of work to get the need right, but once you are there, the invention will almost certainly follow,” said Paul Yock, MD, director of Stanford Biodesign. With the help of this methodology, members of Callaghan’s team were able to focus their concepts to more effectively address a need device manufacturers missed — the pandemic/disaster ventilator market in developing nations. In these areas of explosive population growth, health-care infrastructure is limited, and the demand for low-cost ventilators is great, especially in China, where large influenza outbreaks are common. “Our team decided to design a ventilator that could operate in the middle of nowhere during emergencies, without all the bells and whistles — such as remote monitoring or neonatal care — that are not only hard to use, but are only needed for one in 1,000 patients,” said Callaghan. By starting with a narrow design target, the form and function of their device began to diverge radically from hospital ventilators, which often resemble 747 cockpits on rollers, with busy computer screens, control modules, air reservoirs, oxygen supplies and a tangle of cords and tubes. Structurally, the OneBreath team lowered manufacturing costs by reducing the number of parts; airflow is measured and controlled with propriety software rather than hardware. To ensure operability and portability during earthquakes, floods, tsunamis and other disasters, the compact plastic housing is rugged, grime-resistant, stackable and easy to carry. To cope with power outages, units come with a seven-hour rechargeable battery. Because expert technicians are few and far between during disasters, the units are simple enough for novices to operate and repair, and breathing tube replacement costs are 50 cents, rather than the $180 required with high-end ventilators. With an out-the-door cost targeted at less than $800, OneBreath’s retail price should be a fraction of comparable ventilators, priced so that governments and institutions can afford to stockpile units for potential disasters. Thomas Krummel, MD, chair of the Department of Surgery and a Stanford Biodesign co-director, is enthusiastic about the project: “I love the duality of the OneBreath solution, the way its affordability addresses the West’s need for pandemic preparedness, while at the same time addressing the developing world’s need for basic, inexpensive ventilators.” So far the product has been well-received; it was named a Popular Science Invention of the Year in 2010 and has won awards from the American Association for Respiratory Care, the American College of Surgery Clinical Congress and NCIAA BMEidea. Callaghan credits the Stanford entrepreneurial spirit, in part, for OneBreath’s success. “When we needed a business plan, we visited the Stanford Graduate School of Business, and three students wrote our plan as part of a class assignment. After we built our first cardboard prototypes, we went over to Stanford’s pulmonary and critical care office with donuts and coffee, and the physicians were happy to provide user feedback.” Before his biodesign fellowship, Callaghan had no idea how hard it was to get a medical device through the regulatory process: “I laugh when I look back at our early grant applications, where we estimated that it’d take $20,000 and seven months to get our device approved by the FDA.” Thus far, the biodesign-led development process has taken two years, with the addition of a Wallace H. Coulter Foundation grant and award money from a number of design competitions. Biodesign is supported from a variety of internal and external sources, including pilot and fellowship grants from Spectrum, the organization that oversees Stanford's NIH-funded Clinical and Translational Science Award. Callaghan estimates it'll take at least another year and $2.5 million to usher OneBreath through final testing, agency approvals, pilot manufacturing and lockdown of technical documentation. If the device is successfully launched, all the intellectual property holders — the OneBreath inventors, the investors and Stanford — share in any future profits. While they're waiting for agency approvals in the United States and Europe, they'll field test pilot units in China and India. By documenting their successes overseas, they hope to convince U.S. institutional buyers, who often perceive lower-priced medical devices as less effective or risky, to give their ventilators a try. Callaghan is now going through the bittersweet process of transitioning his recently incorporated company to a new CEO, Bryan Loomas, who has 27 years in the medical device business; and a VP of business development, Frederick Winston, who graduated from the Stanford Graduate School of Business. Stephen Ruoss, MD, associate professor of pulmonary and critical care medicine is Callaghan's technical advisor. Looking forward, Callaghan has several new medical ideas that he's eager to develop. His advice to others with similar aspirations: "Assemble a small team of quality people — engineers, physicians, MBAs — who are all willing to wear multiple hats. In a start-up, everyone needs to do everything, from spell-checking brochures to taking out the trash." Kris Newby is the communications manager for Spectrum, the Stanford Center for Clinical and Translational Education and Research.

Most-Read Articles by Emergency *Medicine Physicians*

Jennifer A. Eaton

Source: http://www.medscape.com/viewarticle/733492?src=mp&spon=45

Medscape publishes thousands of articles each year, ranging from our own expert commentaries and medical news to full-text selections from your favourite journals. Our editors aim to provide physicians with timely clinical updates, perspectives on healthcare reform, practice management ideas, and more. Below is a list of the top-10 most-read articles by emergency medicine physicians on Medscape in 2010.

1. Safety and Efficacy of Rapid Titration Using 1 mg Doses of IV Hydromorphone in Emergency Department Patients With Acute Severe Pain: The «1+1» Protocol
   Journal Article/Access Medicine from McGraw Hill
2. Treating the Intense Pain of Renal Colic
   Viewpoint/Knox H. Todd, MD, MPH
3. NDM-1 — Making Resistant Bugs in New Ways
   Article/Carol Peckham, Editor, Medscape
4. Six Ways to Earn Extra Income From Medical Activities
   Article/Dennis G. Murray
5. Revolutionary Advances in the Management of Traumatic Wounds in the ED: During the Last 40 Years: Part I
   Journal Article/The Journal of Emergency Medicine
6. Washington Watch: CDC Report on ED Capacity
   Article/American Academy of Emergency Medicine
7. 25 Years in the Emergency Department — Lessons Learned:
   An Expert Interview With Robert McNamara, MD
   Conference Coverage/AAEM 16th Annual Scientific Assembly
8. Is CT Indicated for Patients With Isolated Syncope?
   Ask the Experts/Robert Glatter, MD
9. An Unusual Foreign Body As Cause of Chronic Sinusitis
   Case Report/Journal of Medical Case Reports
10. What Does the Healthcare Reform Bill Really Mean for Doctors?
    Article/Leslie Kane, MAC, Editor, Medscape

CSS
ETH Zürich
Strategic Trends Analysis
ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

The Centre for Security Studies at ETH Zurich would like to draw your attention to the following recent publications on its Strategic Trends Analysis website:

CSS Analysis in Security Policy No. 88
Progress in Biotechnology as a Future Security Policy Challenge
by Sergio Bonin

Biological weapons do not figure prominently in current threat analyses. However, this might change with advances in biotechnology, and synthetic biology in particular. If the synthetic construction and modification of bacteria and viruses should become a reality, a broad range of useful applications in medicine, environmental protection, and other fields would be facilitated. At the same time, however, constructing biological weapons could become easier, and the necessary skills would be available to a larger spectrum of actors. It seems advisable to explore preventive countermeasures at an early stage.

Dirty News

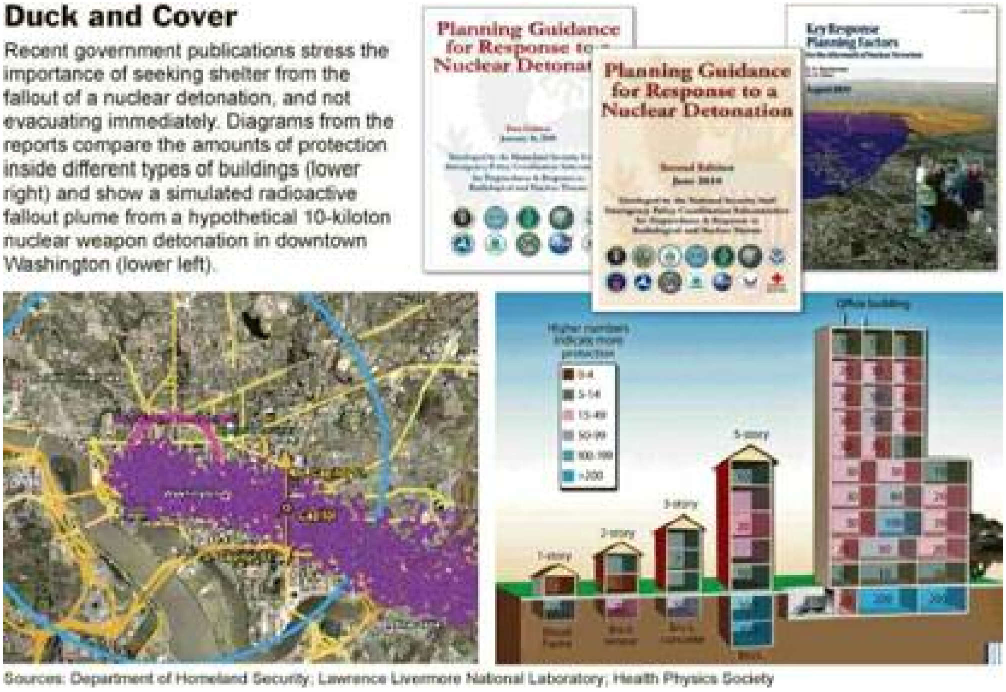
“Dirty bomb” threat at Sellafield; Staff vettig loophole raises

Source: http://findarticles.com/p/articles/mi_qn4156/is_20020616/ai_n12576799/

The ultimate nightmare of a terrorist with a nuclear bomb may be closer than you thought. Britain’s nuclear security is shot full of holes, according to a startling new report for the government. Procedures for vetting workers at a plutonium plant in Sellafield in Cumbria have been flawed, raising the alarming spectre of an insider being recruited by a terrorist organisation. With just five kilograms of plutonium a well organised group like al-Qaeda could make a bomb capable of blowing the heart out of a city.

The revelation is contained in the first ever report from the Office for Civil Nuclear Security, a shadowy state agency charged with protecting Britain’s 31 nuclear sites against terrorist attack. It discloses that there were problems at the Sellafield plant with «outstanding vetting clearances for which temporary compensation arrangements had to be made». The Office, which has an annual budget of (pounds) 1.6 million and a staff of 35, is responsible for vetting all the workers in nuclear plants who have access to sensitive materials like plutonium and uranium. It has faced «unremitting pressure» over the past 12 months in vetting 9178 staff for the first time and 3356 staff for a second time, Frank Barnaby, a nuclear consultant who used to work at the Aldermaston atomic weapons plant in Berkshire, pointed out that insiders could also damage vital cooling systems at waste stores or reactors. «That would be a disaster,» he said. «We should do everything to make sure that it doesn’t happen.»

Rob Edwards «‘Dirty bomb’ threat at Sellafield; Staff vettig loophole raises». Sunday Herald, The. FindArticles.com. 14 Dec, 2010. http://findarticles.com/p/articles/mi_qn4156/is_2002 0616/ai_n12576799/



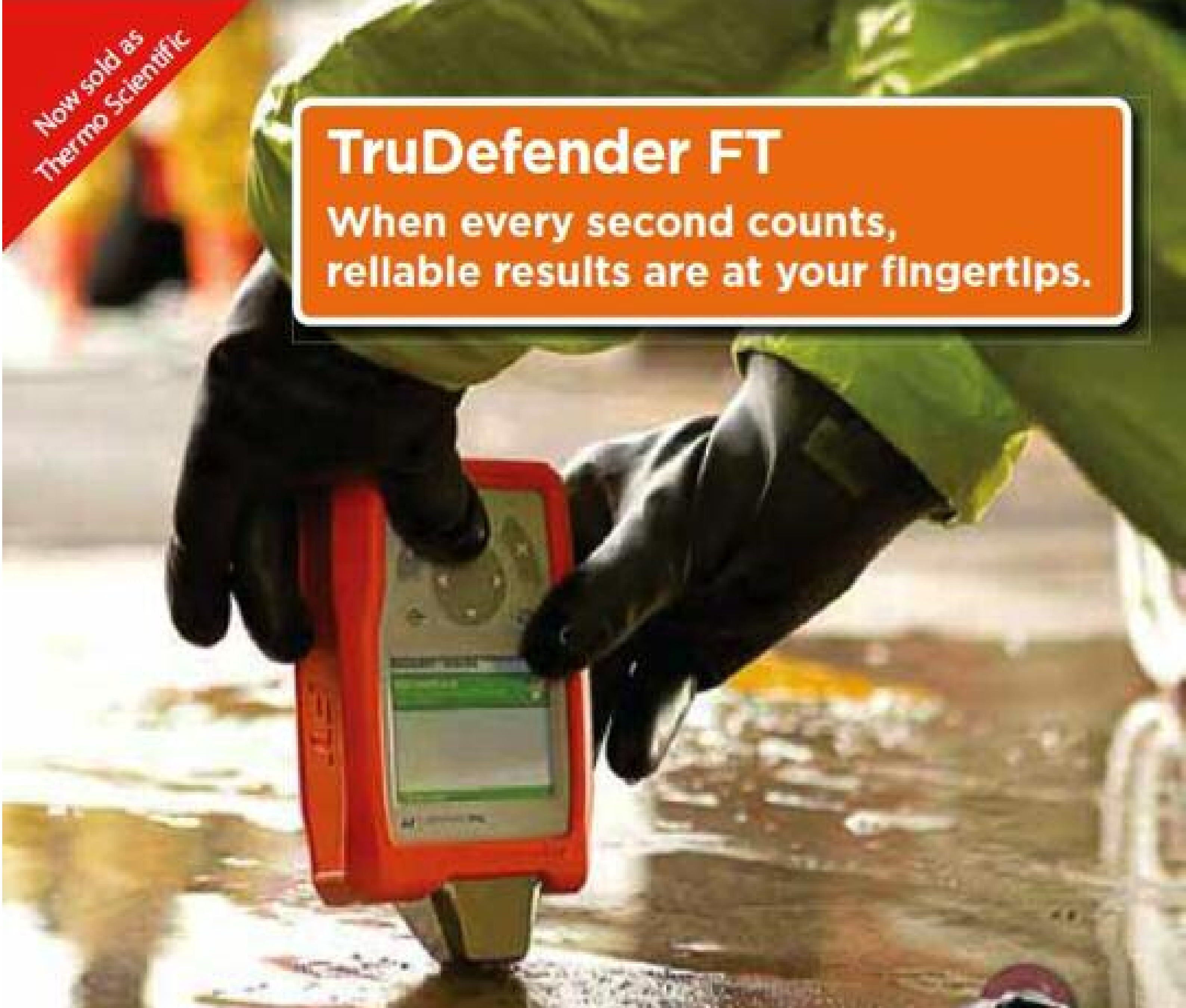
Duck and Cover

Recent government publications stress the importance of seeking shelter from the fallout of a nuclear detonation, and not evacuating immediately. Diagrams from the reports compare the amounts of protection inside different types of buildings (lower right) and show a simulated radioactive fallout plume from a hypothetical 10-kiloton nuclear weapon detonation in downtown Washington (lower left).

Planning Guidance for Response to a Nuclear Detonation
Planning Guidance for Response to a Nuclear Detonation
Second Edition
June 2010
Key Response Planning Factors
Higher numbers indicate more protection
0-4
5-14
15-49
50-99
100-199
>200
Office building
5-story
3-story
2-story
1-story

Sources: Department of Homeland Security; Lawrence Livermore National Laboratory; Health Physics Society

Source: http://www.nytimes.com/imagepages/2010/12/16/us/16terrorGraphic.html?ref=science



WikiLeaks cables: How US ’second line of defence’ tackles nuclear threat

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

Diplomatic dispatches reveal world of smugglers, ex-military fixers and radioactive materials found in unlikely locations

The leaked US cables reveal the constant, largely unseen, work by American diplomatic missions around the world to try to keep the atomic genie in its bottle and forestall the nightmare of a terrorist nuclear attack.

The leaked cables tell hair-raising tales of casks of uranium found in wicker baskets in Burundi, a retired Russian general offering to sell “uranium plates” in Portugal, and a radioactive Armenian car on the Georgian border.

As part of what the US government calls its “second line of defence”, it is America’s diplomatic corps who are called out in the middle of the night when radiation detectors goes off on a border crossing or smugglers turn up with fissile or radioactive materials in his pocket.

Each time that happens, and UN data suggests it has happened about 500 times in the past 15 years, it means the “first line of defence” has already been breached. The fissile material (the fuel for a nuclear warhead) or radioactive isotopes (which emit harmful radiation), have already been stolen from their source.

Three months after taking office, Barack Obama vowed to secure all the world’s vulnerable nuclear stocks within four years in a global drive to pre-empt nuclear terrorism. But a cash-strapped Congress has yet to do approve any increase in funding for the ambitious project and Obama’s deadline looks almost certain to be missed. Meanwhile, from Africa to the former Soviet Union, there are signs it may already be too late.

In June 2007, the US embassy in Burundi reported an approach by a local elder alerting the Americans to a cache of uranium in a concrete bunker over the border in the Democratic Republic of Congo (DRC). He was concerned that it would fall into the hands of “the wrong people”, specifically the Arabs who will “destroy” people with it. At the request of the sceptical Americans, he returned a few weeks later with a Congolese smuggler who said he found the material hidden at an old Belgian colonial building. He had pictures of a wicker basket with a uranium cask inside, apparently the property of the country’s Atomic Energy Commision.

There was good reason for alarm. After Mobutu Sese Seko seized power in the mid-1960s, two uranium fuel rods from a colonial-era research reactor went missing. One turned up in 1998 when the Sicilian mafia were caught in a sting operation trying to sell it for over $12m (£7.7m) to a customer in the Middle East. The other is still unaccounted for.

Another decade on, security at the Kinshasa nuclear research centre had scarcely improved. A diplomatic cable in September 2006 describes the security measures separating the reactor from the university next door.

“The fence is not lit at night, has no razorwire across the top, and is not monitored by video surveillance,” a US diplomatic team reports. “There is also no cleared buffer zone between it and the surrounding vegetation. There are numerous holes in the fence, and large gaps where the fence was missing altogether. University of Kinshasa students frequently walk through the fence to cut across [the reactor site] and subsistence farmers grow manioc on the facility next to the nuclear waste storage building.”

At the same time, there was concern over established smuggling routes shipping both uranium fuel and raw uranium ore abroad, possibly to Iran. Congo has some of the richest uranium reserves on earth, both in terms of the scale of the deposits and the purity of its ore.

It would require just a few lorry loads of Congolese ore to process and enrich enough uranium for a bomb. Both Washington and inspectors at the International Atomic Energy Agency (IAEA) have been concerned that such a black market source of high quality ore, outside IAEA controls, could be used in a covert weapons programme in Iran.

A cable from Tanzania in September 2006 passed on a tip that some of the smuggled material may be passing through the nation's capital.

"According to a senior Swiss diplomat, the shipment of uranium through Dar es Salaam is common knowledge to two Swiss shipping companies … though no one at either company would admit it in writing."

The other major front in America's "second line of defence" runs around the edge of Russia's borders, where the collapse of the Soviet Union created a black market in nuclear and radioactive material that endures two decades on.

As in Africa, the fears are based on poor security, particularly in the immediate aftermath of the Soviet implosion, when a significant amount of fissile material went missing, some of it undoubtedly stolen by former military officers and officials as a private pension plan. As in Africa, the diplomats are left with the challenging task of separating nuclear fact from fiction.

In July 2008, the embassy in Lisbon reported a "walk-in" informant with a tale of a retired Russian general who had a brick of uranium metal to sell. The informant handed over a picture of the merchandise – a lump of grey metal.

Noting that the "walk-in stated he is not on any medications and has not consulted any mental health specialists", the case is handed over to specialists, and there is no further mention of it in the cables.

More often, the post-Soviet nuclear black market has remained closer to home. An illicit trafficking database maintained by the IAEA records 500 incidents since the mid-90s, involving "the theft or loss of nuclear or other radioactive material". Of those, 15 involved high enrichment uranium (HEU) and plutonium, from which nuclear warheads are made. Most of those were in former Soviet republics or in eastern Europe.

As part of the "second line of defence" programme, the US National Nuclear Security Administration (NNSA) is helping Russia build radiation detectors on every one of the country's border crossings, about 350 sites, by the end of next year.

However, there are doubts that this expensive hi-tech approach will work. Critics point to the fact that out of 20 high profile cases where nuclear smuggling has been uncovered, radiation detectors have played a part in only one. That is partly because they are so easily triggered, there are often turned off or ignored by local officials.

A confidential cable from the US embassy in Tbilisi records an incident in August last year when a car carrying three Armenians set off a detector on the Georgian-Armenian border. The driver was waved on by customs guards, however, after he claimed to have been injected with radioactive isotopes during surgery.

The car was only searched when it set off the alarm again on the way back to Armenia. It was found to be contaminated throughout by Cesium-137, a highly radioactive isotope, which could make a devastating "dirty bomb". A cloth in the car produced the highest radiation reading, but no radioactive material was found. It appears that whatever the car was carrying, had been delivered.

Eight months later, two more Armenian smugglers crossed the same border carrying HEU, but managed to shield it from the detectors by the simple expedient of carrying it in a lead-lined cigarette box. The alarms did not sound, and instead, the two Armenians, Hrant Ohanyan and Sumbat Tonoyan, were caught in a Georgian sting operation and were sentenced last month to prison terms of 13 and 14 years respectively. As the US cables make vividly clear, their cases are the tip of the iceberg.

Performance
... the best IMS based TIC and CWA detectors in their class!

WikiLeaks: Yemen radioactive stocks «easy al-Qaeda target»

Source: http://homelandsecuritynewswire.com/wikileaks-yemen-radioactive-stocks-easy-al-qaeda-target

Yemeni official told U.S. diplomats that the lone sentry standing watch at Yemen's national atomic energy commission (NAEC) storage facility had been removed from his post, and that the facility's only closed circuit TV security camera had broken down six months previously and was never fixed; «Very little now stands between the bad guys and Yemen's nuclear material,» the official warned, in a cable dated 9 January this year sent from the Sana'a embassy to the CIA, the FBI, and the department of homeland security; when told of the Yemeni nuclear storage problem, Matthew Bunn, a Harvard University nuclear terrorism expert, said: «Holy cow. That's a big source. If dispersed by terrorists it could make a very nasty dirty bomb capable of contaminating a wide area»

Meeting of Yemen's NAEC // Source: iaea.org

A senior government official in Yemen warned U.S. diplomats that poor security at the country's main store of radioactive products could allow dangerous material to fall into the hands of terrorists, according to a leaked U.S. embassy cable.

The official told the Americans that the lone guard standing watch at Yemen's national atomic energy commission (NAEC) facility had been removed from his post and that its only closed circuit TV security camera had broken down six months previously and was never fixed.

"Very little now stands between the bad guys and Yemen's nuclear material," the official warned, in a cable dated 9 January this year sent from the Sana'a embassy to the CIA, the FBI, and the department of homeland security as well as the U.S. secretary of state in Washington and others.

Yemen, the Arab world's poorest nation, has emerged as al Qaeda's most active base, after Iraq and Afghanistan. It is home to Al Qaeda in the Arab Peninsula (AQAP), the group behind a series of attacks on western targets, including the failed airline cargo bomb plot in October and the attempt to bring down a U.S. passenger jet over Detroit on Christmas Day last year. The Nigerian-born Detroit bomber, Umar Farouk Abdulmutallab, was radicalised in Yemen, according to security sources.

The Guardian reports that the cable, classified as secret by the U.S. ambassador Stephen Seche, and sent during the immediate aftermath of the Christmas Day bomb, describes how the "worried" official implored the U.S. to help convince the Yemen government "to remove all materials from the country until they can be better secured, or immediately improve security measures at the NAEC facility."

The cable revealed that the facility holds large quantities of radioactive material used by hospitals, local universities for agricultural research and in oilfields. The international community fears radioactive isotopes could be used to make a dirty bomb — a device combining simple explosives with radioactive materials, which it would disperse over a wide area.

The isotopes are not explosive themselves, unlike nuclear material such as uranium. Although unlikely to kill a large number of people, such a device could cause tremendous damage and disruption by creating large no-go areas contaminated by radioactivity.

International experts said today the lack of security at the Yemen facility would be a "high priority" for the U.S. government. Told of the cable's revelation of the type of materials and the amount stored in Yemen's NAEC facility, MatthewBunn, a former White House science adviser who specializes in nuclear threat and terrorism, said: "Holy cow. That's a big source. If dispersed by terrorists it could make a very nasty dirty bomb capable of contaminating a wide area," said Bunn, an associate professor at Harvard University's John F Kennedy school of government, who compiles an annual assessment of the nuclear terrorism threat titled Securing the Bomb.

Such a bomb would be "enough to make a mess that would cost tens of billions of dollars in cleanup costs and economic disruption, with all sorts of controversy over how clean is clean, how will people go back there," he said.

It's the type of thing that the U.S. program have been working on securing all over the world. The global threat reduction initiative (GTRI) in the department of energy has two missions: one, to get rid of enriched uranium and two, to improve security on radioactive facilities so that dirty bombs cannot be used.

The location in Yemen is obviously of particular concern given terrorism, given al Qaeda in the Arab Peninsula headquartered there, also the spotty effectiveness of the government.

I would think it would be a high priority to do something about it.

While a dirty bomb has never been detonated, terrorists have been accused of plotting such attacks.

A Briton, Dhiren Barot, admitted plotting to build a radioactive bomb in the United Kingdom and was convicted in 2006.

The leaked U.S. cable revealed that, in the days following the official's warning over security and probably as a result of US diplomatic pressure, the radioactive material was moved to a more secure facility and the remainder of it was likely to follow.

In a section of the cable titled Comment, it read: "Post will continue to push senior ROYG (Republic of Yemen Government) officials to increase security at all national atomic energy commission facilities and provide us with a detailed accounting of all radioactive materials in the country."

A spokesman for the US state department said: "We decline to comment on any cable. A team from the U.S. department of energy visited Yemen in February and continues to work with the government on security upgrades at relevant sites as part of its global threat reduction initiative."

The U.S. national nuclear security administration declined to comment on the cable or any action taken as a result of it.

A spokesman added: "I am not going to comment on upgrades to any specific sites. I can say that we have programs to co-operate with more than 100 countries around the world to secure vulnerable nuclear material, improve security at nuclear facilities, and prevent nuclear smuggling. We are working day and night to prevent terrorists from acquiring nuclear material, no matter the source."

Geologists develop way to monitor covert nuclear tests in the Middle East

Source: http://homelandsecuritynewswire.com/geologists-develop-way-monitor-covert-nuclear-tests-middle-east

Not only is it difficult to identify exactly where an explosion takes place, but it is especially challenging to differentiate the seismic waves generated by nuclear explosions from those generated by earthquakes, volcanic activity, and mine collapses; geologists develop improved seismic model for monitoring nuclear explosions in Middle East

Geologists from the University of Rhode Island and Princeton University, in collaboration with Lawrence Livermore National Laboratory, have taken an important step toward helping the United States government monitor nuclear explosions by improving a 3-dimensional model originally developed at Harvard University. The improvements make the model more accurate at detecting the location, source, and depth of seismic activity.

The results of their research were presented last week at a meeting of the American Geophysical Union in San Francisco. The U.S. National Nuclear Security Administration uses numerous seismic models in its efforts to monitor the globe for underground nuclear explosions detonated by nations that seek to keep their nuclear activities undetected. Not only is it difficult to identify exactly where an explosion takes place, but it is especially challenging to differentiate the seismic waves generated by nuclear explosions from those generated by earthquakes, volcanic activity, and mine collapses.

"The goal is to build a model of the Earth that will locate seismic events and characterize those events precisely while reducing potential errors," said Brian Savage, URI assistant professor of geosciences.

The model spans the politically sensitive region from Turkey to India, including Iran, Iraq, and Afghanistan, a region Savage describes as "tectonically complex."

Savage and his colleagues analyzed data from 200 earthquakes collected by 150 seismic stations in the region between 1990 and 2007. They compared the data with that from simulated earthquakes to identify deficiencies in the model, then propagated the simulated earthquakes in reverse to determine where to improve and update the model.

Different types of seismic waves travel in different ways and at different speeds. P-waves, for instance, are the first waves recorded from an earthquake or explosion, and they behave similar to sound waves. S-waves are secondary waves that travel in a snake-like side-to-side fashion. Surface waves are a combination of the two traveling much slower with much larger amplitude.

"Depending on the material the waves travel through, it may slow down or speed up the waves," said Savage, who notes that the model requires a great deal of computer power to run. "So when you look at the relative timing of the waves, you can tell what the material is that it's traveling through."

The improvements the researchers made to the model focused on long period surface waves and identifying the magnitude of a seismic event. "The amplitude ratios of different wave types is a key factor in discriminating whether an event is manmade or not," Savage said. The improved model is expected to be complete by next summer. The research was funded by he National Nuclear Security Administration and the Air Force Research Laboratory.

A Dangerous Gap in Our Defenses?

An EMP attack is a terrible threat, but countering it is affordable.

Source: http://www.nationalreview.com/articles/255192/dangerous-gap-our-defenses-henry-f-cooper-brrobert-l-pfaltzgraff-jr

For several days in early November, a series of U.S. government agencies were either unable or unwilling to explain what had produced a vapor trail that had illuminated the Southern California skies. Public speculation abounded, first that it was a missile, then that it was in fact the condensation trail (contrail) of a plane. Controversy continues in the blogosphere and elsewhere.

The absence of a cogent official explanation reveals a dangerous gap in our defenses, specifically in our warning systems. Our surveillance systems should be able to distinguish a missile from an airplane instantaneously. If the source of the vapor trail had been a short-range ballistic missile launched from a freighter, tanker, or container ship, or even a small vessel off our shores, we should have been able to detect it unambiguously and shoot it down quickly. Failure to do so could have produced long-lasting local and global consequences.

The 2004 Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack observed that a single nuclear weapon exploded at high altitude above the United States will interact with the Earth's atmosphere, ionosphere, and magnetic field and can produce a damaging electromagnetic pulse over hundreds of square miles. This could shut down, for an indefinite period, telecommunications and electrical-power grids, as well as the electronics-dependent transportation systems that support the "just-in-time" marketing, manufacturing, and delivery of essentially all commodities upon which we are dependent. It could cut off water and food supplies to urban areas and create chaos that would return the United States to 19th-century life, but without the life support then provided by an indigenous agricultural society. It could also hobble banking and related business transactions, which in turn could extend the catastrophic effects into the global economy. Disabling even one of our critical infrastructure elements would have severe consequences for others — effects from which advanced, technologically interdependent societies might not easily recover.

This threat is not merely hypothetical. Several years ago, Iran tested a short-range ballistic missile in a way that indicated an interest in developing an EMP capability. Even terrorists might purchase such missiles, possibly armed with nuclear weapons. Furthermore, recent reports that Iran has agreed to install ballistic missiles in Venezuela suggest that we could face a threat via future pathways across the Caribbean. This could become a modern version of the Cuban Missile Crisis. Yet no national strategy addresses this threat or underwrites a serious program to counter its effects — though such a capability would be possible as an inexpensive adjunct to existing and planned missile-defense programs.

Presidents George W. Bush and Barack Obama both have placed a top priority on preventing the smuggling of nuclear weapons to the United States. Such a program must be able to counter the maritime smuggling of nuclear weapons, including the identification and interdiction of a ship carrying short- or medium-range nuclear-armed ballistic missiles. And if such a ship escapes detection or interdiction before it approaches U.S. coasts, effective defenses could intercept a launched nuclear-armed missile in its ascent phase just after launch and before it can detonate a nuclear warhead.

Fortunately, the dangerous gap in our defenses that may have been revealed by the vapor trail in early November can be filled by technologies that are already available or presently under development. This includes countering a would-be EMP attacker, who might be deterred by an integrated U.S. system that: 1) identifies a ship carrying one or more nuclear-armed ballistic missiles and interdicts it before it reaches striking distance of the United States; 2) failing that, intercepts the attacking missile before its EMP-producing nuclear warhead is detonated; and 3) failing that, reduces casualties and provides for critical infrastructure reconstitution, including hardening to minimize EMP effects.

Such an integrated system would contain three components fashioned from ongoing missile-defense programs — Aegis ballistic-missile-defense (BMD) ships, Aegis Ashore ground-based interceptors, and unmanned aerial vehicle (UAV) capabilities. An effective command-and-control system, together with intelligence and early warning, is vitally important in preventing the smuggling of nuclear weapons into the United States, as well as for timely missile-defense operations.

Interceptors on even a single U.S. Navy Aegis cruiser or destroyer operating in a region near Norfolk, Va., could defend a large portion of the eastern seaboard. Additional ships could extend and reinforce the protective shield from New England to Florida. The five Aegis BMD-capable ships now stationed in the Atlantic will grow to 18 by 2015, and a few of these could provide an anti-EMP mis sile defense for the entire east coast, while still performing their other day-to-day operations. A similar number are already deployed in the Pacific, and several of these could defend Hawaii, Alaska, and the west coast. A land-based version of the Navy's Standard Missile-3 (SM-3), deployed on military bases along the Gulf coast, could defend those who live there against an EMP attack from Venezuela or the Caribbean.

Already-deployed SM-3s can begin to counter the EMP threat almost immediately, and planned higher-velocity SM-3 improvements, along with an increase in deployed numbers, will make an EMP attack even less likely to succeed. Similarly, a land-based variant of the current SM-3 could be rapidly deployed and improved. The current Aegis Ashore program plans initial overseas land-based deployments beginning in 2015 — and improvements following in the next five years. Obviously, this same capability could be deployed as part of an anti-EMP capability to protect the United States, particularly in the Gulf-coast region, where Aegis ships seldom operate.

To help fill the November vapor-trail mystery gap, a dedicated UAV-sensor system could provide timely tracking information, which is essential to initiating defensive operations somewhere between seconds and a very few minutes after a threatening missile is launched from a ship off our coasts. Such UAVs could also carry interceptors as an additional defensive layer to Aegis. UAV-borne sensors and weapons have already demonstrated impressive capabilities in Afghanistan and Iraq, and appropriate versions could be placed in "orbits" off the U.S. coast to identify ballistic-missile launch preparations, provide warning if a ballistic missile is launched from an offshore ship, and intercept it in its boost or ascent phase.

America's current state of essentially complete vulnerability to the EMP threat is unacceptable, especially since relatively inexpensive steps can be taken now to build missile-defense systems that would begin to counter this 21st-century threat. Existing, already-funded programs will improve possible near-term capabilities, which can begin initial operations by 2015. The confusion over what produced the vapor trail off the California coast in early November, along with the potential threat from Venezuela, should inspire action to fill a gap that, if unaddressed, could have catastrophic consequences for our security.

Henry F. Cooper was chief U.S. negotiator at the Geneva defense and space talks with the Soviet Union (1985–1989) and director of Strategic Defense Initiative (1990–1993). Robert L. Pfaltzgraff Jr. is president of the Institute for Foreign Policy Analysis, Shelby Cullom Davis Professor of International Security Studies at the Fletcher School, Tufts University, and co-chairman of the Independent Working Group.

New technology speeds cleanup of nuclear contaminated sites

Source: http://homelandsecuritynewswire.com/new-technology-speeds-cleanup-nuclear-contaminated-sites

Hundreds of millions of dollars are spent on cleanup of some major sites contaminated by radioactivity, primarily from the historic production of nuclear weapons during and after the Second World War; Oregon State University researchers have invented a new type of radiation detection and measurement device that will be particularly useful for cleanup of sites with radioactive contamination, making the process faster, more accurate and less expensive. Members of the engineering faculty at Oregon State University have invented a new type of radiation detection and measurement device that will be particularly useful for cleanup of sites with radioactive contamination, making the process faster, more accurate and less expensive. A patent has been granted on this new type of radiation spectrometer, and the first production of devices will begin soon. The advance has also led to creation of a Corvallis-based spin-off company, Avicenna Instruments, based on the

OSU research. The market for these instruments may ultimately be global, and thousands of them could be built, researchers say. Hundreds of millions of dollars are spent on cleanup of some major sites contaminated by radioactivity, primarily from the historic production of nuclear weapons during and after the Second World War. These include the Hanford site in Washington, Savannah River site in South Carolina, and Oak Ridge National Laboratory in Tennessee. “Unlike other detectors, this spectrometer is more efficient, and able to measure and quantify both gamma and beta radiation at the same time,” said David Hamby, an OSU professor of health physics. “Before this two different types of detectors and other chemical tests were needed in a time-consuming process.” “This system will be able to provide accurate results in 15 minutes that previously might have taken half a day,” Hamby said. “That saves steps, time and money.” The spectrometer, developed over ten years by Hamby and Abi Farsoni, an assistant professor in the College of Engineering, can quickly tell the type and amount of radionuclides that are present in something like a soil sample — contaminants such as cesium 137 or strontium 90 — that were produced from reactor operations. And it can distinguish between gamma rays and beta particles, which is necessary to determine the level of contamination. “Cleaning up radioactive contamination is something we can do, but the process is costly, and often the question when working in the field is how clean is clean enough,” Hamby said. “At some point the remaining level of radioactivity is not a concern. So we need the ability to do frequent and accurate testing to protect the environment while also controlling costs.” This system should allow that, Hamby said, and may eventually be used in monitoring processes in the nuclear energy industry, or possibly medical applications in the use of radioactive tracers. The OSU College of Engineering has contracted with Ludlum Instruments, a Sweetwater, Texas, manufacturer, to produce the first instruments, and the OSU Office of Technology Transfer is seeking a licensee for commercial development. The electronic systems for the spectrometers will be produced in Oregon by Avicenna Instruments, the researchers said.

Privacy pants for airport security

Source: http://homelandsecuritynewswire.com/privacy-pants-airport-security

«Privacy pants» would allow airport security personnel to do their job while keeping passengers’ privacy and dignity intact. The numbers are not yet in, but one item which enjoyed brisk sales this holiday season is what should be described as “privacy pants.” The designers claim that the pants would allow airport security personnel to do their job while keeping passengers’ privacy and dignity intact. The folks over at Rocky Flats Gear have designed a special fig leaf underwear that protects travelers from the gaze of TSA. So what makes these panties so special? They are laced with tungsten and other metals to block the X-rays from the body scanners. It gets you right through the metal detectors with no hassle. They even make bras for women who are self-conscious about flashing their boobies. The only drawback, besides the fact that it looks like a pair of grannie underwear with a giant fig leaf slapped on, chances are TSA could get suspicious about what is behind that giant fig leaf. Which means? One-way ticket to a hand down your pants and getting groped.

Comfortable radiation blocking brief with radiation shield

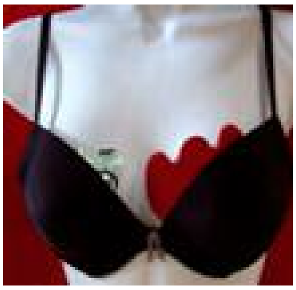
- Wear every day to block natural and man-made radiation.
- Use for extended air travel to protect from whole body scanners.
- Protect from increased radiation while flying or living at high altitudes.

- Blocks/diminish Alpha and Beta radiation.
- Blocks/diminish T-Wave/Tera hertz radiation from remote strip cameras.
- Blocks/diminish X-ray/gamma radiation from back scatter x-ray machines.
- Insures privacy of medical and body scanner images
- Uni-Sex Brief Gray Green shield
- Size 28-30» 71-76 cm small to 36-38» 91-96 cm large
- Care:Wash Cold chlorine free bleach
- Weight:2.5 Oz(0.075kg)

Velvet Privacy bra insert x-ray shield

Comfortable radiation blocking velvet bra insert with patent pending radiation shield, sizes small to large. Protect your sensitive tissues and privacy from remote strip search cameras (mm-wave) and dangerous x-ray airport scanners. Product is warn velvet side toward the body shield toward the source, fabric tape included for affixing to undergarment if desired. Just slip in and your protected, so comfortable you not know you have it on. Also doubles as reusable a nipple concealer.

- Wear every day to block natural and man-made radiation
- Use extended air travel to protect from whole body scanners



- Protect from increased radiation while flying at high altitudes
- Blocks/diminish-Alpha and Beta radiation
- Blocks/diminish T-Wave/Terahertz radiation (remote strip cameras)
- Blocks/diminish X-ray radiation - (back scatter x-ray)
- Insures privacy of medical and body scanner images
- Use over and over again.
- Clean with a damp cloth air dry
- Light weight 2.5 Oz (0.075 kg)
- Proudly Made in USA

Cement prison for old radioactive waste

Source: http://homelandsecuritynewswire.com/cement-prison-old-radioactive-waste?page=0,0

The cold war may be over, but its radioactive legacy is not; between 1950 and 1990, nuclear weapons materials production and processing at several federal facilities generated billions of gallons of water contaminated with radioactive byproducts; researchers at Idaho National Laboratory test an inexpensive method to sequester strontium-90 where it lies. The researchers can coax underground microbes to form calcite, a white mineral form of calcium carbonate and the main ingredient in cement. Calcite should be able to trap strontium-90 until long after it has decayed into harmless zirconium

The cold war ended long ago, but its radioactive legacy still lingers in the water and soil of the western United States. Between 1950 and 1990, nuclear weapons materials production and processing at several federal facilities generated billions of gallons of water contaminated with radioactive byproducts.

These sites have since updated their waste treatment practices to keep new contamination from entering the water supply. Some old contamination, though, is still present.

Though public drinking water near Department of Energy sites in Washington and Idaho does not contain strontium-90 at concentrations above the EPA's safe drinking water limit, some monitoring wells at the sites do. At least some contamination in the monitoring wells is strontium-90 that slowly leached out of the soil.

"It's not something you want to leave to wash out," says James Henriksen, an INL microbiologist.

Researchers at Idaho National Laboratory, the Center for Advanced Energy Studies, and other national labs and universities are working together to test an inexpensive method to sequester strontium-90 where it lies. The researchers can coax underground microbes to form calcite, a white mineral form of calcium carbonate and the main ingredient in cement. Calcite should be able to trap strontium-90 until long after it has decayed into harmless zirconium. Strontium-90 has a nearly 30-year half-life, which means that a sample of the stuff will take around 300 years to decay more or less completely.

"Three hundred years is nothing for calcite," Henriksen says.

When people consume strontium-90 in contaminated food or drinking water, the radioactive isotope can replace some of the calcium in living bone.

The bone-bound strontium-90 acts as a long-term source of damaging radiation that can spawn deadly cancers of blood, bone and skin.

Cleaning strontium-90 out of the ground and water hasn't been easy. "There have been heroic efforts that cost enormous amounts of money," Henriksen says. Some of the most contaminated dirt was excavated, but digging up all the contamination would be astronomically expensive. A project to pump out and treat contaminated groundwater only removed a tenth as much strontium-90 as did natural decay during the same period.

Pumping the groundwater was not effective because most of the contamination was stuck on solid surfaces underground, says INL environmental researcher Yoshiko Fujita. Remove the strontium-90 from the water, and more leaches off the solids to replace it.

So instead of trying to strip strontium-90 out of the ground, Fujita, Henriksen and their colleagues are trying to coax microbes to set a trap for it in the ground. The researchers are betting that the same chemical similarity that draws strontium-90 to bone will bind it into a microbe-made calcite "prison."

Calcium is an essential ingredient for calcite. Fortunately, there is no shortage of calcium in the ground at most sites with old radioactive contamination.

Much of the groundwater in the arid American West contains so much dissolved calcium that crusty deposits of the mineral often clog water pipes near the DOE's Washington and Idaho sites.

Getting that calcium to turn into calcite on location and on demand requires molasses, urea and a little help from microbes. First, the microbes chow down on molasses and multiply, swelling their numbers by tenfold or more. A second course of urea, a cheap nitrogen fertilizer, prompts part of the expanded microbe population to generate calcite. They do so by using a protein called urease, to convert urea and water to carbonate and ammonium.

The carbonate then joins with calcium in the ground and groundwater to form calcite.

Ammonium, on the other hand, performs the critical function of scrubbing strontium-90 ions off solid surfaces. The contaminant tends to cling to dirt and rock and resists efforts to extract it from soil. But ammonium, like strontium-90, carries a positive charge, which helps it boot strontium-90 off the surfaces of solids.

The research team has screened the Washington and Idaho sites to see if microbially generated calcite might offer a solution at contaminated sites in the West. Fujita and her colleagues describe the results of testing samples from the Washington site in a September 2010 paper in the journal Environmental Science & Technology. In addition to containing enough calcium and the right chemical conditions to support long-lived calcite formation, the water and soil at that site contained plenty of bacteria that could make urease and calcite — as many as several thousand such microbes in a drop of water or a gram of sediment.

Earlier studies of molasses and urea injections into the groundwater near INL showed that the microbes there will make calcite, too. Indeed, many places around the world contain all the ingredients to make microbial calcite. For example, urea and microbes have been used to make sustainable bricks from sand in Abu Dhabi, and have been proposed as a way to repair stone surfaces in Europe.

Before researchers can use the technique to clean up contamination in the ground, they need to show that they can control and predict microbial calcite formation. That iss easy enough to do in a laboratory beaker, but reining in bacteria and chemical reactions in a complex underground environment has posed many practical and scientific challenges.

For instance, in one of their first field experiments, Fujita and her colleagues generated so much calcite that they clogged their injection well and burned out a pump. “What a success!” Fujita recalls collaborator and University of Idaho geochemist Robert Smith saying upon hearing the news. “He was only half-joking,” Fujita says. The clog made it difficult for the researchers to measure how much calcite they’d made or how much bacterial growth they had stimulated.

For their next set of field experiments, the team upgraded to multiple wells and moved to the Vadose Zone Research Park at the INL desert Site.

Having more than one well meant they could create their own water flow and study how far they could get the injected urea to go. They had trouble, however, getting the urea and molasses injections to go the way they wanted.

Henriksen describes the problem by sketching an underground stream taking a tortuous route through hidden gravel pits and around impermeable layers of basalt and clay before finally draining into the Snake River Plain Aquifer. “It’s really complicated and dynamic,” Henriksen says. “You can’t just reach down there and make the water go where you want.”

In addition, the amount and rates of water moving through the ground at the park can change. Fujita and colleagues spent their first year at the research park studying underground water movement. The team showed up the next year with many carefully planned experiments, only to find that the park water conditions had drastically changed. One well was even completely dry. The experiments had to be scrapped.

Fujita, Smith, and Henriksen have not yet given up on microbial calcite. They took care to locate their latest experiment at a well-studied DOE research site at an old uranium ore processing facility in Rifle, Colorado. Henriksen and his colleagues are evaluating the effect of their molasses and urea injections on the local microbe community and working with hydrologists to help them understand Rifle’s underground water dynamics. The INL researchers couldn’t dig up enough of the ground to look directly at how much calcite they’d generated and where, so they enlisted geophysicists to help them detect those things remotely with ground radar and by measuring any effects the underground reactions might have had on the ground’s capacity to conduct electric current.

The forthcoming results of the Rifle experiment should get INL researchers closer to being able to predict the results of future efforts to stimulate microbial calcite formation. The researchers would like to expand their knowledge of the process with more and larger scale tests at contaminated locations, such as a pilot study at the Washington site, Fujita says.

Despite the frustration of thwarted experiments, Henriksen remains enchanted by the complexity of studying and manipulating microbes in the environment.

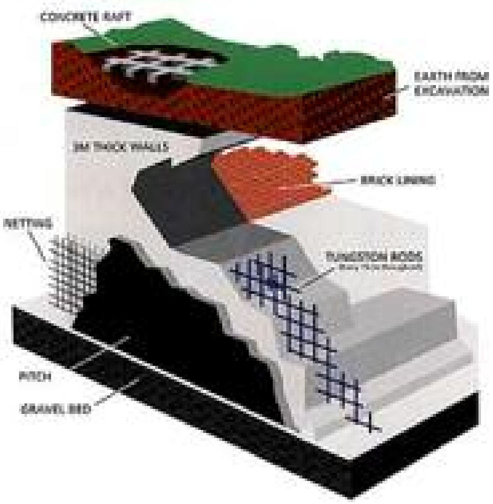
“Most people don’t think about the bacteria everywhere around them or about utilizing the amazing capabilities bacteria have,” Henriksen says. “They can do a lot of things we can’t. Now we have the tools to work with them.”

End-of-World’ Threat Stirs Interest in Scottish Nuclear Bunker

Source:http://www.bloomberg.com/news/2011-01-27/-end-of-world-threat-stirs-interest-in-scottish-nuclear-bunker.html

A nuclear bunker in Scotland built as the Cold War thawed is drawing interest from a U.S.-based group worried about another possible threat: doomsday. The Vivos Group, a Del Mar, California-based company that provides protection against what it calls “end-of-the-world scenarios,” is considering buying the two-story bunker constructed for the U.K. gov

ernment in 1990 near Comrie, 67 miles (108 kilometers) northwest of Edinburgh. “We have been evaluating it, but it has issues,” Robert Vicino, the founder of Vivos, said in a telephone interview yesterday while travelling in Arizona. “The biggest one is altitude. It is also well known, so there would be diminished secrecy. But we haven’t ruled it out.” Large nuclear bunkers that are no longer needed by governments have been converted into a variety of uses. One in Switzerland has been turned into a hotel (picture: Null Stern Hotel), while others have become wine cellars, museums or data-storage centers. One in Berlin now houses a private art collection. The former facility in Scotland, which was designed to shelter 150 politicians, the emergency services and military chiefs in the event of a nuclear attack, officially goes on sale on Feb. 1 with a guide price of 400,000 pounds ($635,000). “We are in talks with a couple of possible international bidders,” Andrew Black, the realtor at Carter Jonas who is selling the property, said in an interview from Shrewsbury, central England. “There is a lot of chatter around the Internet about the world coming to an end next year.”



Headquarters

The windowless bunker, which has one floor above ground and one below, has 26,000 square feet (2,400 square meters) of space, according to the sale documents. It was designed to provide an underground regional government headquarters and also included broadcasting facilities. It was built at Cultybraggan, a former prisoner-of-war camp that lies in a valley below the Trossach mountains. The 90-acre (36-hectare) camp was bought from the U.K. Ministry of Defence by the local community in 2007 for 350,000 pounds. Any development of the site will require approval from planning officials, said Mary Willis, a spokeswoman for Perth and Kinross Council, the local municipality. The Cultybraggan bunker is 66 miles west of its predecessor near the coast in eastern Scotland. That structure, which was built in the 1950s, has since been turned into a museum with a store and restaurant. Visitors access it through a farmhouse leading to a 150-meter tunnel and three-tons of sealable blast- proof doors, according to its website.

Preparing for Worst

Vicino’s group is building shelters in the U.S. and elsewhere for its 10,000 members around the world who believe the world may soon be the victim of a cataclysmic event ei-

ther man-made or from natural causes. One opening this year at an unidentified location in central Europe will house 2,000 people paying 25,000 euros ($34,000) for a year's protection including food, Vicino said. Activity from the current solar cycle will peak in about June next year and last for around 12 months, Vicino said. Debris from the sun would wipe out most of civilization and could create a tsunami wave that would cover the U.K., he said.

Medical isotopes could be made without a nuclear reactor

Source: http://homelandsecuritynewswire.com/medical-isotopes-could-be-made-without-nuclear-reactor

Canadian researchers are racing to perfect a safe, clean, inexpensive, and reliable method for making isotopes used in medical-imaging and diagnostic procedures — a method which would not require a nuclear reactor and could, therefore, eliminate future shortages of technetium-99m, the most widely used medical isotope today; what is more, the new method generates virtually no radioactive waste materials that must be stored indefinitely. Canadian researchers are racing to perfect a safe, clean, inexpensive, and reliable method for making isotopes used in medical-imaging and diagnostic procedures. The new method does not require a nuclear reactor and could therefore eliminate future shortages of technetium-99m — the most widely used medical isotope today. Until recently, the National Research Universal (NRU) reactor at Chalk River, Ontario, produced almost 50 percent of the world's supply of medical isotopes. Then in May 2009, the NRU was shut down for repairs. This halt in operations, combined with several delays in its restart, contributed to a global isotopes shortage. While the reactor has been back in operation since August 2010, it is scheduled for closure by 2016. The Engineer reports that last June the Government of Canada announced a $35 million program to promote research into alternative methods of producing medical isotopes. Backed by NRC and other collaborators, the Canadian Light Source submitted one of four successful proposals under this research program to explore the technical and economic feasibility of using an electron linear accelerator to produce molybdenum-99 (Mo-99) — the "parent isotope" of technetium-99m (Tc-99m).

Its proposal builds on research by the Idaho National Laboratory and a suggestion made by Ottawa-based Mevex. Scientists at the NRC Institute for National Measurement Standards (NRC-INMS) have already tested every step of the linear accelerator method. The research partners expect it could ultimately make enough isotopes to supply all of Canada's requirements. According to Dr. Carl Ross, who leads the NRC-INMS team, the new method does not pose any security or nuclear proliferation concerns because, unlike a nuclear reactor, it requires no weapons-grade uranium. What is more, it generates virtually no radioactive waste materials that must be stored indefinitely. "Using a linear accelerator, you essentially produce only the isotope that you want, so there is negligible waste," he said. "The linear accelerator method is virtually guaranteed to replace the nuclear-reactor production method," added Dr. Ross. "The physics are well established. The chemistry of separation is well known. So I don't really see any impediment to it being successful." In the new method, a high-energy linear accelerator bombards coin-sized discs of the stable isotope molybdenum-100 with X-rays to produce radioactive Mo-99. Mo-99, with a half-life of 66 hours, soon decays into the desired Tc-99m. Tc-99m can then be separated from Mo-99 using technology developed by U.S.- based Northstar Medical Radioisotopes. Over the next two years, NRC will work with its collaborators to develop a manufacturing process. A demonstration facility will be constructed at the Canadian Light Source in Saskatoon to prove that a high-power electron accelerator can produce a significant fraction of the medical isotopes required by nuclear pharmacies across the country.

WikiLeaks: 'Al-Qaida on Brink of Using Nuclear Bomb'

Source:http://nation.foxnews.com/dirty-bomb/2011/02/01/wikileaks-al-qaida-brink-using-nuclear-bomb#ixzz1Cnkfzxmg

Al-Qaida is on the verge of producing radioactive weapons after sourcing nuclear material and recruiting rogue scientists to build «dirty» bombs, according to leaked diplomatic documents. A leading atomic regulator has privately warned that the world stands on the brink of a «nuclear 9/11». Security briefings suggest that jihadi groups are also close to producing «workable and efficient» biological and chemical weapons that could kill thousands if unleashed in attacks on the West. Thousands of classified American cables obtained by the WikiLeaks website and passed to The Daily Telegraph detail the international struggle to stop the spread of weapons-grade nuclear, chemical and biological material around the globe.

China's nuclear power expansion is based on thorium

Source: http://homelandsecuritynewswire.com/chinas-nuclear-power-expansion-based-thorium

The thorium fuel cycles produce almost no plutonium, and fewer higher-isotope residuals; thorium is much more abundant than uranium, and the reduced plutonium output eases proliferation concerns; the energy output per ton is also attractive; China has committed itself to establishing an entirely new nuclear energy program using thorium as a fuel; six heavy-water thorium reactors are planned in India, which has the world's largest thorium deposits.

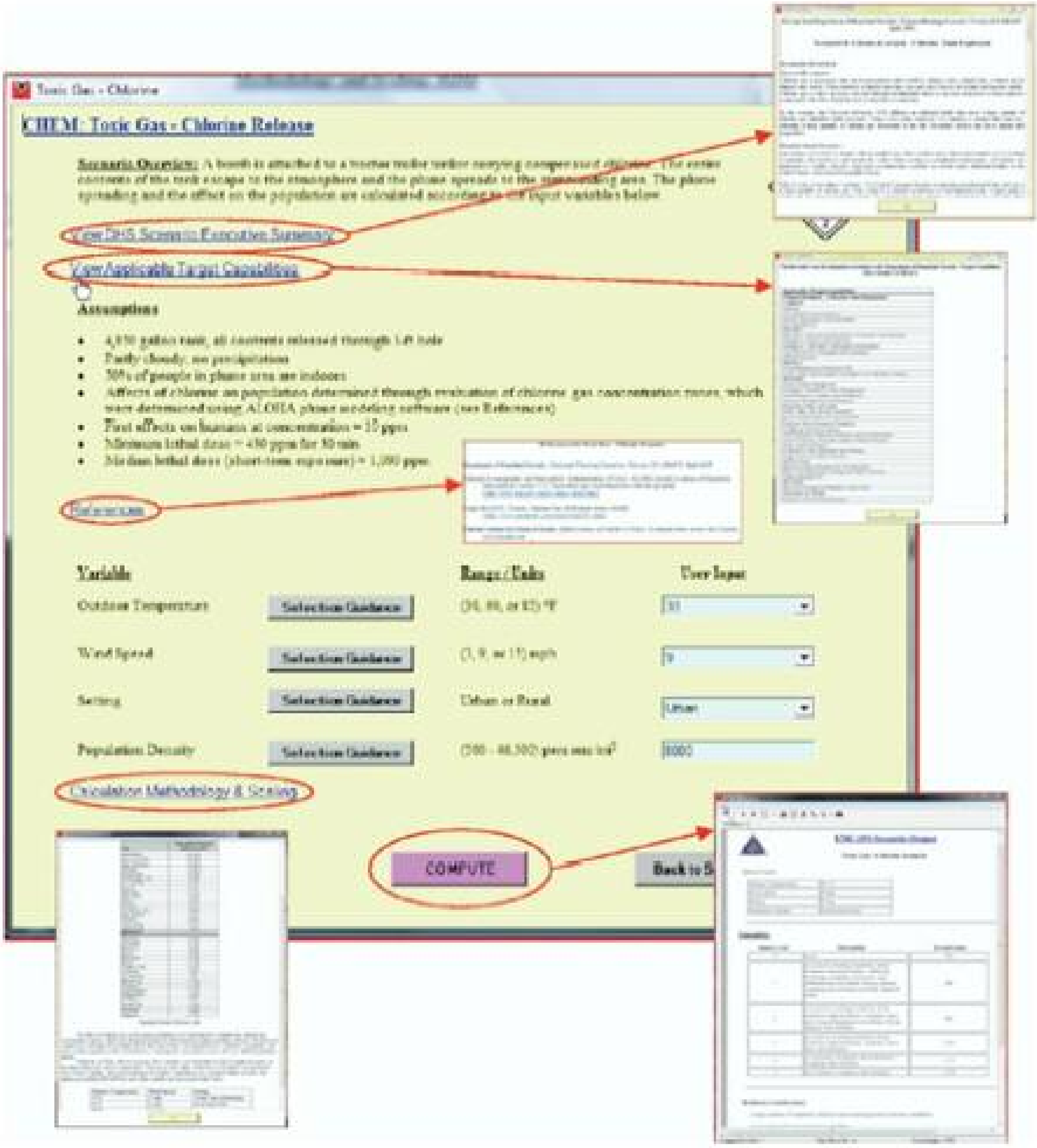
China has committed itself to establishing an entirely new nuclear energy program using thorium as a fuel, within twenty years. The LFTR (Liquid Fluoride Thorium Reactor) is a 4G reactor that uses liquid salt as both fuel and coolant. China uses the more general term TMSR (Thorium Molten-Salt Reactor). The thorium fuel cycles produce almost no plutonium, and fewer higher-isotope residuals, the long-lived minor actinides. Thorium is much more abundant than uranium, and the reduced plutonium output eases proliferation concerns. The energy output per ton is

China's Fangjiashen nuclear power plant during construction // Source: energytribune.com also attractive, even though thorium is not itself a fissile material. Thorium reactors are also safer, with the fuel contained in a low-pressure reactor vessel, which means smaller (sub-500GW) reactors may be worth building. The first Molten-Salt Breeder prototype was built at Oak Ridge in 1950, with an operational reactor running from 1965 to 1969. Six heavy-water thorium reactors are planned in India, which has the world's largest thorium deposits. The Register reports that the design has also had its champions in Europe, but planning restrictions and a continent-wide policy preoccupation with conservation and renewables have seen little commercial action. This might change. A private company founded by Kazuo Furukawa, designer of the Fuju reactor, called International Thorium Energy & Molten-Salt Technology Inc. (iThEMS) aims to produce a small (10KW) reactor within five years. Furukawa is aiming for a retail price of $0.11 per kWh. Just to put that into perspective, the U.K.'s feed-in tariff ranges from 34.5p/kWh for a small wind turbine to 41.3p/kWh for a retro-fitted solar installation, making LFTR attractive.

Disaster Preparedness Tool From Homeland Security's Science And Technology Directorate Calculates Casualty Estimates

Source: http://www.medicalnewstoday.com/articles/214789.php

In the aftermath of a dirty bomb, hundreds or even thousands of victims could require medical attention. First responders conduct extensive training to prepare for such a cataclysmic event, but planning is difficult without a solid estimate of how many people could be injured. The toll would be influenced by a number of variables. For example, the toll from a dirty bomb detonation would depend upon the population density at the explosion site and the components used in the explosive. To plan effective training scenarios and tabletop exercises, first responders need a simple way to estimate realistic casualty figures as a result of catastrophic events. To provide first responders with this ability, the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) continues to support the development of the Electronic Mass Casualty Assessment and Planning Scenarios (EMCAPS) software. Sponsored by the National Center for the Study of Preparedness & Catastrophic Event Response (PACER), a DHS Center of Excellence, an updated version of EMCAPS is scheduled for release in 2011. The state of Maryland provided some startup funding for the software program. Johns Hopkins University Office of Critical Event Preparedness and Response (CEPAR) and the Johns Hopkins University Applied Physics Laboratory are responsible for the software's development. The current version was first released in 2005 and is available as a free download here. The program allows first responders to customize nine scenarios for their geographic area and then estimate the number of likely casualties. Researchers used high-consequence threat scenarios identified by DHS to incorporate into the software program. These include a pandemic flu outbreak, a chlorine gas release, a truck bomb, and inhalation anthrax exposure. The scenarios can be customized for different conditions. Thousands of people have accessed the software, according to Heidi R. Whiteree, DHS S&T program manager. «The advantage of this [program] is it is so easily downloadable, and you can manipulate the variables to suit your own jurisdiction,» said Whiteree. For example, in the case of a dirty bomb scenario, first responders can customize information about the explosive and detonation site to match their own locations. One way to customize a scenario is to select the population density of the affected area. While a crowded New York City sidewalk might have one person every 25 square feet, a small town's pedestrian area might contain one person every 225 square feet. A guide in the software assists users in selecting the population density that most closely mirrors the local community. James Scheulen, chief administrative officer for the



Toxic Gas - Chlorine

CHEM: Toxic Gas - Chlorine Release

Scenario Overview: A bomb is attached to a tractor trailer tanker carrying compressed chlorine. The entire contents of the tank escape to the atmosphere and the plume spreads to the surrounding area. The plume spreading and the effect on the population are calculated according to the input variables below.

View DHS Scenario Executive Summary

View Applicable Target Capabilities

Assumptions

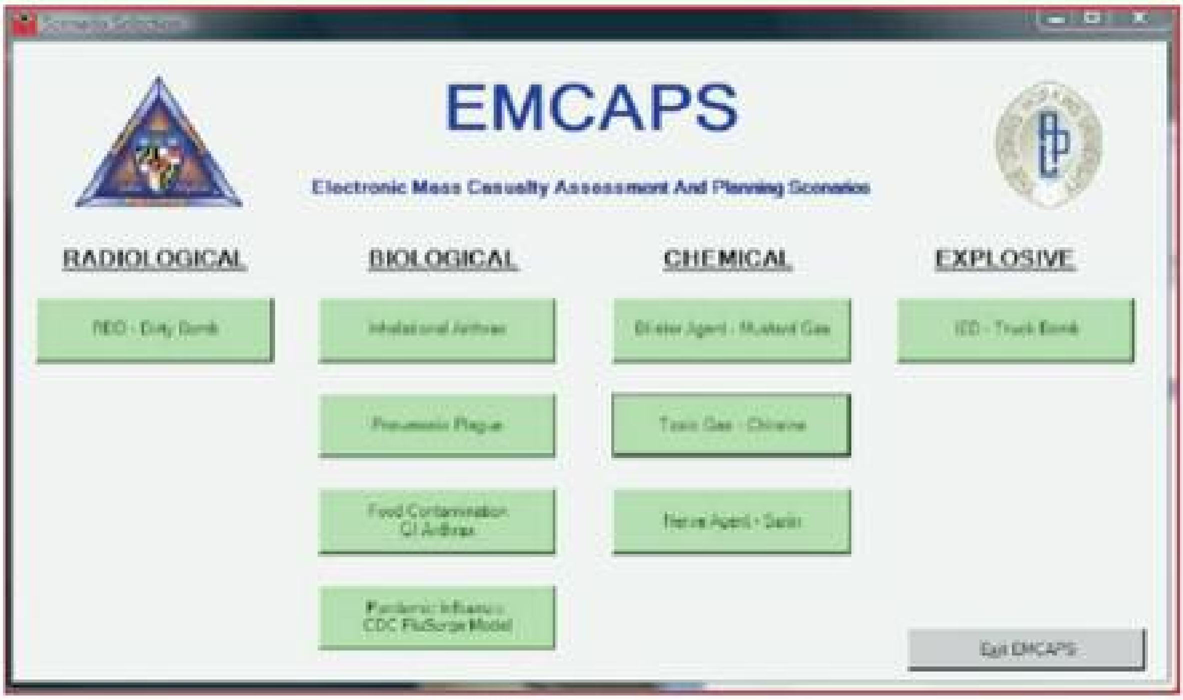
- 4,950 gallon tank, all contents released through 1.6 hole
- Partly cloudy, no precipitation
- 50% of people in plume area are indoors
- Affects of chlorine on population determined through evaluation of chlorine gas concentration zones, which were determined using ALOHA plume modeling software (see References)
- First effects on humans at concentration = 15 ppm
- Minimum lethal dose = 430 ppm for 30 min
- Median lethal dose (short-term exposure) = 1,000 ppm

References

Variable		Range / Units	User Input
Outdoor Temperature	Selection Guidance	(50, 68, or 82) °F	68
Wind Speed	Selection Guidance	(3, 9, or 15) mph	9
Setting	Selection Guidance	Urban or Rural	Urban
Population Density	Selection Guidance	(500 - 48,502) pers. per km²	8000

Calculation Methodology & Scaling

Johns Hopkins University School of Medicine's Department of Emergency Medicine, recognized a need for a technology like EMCAPS when he was attending an emergency response drill several years ago. The drill scenario involved an explosion at a baseball stadium filled with 45,000 fans. As part of the scenario, participants were told to plan to treat 30,000 patients. The number struck Scheulen as unrealistic. This lack of realism was problematic, because without credible estimates, it is difficult for emergency preparedness officials to judge just how many hospital beds, ambulances, personnel, and equipment truly would be needed in an emergency. EMCAPS mitigates this problem by providing first responders with an estimate rooted in scientific facts. For example, EMCAPS relies on data from explosive experts about the likely force and circumference of a dirty bomb blast to calculate the number of casualties first responders could expect in that situation. «It's meant to tell you if you're talking about 100 people being hurt or 1,000 people being hurt,» Scheulen said. «Now you have some realistic numbers you can use to go about the rest of



your planning.» EMCAPS helps emergency response officials ensure they are ready for a large-scale threat. Melinda Johnson, Metropolitan Medical Response System program coordinator for the north central region of Colorado, began using the software three years ago. With EMCAPS, she can run a scenario and see how the estimated number of patients compares to the surge capacity at area hospitals. If a given situation would overwhelm a particular local hospital, medical personnel would work with local and state officials to move patients to another hospital in the 10-county region or elsewhere in the state. Prior to the creation of EMCAPS, first responders and emergency planners had few tools to calculate the likely impact of an emergency. «It's difficult to find an algorithm that says x disaster in this community causes y casualties,» Johnson said. In addition to estimating the numbers of casualties in a given disaster, EMCAPS lists the kinds of injuries victims are likely to sustain based upon the disaster type. With this information, first responders participating in training scenarios can consider what equipment and planning would be needed to effectively treat patients. Victims of a dirty bomb detonation, for instance, would likely experience partial or total hearing loss. In that situation, first responders must consider ways to effectively communicate with patients during the triage process, according to Scheulen. When the significantly upgraded version of the software is released next year, it will offer even more scenarios, including earthquakes and hurricanes, so first responders can plan for natural disasters as well as terrorist attacks, according to Whiteree. Researchers are reviewing the existing scenarios to see if the calculations can be improved or updated. The release also will revise the injury severity scale used in the current EMCAPS, according to Johns Hopkins University Applied Physics Laboratory Epidemiologist Jacqueline Coberly. To make the software more applicable to real emergencies, the injury scale in the new version will match the designations used by emergency room doctors to rank injuries. Johns Hopkins University researchers and DHS also are exploring the possibility of linking future versions of the EMCAPS software to a mapping program, according to Whiteree. The capability would allow first responders to consider the best locations for shelters and other emergency facilities.

EMCAPS may be downloaded as shareware without cost from:
http://www.hopkins-cepar.org/EMCAPS/EMCAPS.html

Concerns grow over Egypt’s WMD research

U.S. has been quiet about Cairo’s weapons programs, but revolt changes the calculus

By Robert Windrem – NBC Senior investigative producer

Source: http://www.msnbc.msn.com/id/41452744/ns/world_news-mideast/n_africa/

With Egypt in revolt and the country’s future uncertain, concern is growing over whether a new government in the Arab world’s most militarily and industrially advanced country could accelerate an arms race in one of the world’s most volatile regions. At the heart of the concern is intelligence indicating that Egypt has quietly carried out research and development on weapons of mass destruction, including nuclear, chemical, biological and missile technology. The research and development has continued virtually without pause over the past three decades, according to interviews with U.S. officials and a review of intelligence and other government documents by NBC News. Specifically, the intelligence indicates that Egypt has carried out experiments in plutonium reprocessing and uranium enrichment, helped jump-start Saddam Hussein’s missile and chemical weapons programs in Iraq, and worked with Kim il-Jung on North Korea’s missile program. “If we found another country doing what they’ve done, we would have been all over them,” said a former U.S. intelligence official, speaking on condition of anonymity. The reason the U.S. didn’t move, officials say, was Egypt’s role as a staunch U.S. ally and stabilizing force in the Middle East and later as a key player in U.S. counterterrorism efforts. If Egyptian President Hosni Mubarak is forced to step down, new leadership in Cairo could mean a radical change in that relationship, analysts say.

Withdraw from nuke treaty?

In fact, at least one nuclear proliferation analyst believes that a shift may already be under way in Egyptian policy and that the U.S. may have to deal with Cairo withdrawing from the Nuclear Non-Proliferation Treaty, which it signed and ratified in 1968. “They hint that if something isn’t done about Israel’s nuclear weapons program or Iran’s nuclear ambitions, they may be prepared to leave the (treaty),” said David Albright, president of the Institute for Science and International Security and a former inspector with the International Atomic Energy Agency. The Egyptians have pushed for a U.N. conference next year on weapons of mass destruction, or WMD, in the Middle East, and would like to see constraints placed on Israeli and Iranian arms programs. But “these requirements are hard to meet,” Albright said. “(The conference) may not end well, and that could be a catalyst for them to leave the (Non-Proliferation Treaty).” So far, the international community has not made the conference a priority. Seven months after the agreement to hold the conference, the U.N. has yet to establish a venue, an agenda or a facilitator to organize it. If Egypt was to withdraw from the treaty, there would be no restraints on its development of nuclear technology, whether for energy or for weapons. And Cairo already has given indications that it may harbor nuclear ambitions, according to analysts inside and outside the U.S. government. The International Atomic Energy Agency criticized Egypt in February 2005 for failing to report a variety of nuclear experiments over 20 or more years. The agency noted the Egypt had used “small amounts” of nuclear material to conduct experiments related to producing plutonium and enriched uranium, both of which can be used to make nuclear weapons. (The agency was then led by Mohamed ElBaradei, now an opposition figure and potential candidate to become at least an interim leader of a post-Mubarak government.)

Uranium, plutonium experiments

While the plutonium experiments appear to have taken place at least 20 years ago, the uranium experiments were more recent. According to the IAEA report, Egypt used its two research reactors at Inshas in the Nile Delta between 1990 and 2003 to irradiate “small amounts of natural uranium,” conducting a total of 16 experiments. According to the

IAEA, none of the experiments fully succeeded, but in each case, Egypt failed to report them to the agency as required by the Nuclear Non-Proliferation Act. Egypt eventually acknowledged that it had not fully disclosed the extent of its nuclear facilities, failed to declare the pilot plant used for the plutonium and uranium-separation experiments and did not provide design information for a new facility under construction, also at Inshas. The IAEA declared the lapses a "matter of concern" but stopped short of accusing Egypt of having a clandestine nuclear weapons program.

What do we know about Egypt's arsenal?

In a statement responding to the IAEA, Egypt played down the violations, claiming that "differing interpretations" of its obligations under the treaty had led to the problems. But Albright said the experiments triggered concerns that Egypt was interested in the nuclear fuel cycle — the full development of fuel that can be used to power reactors or build bombs. "For 15 years, they have made credible moves to build up their nuclear fuel cycle capability," he said. Egypt has admitted that it pursued nuclear weapons in the 1960s as it first learned about Israel's nuclear program, which by 1966 had produced its first atomic bombs. At that point, at least some of those weapons would have targeted Egyptian cities.

Mubarak on the record

And Mubarak himself has occasionally raised the possibility of a nuclear Egypt. In an October 1998 interview, Mubarak said that Egypt could, if need be, develop nuclear weapons or buy the technology. «If the time comes when we need nuclear weapons, then we will not hesitate," he told London's al-Hayat newspaper. «… Acquiring material for nuclear weapons has become very easy, and it can be bought.» As always, he then dismissed the idea. "I say, 'if we have to,' because this is the last thing we think about,» he told al-Hayat. «We do not think now of joining the nuclear club." The U.S. now believes that Mubarak's reference to being able to buy nuclear technology was not just an off-hand remark. The statement appears to coincide with a secret offer by Pakistan's A.Q. Khan to help Egypt develop nuclear arms, an offer that was rejected by Cairo, say U.S. intelligence officials. Despite these such hints, some observers do not believe that a new government would risk withdrawing from the non-proliferation treaty and moving to develop nuclear weapons. James Russell, a nuclear non-proliferation expert at the Naval Post-Graduate School in Monterey, Calif., and a former Pentagon official, thinks re-entering the nuclear race would be politically risky and economically unwise. He noted that the Egyptian government abandoned its nuclear ambitions after the 1967 war with Israel because of the cost and the lack of scientific expertise.

'We don't know'

The question is, would a follow-on regime want to revisit this?" he said. "Would it look at the set of calculations and pursue not a peaceful program but consider constructing an illicit program? The answer is that we don't know, but we do have an idea of what the costs of doing that would be … and the prospect that they'd have a pretty damn difficult time trying to hide it. "I have a hard time seeing the costs (for) mounting such a program. The calculus argues for not doing this ... even for an Islamic regime," he added. But as Russell and others note, the Egyptians "don't have a clean record" in other areas of arms proliferation. And if the Egyptians lost part or all of their U.S. military aid, they could be expected to try to make up those losses by developing and exporting more weapons technology. A revealing example of that occurred when Egypt helped Iraq develop its chemical weapons capability before the Gulf War. A CIA report in 2005 indicated that the Egyptian arms industry was sophisticated enough to permit Egypt to help Iraq make "technological leaps" in the 1980s, as Arab Iraq was battling Persian Iran. The 350,000-word report, little noticed until the Associated Press wrote of it in March 2005, stated that in 1981, after the outbreak of war with Iran, the Iraqi government paid Egypt $12 million «in return for assistance with production and storage of chemical weapons agents.» It said the assistance included making modifications to rocket systems to permit the warheads to store and disperse chemical agents and help ing Saddam's scientists develop sarin munitions. The sarin development is the best indicator of the Egyptian chemical weapons capabilities, say military experts. Sarin is a nerve agent, one of the more advanced military chemicals in the world.

A lesson from assistance to Iraq

Before the mid-1980s, Iraq was limited to mustard gas and other disfiguring agents. But not long after the Egyptian scientists arrived, Iraqi sarin production soared — from 5 tons in 1984 to 209 tons in 1987 and 394 tons in 1988, the report says. During that period, sarin was used extensively by Iraq to kill Kurdish dissidents in the north as well as Iranian soldiers in the south. The Egyptians also were critical to the development of an Iraqi missile program, Begun during the Iran-Iraq War in the mid-1980s. With financing from Iraq, Egypt set up a secret $750 million missile development project in the foothills of the Andes, just south of Cordoba, Argentina. Called the Condor-II, it was an advanced, mobile, two-stage, solid-fuel ballistic missile that could carry a half-ton warhead more than 600 miles. By 1985, it was well along in development and the centerpiece of an international consortium run by Egypt's Ministry of Defense. U.S. pressure on Argentina and Egypt stopped the project, say U.S. intelligence officials. And that is not the only example of Egypt working with a rogue state. Also in the mid-1980s, Egypt secretly cooperated with North Korea to improve both countries' missile arsenals. Egypt's shipped at least two of its Soviet-supplied Scuds to North Korea for reverse-engineering. In return, Pyongyang agreed to help Cairo build Scuds on its own. North Korea provided technical documents, drawings and extensive access to North Korea's own Scud production program. The cooperation led to North Korea's development of its Nodong and Taepo-dong missiles. The former was later sent to Pakistan in exchange for nuclear technology, and deployment of the latter led the U.S. to install its "Star Wars" anti-missile system in Alaska, U.S. intelligence officials said. It is this backdrop — and the fact that Egypt still has considerable expertise in missiles and chemical weapons — that has some analysts concerned about the path that a new Egyptian government might take. If an Islamic-dominated government emerges in the wake of Mubarak's departure, "then all bets are off" as far as pursuit of WMDs, said Russell, the former Pentagon official. That also would be true of Egyptian-Israeli relations, he said. If the military retains power and installs another one of its own as leader, the analysts said, the issue will be to what extent Egypt's relationship with the U.S. is damaged by the Obama administration's efforts to exert its influence in the crisis. The only outcome that would entirely calm concerns about Egypt's WMD ambitions would be if ElBaradei emerged as a central figure in a successor government, they said. He is, after all, a Nobel Peace Prize laureate because of his efforts to stop nuclear proliferation.

New sense of nationalism expected

But no matter the outcome, Egypt is likely to become "newly sovereign," or more nationalistic, in the post-Mubarak era, the analysts said. Egypt would face great costs — including loss of U.S. aid and the ability to buy U.S. military equipment — if it became too open in its dealings with rogue states, or if it pressed hard on a nuclear agenda, notes Judith Yaphe, a 20-year veteran of the CIA who is now senior research fellow and Middle East project director at the National Defense University. But that doesn't necessarily mean that a new government might not decide that perilous times call for high-risk actions. "Will it change? Who knows?" she said. "The Egyptian military has important things it has to protect. It would like to protect its relationship with the United States. ... Those close ties are something they value. They value highly the training, the weaponry. "Still, we shouldn't be terribly surprised they are playing with things. Israel is still there, and the Iranians have ambitions. Call it the 'Iran Effect,' if you want. Everyone else has given up on the Egyptians as great leaders, but the Egyptians haven't."

QinetiQ
North America

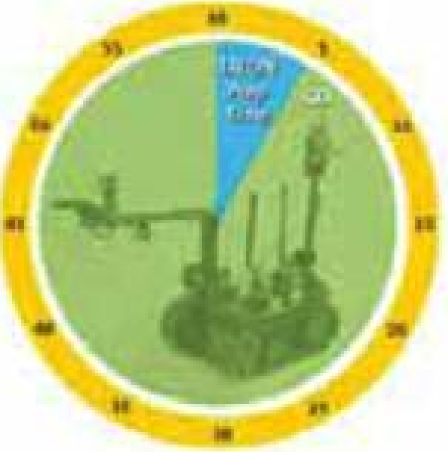
TALONrobots.com

TALON® CBRNE/Hazmat Robots Speed Time to Detection

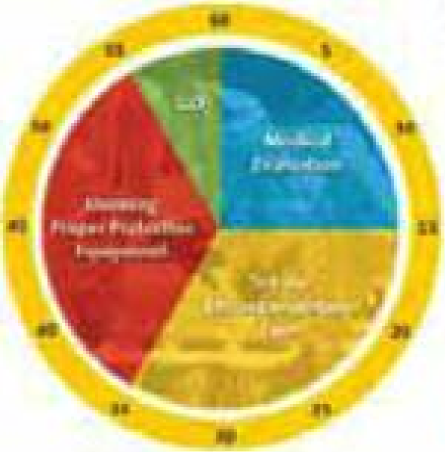
Save precious lives and almost an hour of valuable time by sending a TALON CBRNE / Hazmat robot downrange to assess an incident before putting any personnel at risk. Our robots are equipped to plug and play up to seven detection instruments including:

- JCAD (joint chemical agent detector) for CWAs (chemical warfare agents) and TICs (toxic industrial chemicals)
- RAE MultiRAE Plus for volatile gases
- Canberra AN/UDR-14 for gamma and neutron radiation
- Raytek temperature probe for temperature sensing
- Smiths APD 2000 WMD (weapons of mass destruction) detector
- ICx Technologies Fido® XT for trace explosives

Five minutes to TALON down-range



Fifty-five minutes to Humans down-range



For further information or to arrange a demonstration, please contact Joanne Armstrong at +1.781.684.3960 or Talonsales@QinetiQ-NA.com

QinetiQ-NA.com

M09 055-W

Iranium – the movie

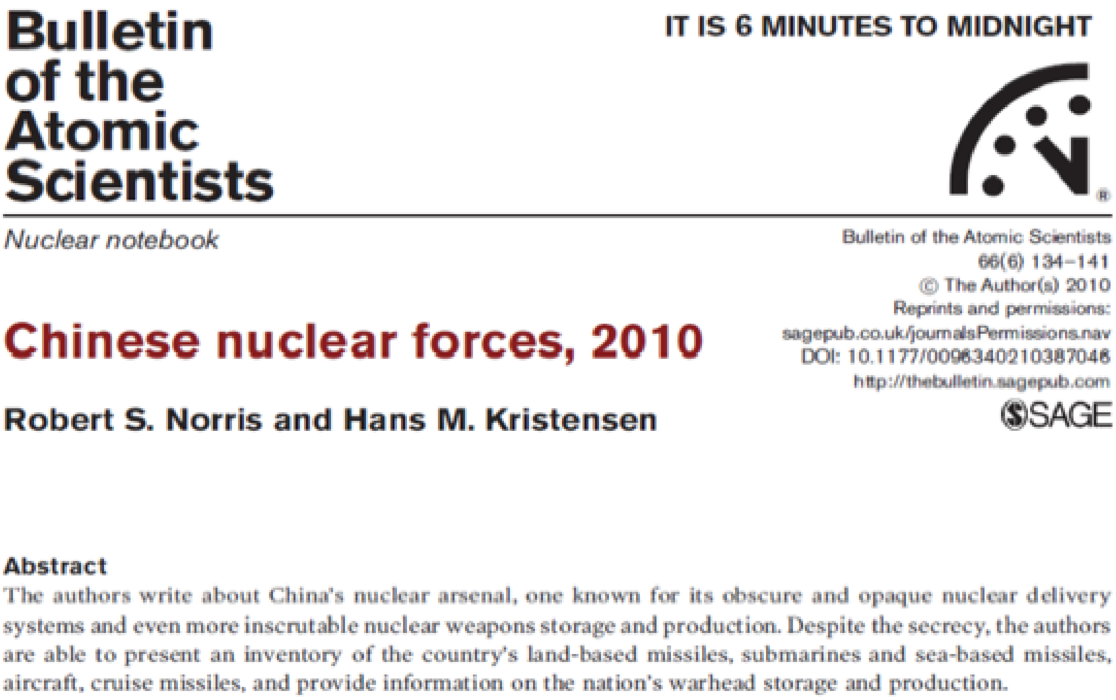
Source: http://www.iraniumthemovie.com/

Iran's nuclear program presents a threat to international stability. Yet successive American administrations-Republican and Democratic alike-have misread the intentions and actions of the Iranian regime. How dangerous is a nuclear Iran, even if it never detonates a weapon? What are the guiding principles of the Iranian leadership? To what lengths would the regime go to carry out its agenda? How far have Iran's leaders already gone to fund the world's most powerful terrorist organizations? And why have American leaders failed to gain the upper hand in relations with Iran during the past 30 years? In approximately 60 minutes, Iranium powerfully reports on the many aspects of the threat America and the world now faces using rarely-before seen footage of Iranian leaders, and interviews with 25 leading politicians, Iranian dissidents, and experts on: Middle East policy, terrorism, and nuclear proliferation.

- Iranium documents the development of Iran's nuclear threat, beginning with the Islamic Revolution of 1979 and the ideology installed by Supreme Leader Ayatollah Khomeini.
- Iranium tracks Iran's use of terror as a tool of policy, beginning with the 444 day seizure of the U.S. Embassy in Tehran, through Iran's insurgent actions in Iraq and Afghanistan.
- Iranium details the brutal nature of the Iranian regime to its own citizens, and the Iranian people's desire to rejoin the international community.
- Iranium outlines the various scenarios the greater Middle East and the Western world may face should Iran cross the nuclear threshold.

Chinese nuclear forces - 2010

Source: http://bos.sagepub.com/content/66/6/134.full.pdf+html



Bulletin of the Atomic Scientists

IT IS 6 MINUTES TO MIDNIGHT

Nuclear notebook

Bulletin of the Atomic Scientists
66(6) 134–141
© The Author(s) 2010
Reprints and permissions:
sagepub.co.uk/journalsPermissions.nav
DOI: 10.1177/0096340210387046
http://thebulletin.sagepub.com
SAGE

Chinese nuclear forces, 2010

Robert S. Norris and Hans M. Kristensen

Abstract

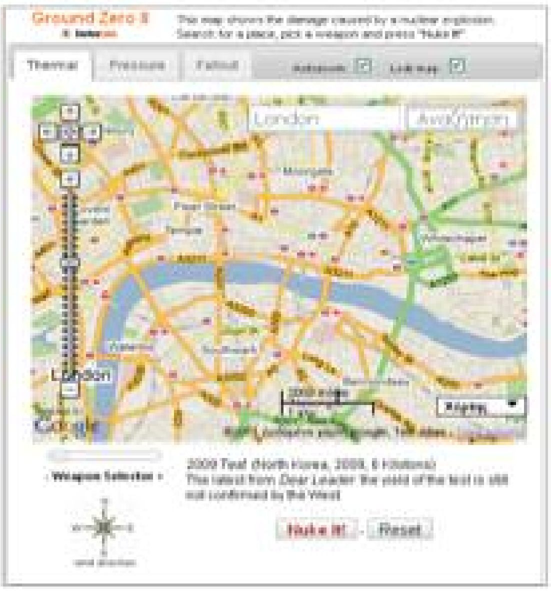
The authors write about China's nuclear arsenal, one known for its obscure and opaque nuclear delivery systems and even more inscrutable nuclear weapons storage and production. Despite the secrecy, the authors are able to present an inventory of the country's land-based missiles, submarines and sea-based missiles, aircraft, cruise missiles, and provide information on the nation's warhead storage and production.

What would happen if your town got nuked?

Source: http://www.gizmag.com/nuclear-bomb-damage-map-nuke/12097/

Editor's Note: A very interesting simulation of a nuke explosion in urban environment. You can set up the following parameters:

1. Weapon selection
2. Wind direction
3. Thermal consequences
4. Pressure consequences
5. Fallout consequences
6. Choose a city via Google maps



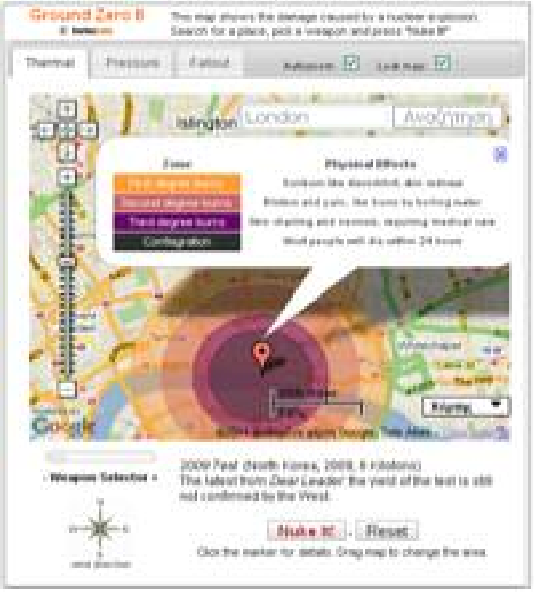
Ground Zero II

This map shows the damage caused by a nuclear explosion. Search for a place, pick a weapon and press "Nuke it!"

Autozoom ☑ Lock map ☑

London

2009 Test (North Korea, 2009, 8 kilotons)
The latest from *Dear Leader*: the yield of the test is still not confirmed by the West



Ground Zero II

This map shows the damage caused by a nuclear explosion. Search for a place, pick a weapon and press "Nuke it!"

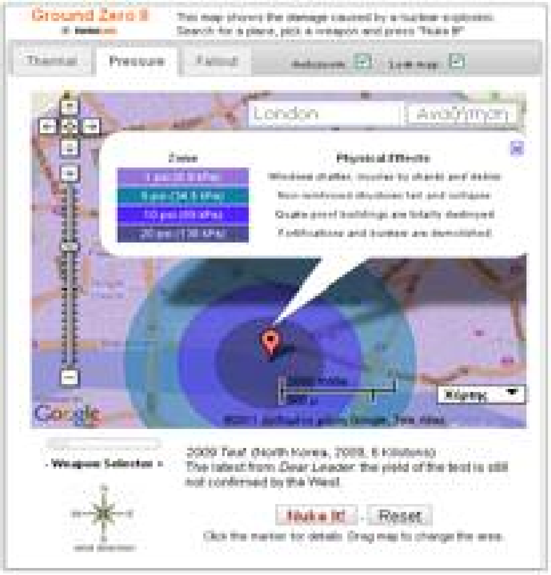
Autozoom ☑ Lock map ☑

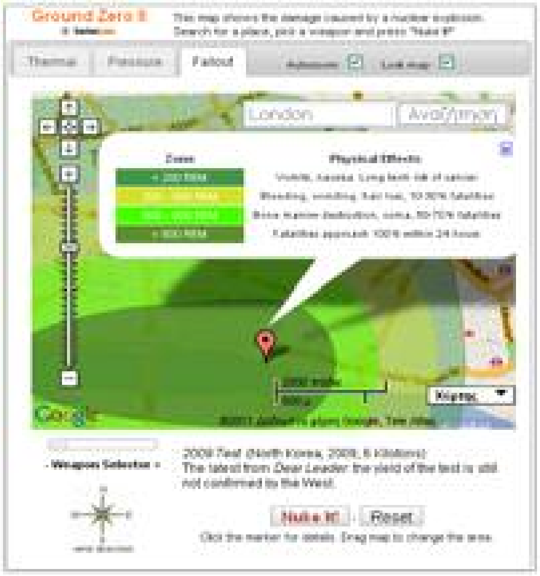
London

Zone	Physical Effects
First degree burns	[illegible]
Second degree burns	[illegible]
Third degree burns	[illegible]
Conflagration	[illegible]

2009 Test (North Korea, 2009, 8 kilotons)
The latest from *Dear Leader*: the yield of the test is still not confirmed by the West

Click the marker for details. Drag map to change the area.


Ground Zero II
This map shows the damage caused by a nuclear explosion. Search for a place, pick a weapon and press "Nuke It!"
Thermal
Pressure
Fallout
London
Zone
Physical Effects
1 psi (6.9 kPa)
5 psi (34.5 kPa)
10 psi (69 kPa)
20 psi (138 kPa)
Windows shatter, injuries by shards and debris
Non-reinforced structures fail and collapse
Quake proof buildings are totally destroyed
Fortifications and bunkers are demolished
Weapon Selector
2009 Test (North Korea, 2009, 6 Kilotons)
The latest from Dear Leader: the yield of the test is still not confirmed by the West.
Nuke It!
Reset
Click the marker for details. Drag map to change the area.


Ground Zero II
This map shows the damage caused by a nuclear explosion. Search for a place, pick a weapon and press "Nuke It!"
Thermal
Pressure
Fallout
London
Zone
Physical Effects
Vomiting, nausea. Long term risk of cancer
Bleeding, vomiting, hair loss, 10-50% fatalities
Bone marrow destruction, coma, 50-70% fatalities
Fatalities approach 100% within 24 hours
Weapon Selector
2009 Test (North Korea, 2009, 6 Kilotons)
The latest from Dear Leader: the yield of the test is still not confirmed by the West.
Nuke It!
Reset
Click the marker for details. Drag map to change the area.

No, a Boy Scout cannot build a backyard nuclear reactor

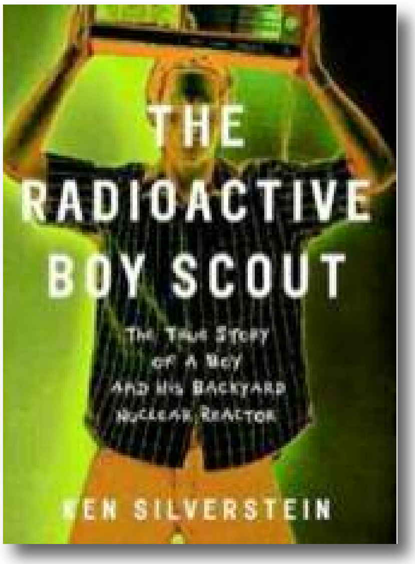
Source: http://homelandsecuritynewswire.com/no-boy-scout-cannot-build-backyard-nuclear-reactor

Dirty bombs are easy to build and only require strapping explosives to radioactive material; in counter-terrorism circles there is a myth that in 1995 a Boy Scout was able to assemble enough radioactive materials to build a nuclear reactor in his backyard in Michigan by gathering all of his materials from common household items; he dismantled lanterns to obtain Thorium, smoke detectors for Americium, and old clock dials for Radium; analysts say that it would take material from roughly two million smoke detectors to build a dirty bomb that would cause any damage

Counter-terrorism officials have long feared that terrorists would detonate a dirty bomb killing hundreds and sending a toxic cloud of radioactive material into the air. While not as deadly as an atomic weapon, they are far easier to build. Making one of these bombs is as simple as strapping explosives to radioactive material, and al Qaeda has publicly announced that it was seeking to obtain nuclear materials. National security officials and law enforcement agents have sought to safeguard the world's supply of radioactive materials, but in counter-terrorism circles there is a myth that in 1995 a Boy Scout was able to assemble enough radioactive materials to build a nuclear reactor in his backyard in Michigan. PBS decided to investigate this myth and get the facts behind the story. In 1995 U.S. Environmental Protection Agency crews, clad in protective suits, descended upon the quiet suburb of Golf Manor, Michigan to dismantle and decontaminate the beginnings of a rudimentary nuclear breeder reactor. The reactor was built by seventeen year old David Hahn, who was an aspiring Eagle Scout on a quest to earn his atomic energy merit badge when he got carried away. The assignment called for the Scout to make a model nuclear reactor out of straws and matches, but Hahn, who had long been fascinated by radioactive materials and science, wanted to build the real thing. He set about gathering as much radioactive material as he could. All of his materials were found in common household items. He dismantled lanterns to obtain Thorium, smoke detectors for Americium, and old clock dials for Radium. According to PBS, Hahn had assembled

David Hahn the «Radioctive Boy Scout» // Source: arstechnica.com

enough material to build a small breeder reactor, which generates more fissile material than it consumes. The Boy Scout spent eight to ten hours a day trying to build the reactor in an attempt to transform one element to the next and believes that he may have done it, but is not sure. He decided to stop his experiment before things progressed too far and was in the process of carting off the dangerous materials when he was stopped by the police. The EPA quickly descended on his parent's home and decontaminated the area, taking his materials and much of the dirt in his backyard to a radioactive waste dump in Utah. Hahn was never charged as he did not break any laws and did not mean any harm. Far from showcasing the ease with which terrorists can gather radioactive materials from household items, Hahn says that it was very difficult to accumulate all the smoke detectors, lanterns, and old clocks. Analysts say that it would take material from roughly two million smoke detectors to build a dirty bomb that would cause any damage. Hahn went on to serve in the military as a Marine and an enlisted member of the Navy. With the Navy he became the helmsman of the USS Enterprise, a nuclear-powered aircraft carrier. Hahn's story is the subject of a book, The Radioactive Boy Scout.


THE RADIOACTIVE BOY SCOUT
The True Story of a Boy and His Backyard Nuclear Reactor
KEN SILVERSTEIN

Explo News

New kind of blast-resistant glass — thinner and tougher — developed

Source:http://homelandsecuritynewswire.com/new-kind-blast-resistant-glass-thinner-and-tougher-developed

Current blast-resistant glass technology — the kind that protects the windows of key federal buildings, the president's limo, and the Pope-mobile — is thicker than a 300 page novel — so thick it cannot be placed in a regular window frame; DHS-funded research develops thinner, yet tougher, glass; the secret to the design's success is long glass fibers in the form of a woven cloth soaked with liquid plastic and bonded with adhesive. Whether in a hurricane, tornado, or bomb attack, a leading cause of injury and death is often fast-flying shards of glass. Explosions and high winds can cause windows in buildings to shatter-spewing jagged pieces of glass in every direction. A Pentagon report on the 1996 Khobar Towers bombing in Saudi Arabia, for example, noted:

> *Two of the 19 deceased had injuries know to be caused by glass fragments that were severe enough to cause death even without other contributing forces. Of the remaining 17 deceased, 10 had glass injuries that were significant and which may have caused death even without blunt force trauma. Thus, for 12 of 19 deaths, glass fragmentation was a significant factor. More than 90% of the people injured suffered laceration injuries, many of which were significant.*

With an international research grant from DHS's Science and Technology Directorate (S&T), a team of engineers from the University of Missouri and the University of Sydney in Australia is working to develop a blast-resistant glass that is lighter, thinner, and colorless, yet tough enough to withstand the force of an explosion, earthquake, or hurricanes winds. Installing blast-resistant glass in buildings that are potential targets of attacks or in regions prone to severe weather can save lives. Current blast-resistant glass technology — the kind that protects the windows of key federal buildings, the president's limo, and the Pope-mobile — -is thicker than a 300-page novel — so thick it cannot be placed in a regular window frame. This makes it very difficult — and expensive — to replace standard glass windows in present structures. Unlike today's blast-resistant windows which are made of pure polymer layers, this new design is a plastic composite that has an interlayer of polymer reinforced with glass fibers-and it's only a quarter-inch thick. The project team recently subjected their new glass pane to a small explosion. "The results were fantastic," exclaimed Sanjeev Khanna, the project's principal investigator and an associate professor of mechanical engineering at Missouri. "While the discharge left the pane cracked, the front surface remained completely intact." The secret to the design's success is long glass fibers in the form of a woven cloth soaked with liquid plastic and bonded with adhesive. The pane is a layer of glass-reinforced clear plastic between two slim sheets of glass. Even the glue that holds it all together is clear. Think of it as a sandwich: the slim sheets of glass are the two slices of break; the liquid plastic and long glass fibers make up the crunchy peanut butter in the middle. The glass fibers are typically 15 to 25 micrometers in diameter, about half the thickness of a typical human hair. The small size results in fewer defects and a decreased chance of cracking. The strong glass fibers also provide a significant reinforcing effect to the polymer matrix used to bind the fibers together. The more fibers used, the stronger the glass reinforcement. And while traditional blast-proof glass usually has a greenish ting, special engineering renders the polymer resin transparent to visible light. Engineers expect the new design will be comparable in cost to current blast-proof glass panes, but lighter in weight. At only a quarter-inch thick, this newly engineered composite would slip into standard commercial window frames, making it much more practical and cost-efficient to install. "Designing an affordable, easy-to-install blast-resistant window could encourage widespread use in civilian structures, thereby protecting the lives of occupants against multiple threats and hazards," notes John Fortune, manager of the project for the Infrastructure and Geophysical Division at S&T. To date, the glass has been tested with small-scale prototypes. "In future tests, the size of the glass panels will be increased by two to four times to determine the effect of size on blast resistance," said Khanna. The goal is to create blast-resistant panes as large as 48 by 66 inches-the standard General Services Administration window size for qualification blast testing-that can still be cost-effective. While dependent on results from upcoming tests, Khanna hopes this glass could become commercially available in three to four years.

Fully robotic, remotely controlled bomb-disposal hand nears

Source:http://homelandsecuritynewswire.com/fully-robotic-remotely-controlled-bomb-disposal-hand-nears

Engineers have developed a robotic hand that offers remotely controlled, highly dexterous movements that could lead to a breakthrough in areas such as bomb disposal; the robotic hand can be remotely controlled by a glove worn by an operator connected to a computer; this can then communicate via a wireless connection with the hand offering real time comparable movements

Engineers have developed a robotic hand that offers remotely controlled, highly dexterous movements that could lead to a breakthrough in areas such as bomb disposal. The Shadow Dextrous Hand (see this YouTube video), developed by U.K. firm Shadow Robot Company, is able to replicate twenty-four highly precise movements that are designed to provide similar force output and sensitivity to the human hand. The humanoid robotic hand, which was on display at the TechnologyWorld forum at London's Excel Centre on Wednesday, is driven by twenty motor units mounted below the wrist which provide compliant movements, with each motor corresponding to a joint on a hand. TechEye reports that the new C6M2 model can be remotely controlled by a glove worn by an operator connected to a computer, this can then communicate via a wireless connection with the hand offering real time comparable movements. In the future this could allow the sophisticated movements that are required in dangerous tasks such as disposing of explosive materials from a safe distance. "We are approximately eighteen months to two years away from being able to have the technology at the stage where it can be reliably used in a environment such as bomb disposal," Jake Goldsmith, robotics engineer at Shadow told TechEye. Goldsmith says one challenge has been getting the pressure right. While it may seem like little effort, something as simple as pushing a button on a mobile phone needs a

Robotic hand demonstration // Source: io9.com fair amount of force behind it — but not too much. As Shadow Robot Company is discussing military applications, the kinks need to be ironed out before it enters the real world: “While the hand functions very well now, to be used in such a situation it would need to work perfectly 100 percent of the time which will take more testing.”

Police robot ends Wisconsin standoff

Source: http://homelandsecuritynewswire.com/police-robot-ends-wisconsin-standoff

Last Friday, a Northrop Grumman police robot was sent to investigate an SUV parked on the shoulder of a Milwaukee, Wisconsin, highway; the robot approached the two potentially dangerous suspects holed up in an SUV, transmitted instructions from a hostage negotiator sitting safely in a nearby truck, and punched out the rear window of the suspects’ stolen car, helping police end the standoff peacefully

The Remotec ANDROS F6A is the most versatile, heavy-duty robot on the market. Speed and agility unite to make it your first choice for a wide range of missions.
ANDROS F6A

The machine can climb stairs, open doors, defuse bombs, and deploy its water cannon like a 12-gauge shotgun. It can also, as evidenced by events that unfolded Friday on the shoulder of westbound I-94 near 19th St. in Milwaukee, Wisconsin, approach two potentially dangerous suspects holed up in an SUV, transmit instructions from a hostage negotiator sitting safely in a nearby truck, and punch out the rear window of the suspects’ stolen car. The hole left by the Remotec Andros F6A, affectionately known as “Ace” by the Milwaukee County Sheriff ‘s Office bomb squad, allowed a SWAT officer to thrust a tear gas canister inside and smoke out the two suspects, effectively ending the 6-hour standoff that had halted traffic for hours on I-94. The events turned the spotlight on the 485-pound, 4-foot-tall Ace, which has spent the last six years quietly investigating suspicious packages and providing surveillance for law enforcement around southeastern Wisconsin. PoliceOne.com reports that Terminator and R2-D2 jokes aside, similar devices have become indispensable to bomb squad units across the country — federal Homeland Security grants have supported the purchases — and point to an increasing reliance on technology in modern law enforcement. “After 9-11, we’ve put a lot of emphasis on the safety of our officers and new technologies,” said Deputy Gary Nell, commander of the Milwaukee County Sheriff ‘s Office bomb squad. “This keeps all the deputies and the public safe.” The Andros F6A by manufacturer Northrop Grumman is operated by remote control, costs about $200,000 and has tracks and wheels to get around uneven terrain. It also has four cameras to zip images back to a command center inside the bomb squad truck, and speakers to transmit instructions from a hostage negotiator to suspects or others on the scene. On Friday, about five people in the truck were huddled around the screens as Ace approached the stolen SUV, Nell said. The man and woman in the SUV seemed surprised to be communicating with a robot, he added. Ace worked so well that it probably should have been brought in sooner, Nell said, but it was the first time the machine had been used for negotiation-type purposes. “It’s easy to look back with 20-20 vision,” he said. “I think the feeling was to try to use the SWAT team equipment first and see how that worked before deciding to bring in the robot.”.

Electromagnetic scanner detects threat liquids without taking the lid off

Source: http://www.gizmag.com/go/7342/

Without going through the hassle of removing bottle-tops, staff at security checkpoints are unable to see the difference between a bottle of drinking water and a potential molotov cocktail - the solution has commonly been to prevent people from passing through checkpoints with bottles. Now there’s a device that can instantly detect whether a bottle contains a potential threat liquid without taking the top off. The Senicon is already in use in Japan’s Kansai International Airport - and it’s currently under review by the U.S. Department of Homeland Security for use in airports and other areas under threat of terrorist attacks.

Sellex International recently announced the availability of the Sencion threat liquids detector, which uses electro-magnetic wavelengths to instantaneously detect threat liquids (flammable or explosive liquids) contained in glass or plastic bottles. As airports deal with large numbers of people every day, the need for technology that screens every passenger, has no additional impact on security line wait time and also allows passengers comfort and peace of mind becomes more apparent.

Sellex’s Sencion thread liquids detector - the flashing red light indicates the presence of a threat liquid like Kerosene.

«Flying today has become a hassle — luggage checks, carry-on exclusions and invasive personal searches. Though necessary, the process certainly is not comfortable or convenient for travelers,» said Jerry Sellman, president and CEO of Sellex International, the company behind the development of the Sencion device. «The Sencion gives travelers back some comfort and control. The ability to carry the drink of your choice through a security checkpoint instead of having to spend extra money on a limited selection of beverages available in the secured areas is a convenience that makes for one less hassle. And most importantly, we can provide this convenience without sacrificing security.»

The Sencion permits people to safely and conveniently carry drinks and other approved liquids through security checkpoints. Such liquids include water, sodas, juices, baby formulas, protein drinks and the like; certain hygiene products, such as shampoo; most liquid medicines; and alcoholic beverages generally purchased in Duty-free shops. The Sencion's instantaneous detection capability can screen all passengers' permitted drink bottles and accommodate even the busiest flow of traffic in any of the nation's airports without increasing wait times.

The Sencion threat liquids detector has been successfully incorporated in the passenger screening process in parts of Asia since August 2004, and is currently helping to protect the more than 15 million passengers that pass through the Kansai International Airport in Osaka, Japan each year.

The Department of Homeland Security is currently reviewing the Sencion as an immediate solution for American airports. After the discovery of a plot to blow up American airliners traveling from the United Kingdom to the U.S. in August 2006, the Department of Homeland Security made a worldwide request for technology that could meet the immediate need for threat liquid detection capabilities at airports and other mass transit facilities. Sellex International responded to the request by the Department of Homeland Security, submitting the Sencion threat liquids detector as a proven and viable solution.

«The Department of Homeland Security and the TSA [Transportation Security Administration] have been instrumental in ensuring the highest security measures are available for airline passengers,» Sellman said. «We believe the Sencion is the only threat liquid detection device that addresses all of the department's security concerns and is ready for immediate deployment in airports nationwide.»

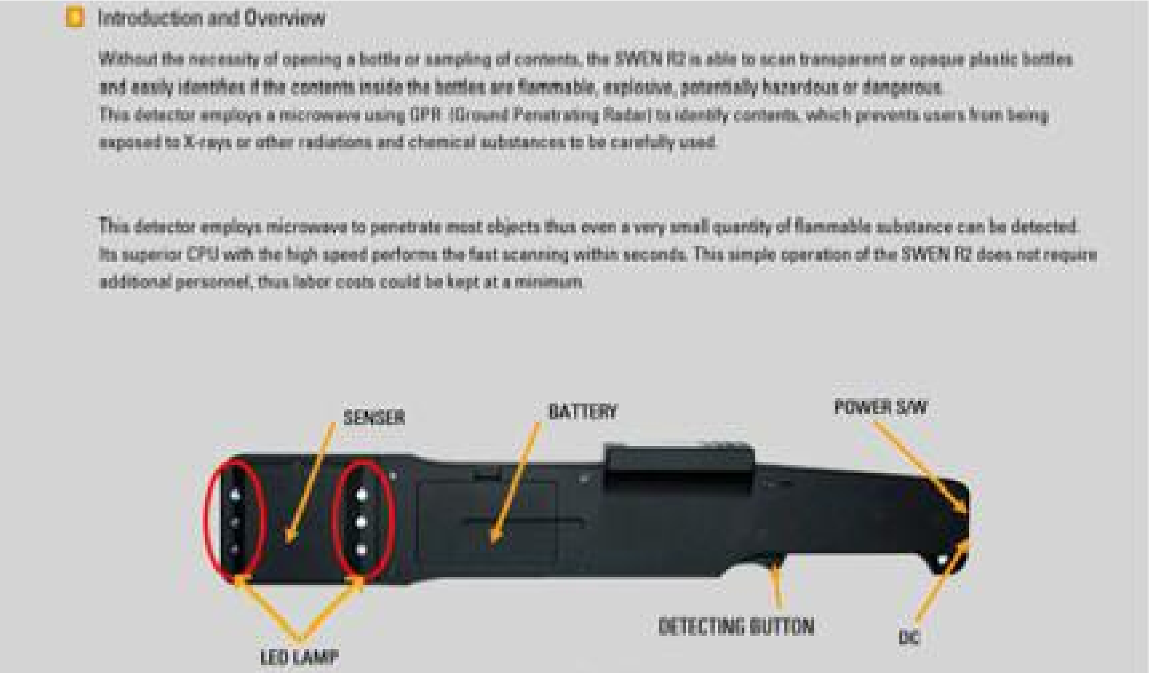
Explosives Detection Using Magnetic and Nuclear Resonance Techniques
NATO Science for Peace and Security Series B: Physics and Biophysics,

2009, 73-79, DOI: 10.1007/978-90-481-3062-7_5

Source: http://www.springerlink.com/content/h28611119rj331x6/
(you can read the text only on-line)

Detection of liquid explosives without opening the lid

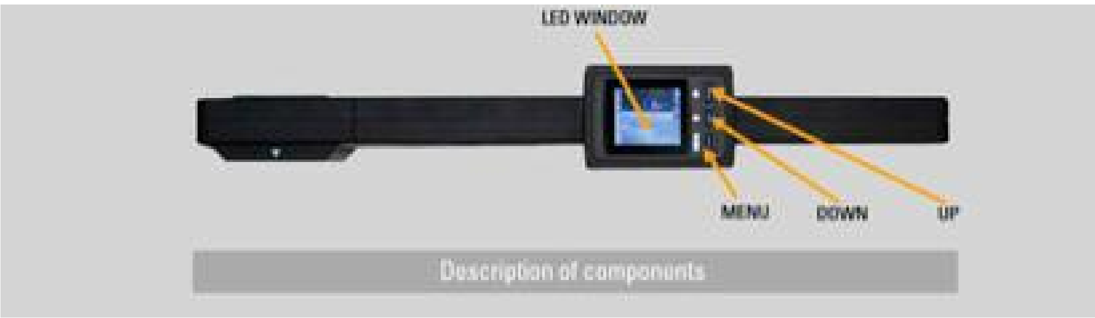
Source: http://www.cnsintglobal.com/scanner.html



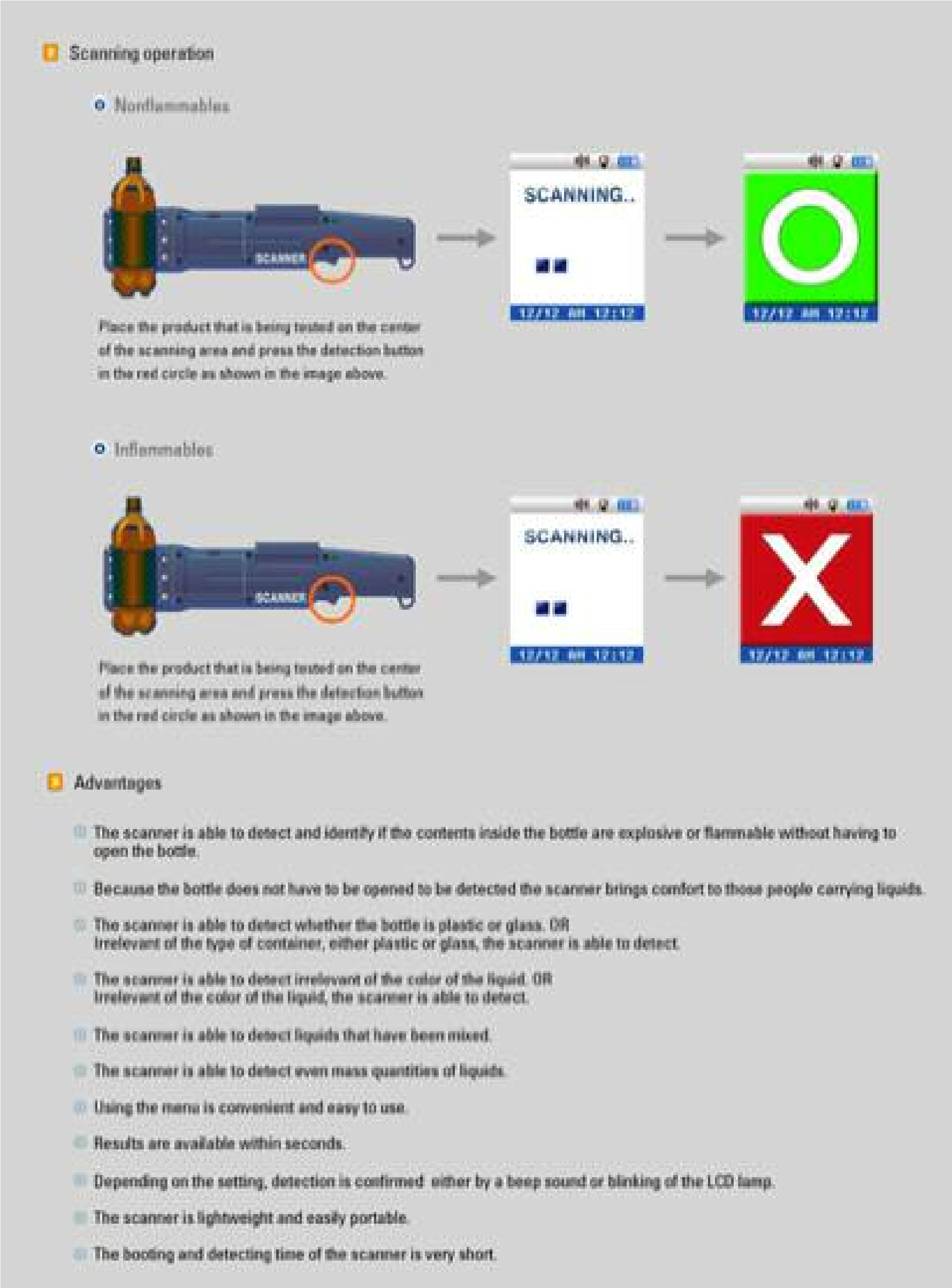
Introduction and Overview

Without the necessity of opening a bottle or sampling of contents, the SWEN R2 is able to scan transparent or opaque plastic bottles and easily identifies if the contents inside the bottles are flammable, explosive, potentially hazardous or dangerous.
This detector employs a microwave using GPR (Ground Penetrating Radar) to identify contents, which prevents users from being exposed to X-rays or other radiations and chemical substances to be carefully used.

This detector employs microwave to penetrate most objects thus even a very small quantity of flammable substance can be detected. Its superior CPU with the high speed performs the fast scanning within seconds. This simple operation of the SWEN R2 does not require additional personnel, thus labor costs could be kept at a minimum.



Description of components



Scanning operation

Nonflammables

SCANNER
SCANNING..
12/12 AM 12:12
12/12 AM 12:12

Place the product that is being tested on the center of the scanning area and press the detection button in the red circle as shown in the image above.

Inflammables

SCANNER
SCANNING..
12/12 AM 12:12
12/12 AM 12:12

Place the product that is being tested on the center of the scanning area and press the detection button in the red circle as shown in the image above.

Advantages

- The scanner is able to detect and identify if the contents inside the bottle are explosive or flammable without having to open the bottle.
- Because the bottle does not have to be opened to be detected the scanner brings comfort to those people carrying liquids.
- The scanner is able to detect whether the bottle is plastic or glass. OR
  Irrelevant of the type of container, either plastic or glass, the scanner is able to detect.
- The scanner is able to detect irrelevant of the color of the liquid. OR
  Irrelevant of the color of the liquid, the scanner is able to detect.
- The scanner is able to detect liquids that have been mixed.
- The scanner is able to detect even mass quantities of liquids.
- Using the menu is convenient and easy to use.
- Results are available within seconds.
- Depending on the setting, detection is confirmed either by a beep sound or blinking of the LCD lamp.
- The scanner is lightweight and easily portable.
- The booting and detecting time of the scanner is very short.

INERT PRODUCTS, LLC.

INERT EXPLOSIVE TRAINING PRODUCTS

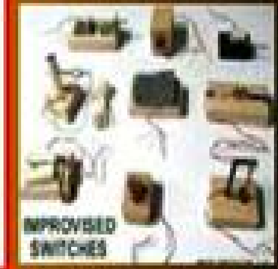
ALL SALES FOR OFFICIAL USE ONLY!
THE WORLD'S LEADING SUPPLIER OF
INERT TRAINING PRODUCTS & DEVICES...

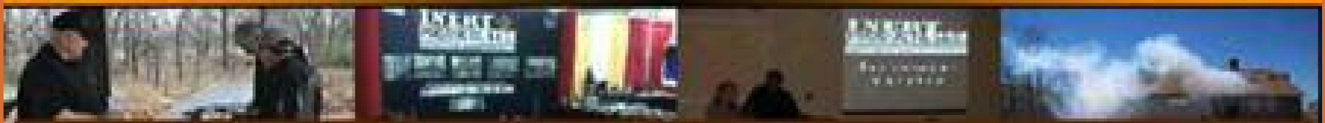
PRODUCTS

- New Products
- IED Training Kits
- IED Training Aids
- Replica Ordnance
- Inert Landmines / Mines
- Replica Grenades
- VBIED Training Aids
- Suicide Vests & Belts
- OPFOR
- Replica Dummy Guns
- Inert Ammunition
- RPG Replicas
- Inert Dynamite
- Detonators, Blasting Caps
- Inert Demolition Blocks
- Inert Detonating Cord
- Inert Shock Tube
- Inert Time Fuse
- Inert Plastic Explosives
- Inert Explosives Samples
- IED Training Posters
- Demolition Components
- Inert Shaped Charges
- IED Components
- IED Firing Devices
- Improvised Switches
- Display Boards
- Cut Aways (Cross Sections)
- Incendiary Devices
- Range Clearance
- Custom Products
- Courtroom Props
- DVDs / Books / Posters
- Tactical 3D Maps
- Clearance
- Movie, Film, & TV Props

INERT PRODUCTS, LLC. provides Law Enforcement, Homeland Security and the United States Department of Defence with extremely durable, highly realistic inert training aids used in training against terrorist threats.

Located in Scranton, PA, Inert Products, Llc produces and supplies support materials used by security forces in training to recognize, respond to, and mitigate the threat of explosives & terrorism.





http://www.inertproducts.com E-mail: Sales@inertproducts.com

Liquid explosives detector – Fast and accurate

Source:http://www.tradingmarkets.com/news/stock-alert/kub_japan-developed-liquid-explosive-detector-is-fast-and-accurate-1303544.html

In 2010, a research group from Osaka University has collaborated with Kubota Corp. (TSE:6326) in a government-backed project to develop a device for the swift and accurate detection of liquid explosives in glass and plastic containers. The prototype can accommodate containers as large as a 2-liter PET bottle, evaluating the contents in just 2-3 seconds and accurately detecting the presence of liquid explosives with a false-detection rate of less than 1 per cent. In addition to liquid explosives, the device can also identify flammable liquids like gasoline and other dangerous liquids such as acids and strong bases. If data is entered into the system ahead of time, the device can also identify beverages to the point of being able to name the specific products. The device works by shining near-infrared light up from below the container and measuring the light that reflects back. Different liquids absorb the near-infrared light in characteristic ways, so they can be identified by analyzing the waveforms of the light that reflects back out from the bottom of the container. The prototype device only works when liquid explosives are held in containers that allow the passage of near-infrared light — such as glass or plastic bottles — but the development team hopes to add functionality to also evaluate liquids held in metallic containers. The device was developed as part of a project supported by the Ministry of Education, Science and Technology. Soon the prototype will be tested at an airport, and the goal is to have a practical version ready soon that can be used in public facilities as a security measure against terrorism.

A New Breed

Scent Dog Program Gets Results

Source: http://www.fbi.gov/news/stories/2010/december/scent_122310/scent_122310

When an Anchorage, Alaska nurse went missing in 2007 and was found dead six weeks later, the FBI Laboratory's Evidence Response Team Unit (ERTU) was called in and asked to bring some experts—our specially trained human scent evidence canines Tinkerbelle, Lucy, and Casey. Following human scent trails from several places linked to the killing, the dogs kept ending up at the same location—the house of a man who lived near the victim.

The neighbor was eventually charged with the murder. In a pre-trial hearing his lawyer challenged the science behind the scent evidence and asked that it be thrown out. The judge ruled that the science was indeed sound, and fully admissible in court. Last February, the man pled guilty to the killing and was sentenced to life without parole.

Human scent evidence has been used in federal court before. However, the federal court judge's ruling sets an important precedent—and by extension acknowledges the Bureau's ef-

Photo Courtesy of Prof. Gary Settles, Penn State University forts to promote the highest standards when scent dogs are used in investigations.

The use of dogs by law enforcement is nothing new. Bloodhounds have traditionally been called upon to pick up the trail of fugitives and missing persons. FBI police and our special agent bomb technicians use dogs trained to sniff for explosives, and we have victim recovery dogs trained specifically to seek out the smell of blood and decomposing bodies.

But our Human Scent Evidence Team (HSET), established in 2002 and now a full-time program in the ERTU, is something of a new breed. After they are trained and certified—a process that can take two to three years—HSET dogs can help point investigators in the right direction when time and resources may be in limited supply—and their efforts may later be scrutinized in the courtroom.

Here's how the program works:

At the crime scene, in addition to collecting fingerprints, DNA, and other evidence, ERT technicians collect scents by using a trace evidence vacuum similar to those used for collection of hair and fibers. Human scent traces, which can be obtained from almost any object, are vacuumed onto a sterile surgical dressing and placed in an airtight glass jar (they can be stored that way for an extended period of time).

Dogs are trained to smell the collected scent by sniffing the scent pad and indicating either a scent match or a non-match. If there is a matching trail of human odor, the dog will follow an invisible "odor highway" in the same way humans might recognize streets, roadways, and intersections.

In most cases handlers know nothing about the cases they are called in to work. They are simply given a scent pad and asked to follow a trail if one is found.

Stockham is working with the Department of Homeland Security and other agencies to establish a uniform set of training and certification standards that would apply to all scent dogs used in investigations.

"Our goal is to promote a science-driven program with the highest standards of training, certification, and professionalism," Stockham explained. "It's part of the FBI Laboratory's commitment to provide exceptional forensic science services to our federal, state, local, and international law enforcement partners."

Liquid explosives' detection by Smiths Detection

Source: http://www.smithsdetection.com/

HEIMANN X-RAY INSPECTION SYSTEM
Feature highlights

- Dual view X-ray inspection system
- Upgradeable to full capability of automatic explosives detection system HI-SCAN 6040aTiX
- X-ray generator with optimized spectrum
- High resolution XADA sensor technology
- Additional highlights
- Fully integratable in networks for system management, archiving, image distribution and TIP functionalities

HI-SCAN 6040aX is an advanced baggage scanner which has recently gained EU Liquid Explosive Detection Systems (LEDS) Standard 1 Type C approval and allows explosives and liquids detection at security checkpoints. HI-SCAN 6040aX is a state-of-the-art dual-view X-ray inspection system that uses independent multi-energy generators. The system's basic security system concept addresses requirements to adapt to future threat scenarios respectively regulatory frameworks and facilitates in-field upgrades to a full 4-view automated explosives and liquid detection system HI-SCAN 6040aTiX, retaining the footprint unchanged. HI-SCAN 6040aX utilizes latest high performance EDS detection technology. The operating concept of the proven HI-SCAN series has been retained which guarantees an optimum passenger throughput at checkpoints. The two detailed views (Dual View) available to facilitate manual analyses support a quick and reliable evaluation process.

BOTTLE LIQUID SCANNER
Feature highlights

- Can easily scan clear, translucent and frosted unopened glass or plastic bottles
- Quick analysis time of 20 seconds
- Uses low energy powered laser <100mW
- Easy to understand results: Potential Threat / No Threat

The RespondeR Bottled Liquid Scanner (BLS) is a desktop system that can accurately distinguish threat liquids from benign liquids in unopened glass and plastic bottles, regardless if they are clear, translucent or frosted. The ability to screen liquids in sealed bottles reduces inspection time, increasing throughput while screening for potential threats. The RespondeR BLS utilizes field- and lab-proven Raman Spectroscopy technology, also in the RespondeR RCI used by emergency responders worldwide. The RespondeR BLS features a touch screen display with a simple user interface. Bottles are placed inside a safety enclosure where its contents are scanned with a 785-nm near infrared laser source. The safety enclosure is designed to protect the operator and public from exposure to the laser. The scan and analysis are completed within 20 seconds with results compared to the onboard threat library, which contains an assortment of different chemical substances that could be used in the creation of a homemade or liquid explosive device. The standard library can be easily modified as threats change. If no threat is detected, the display reads “NO THREAT FOUND” in green and the next bottle can immediately be scanned. If a match is made to a chemical in the library, the display reads “POTENTIAL THREAT FOUND” in red. In this case, the operator can refer the person for additional screening and continue with his duties, or he can perform an optional secondary scan. The secondary scan is completed in less than two minutes and displays the name of the potential threat, which is vital for determining how to proceed with a confirmed threat substance or clearance of a nuisance alarm. Alarms are stored on the internal computer and can be exported via USB memory device. Applications include security checkpoints at airports, special events, high-profile facilities and at building entrances.

MULTI-MODE THREAT DETECTOR
Feature Highlights

- Hand-held, hardened detector for extreme conditions
- Explosives, narcotics and CWA/TIC detection and identification in one instrument
- Simultaneous dual mode detection of explosives and narcotics from a single sample
- Increased range of explosive detection, including optimization for peroxides and taggants
- Intuitive, easy to use interface using a Windows® CE based platform
- Remote, unattended operation capability
- Unlimited data storage via SD memory card

- Up to 5 hours of uninterrupted operation with hot-swappable battery
- Integrated USB
- Wi-Fi Ethernet

The Multi-Mode Threat Detector (MMTD) is a rugged, portable hand-held system for the rapid detection and identification of explosives, narcotics or CWA/TICs featuring an optimized detection capability for peroxides, taggants and methamphetamine precursors. Additionally, a dual mode setting allows for the simultaneous detection of explosives and narcotics from one sample. With a quick switch, operators can select either particle or vapor analysis methods to utilize the best method for detecting the suspected threat. Designed to IP54 rating for operation in extreme environmental conditions, the MMTD takes portable threat detection to a new level without compromising portability or functionality. Other features include up to 5 hours of uninterrupted operation with the two hot-swappable batteries (included), remote, unattended operation for one or more units with alarm and status information reported to Command & Control via Wi-Fi Ethernet, unlimited data storage via SD card and exporting results via USB port. With the included software, advanced operators can perform more in-depth data analyses and print results, all via network connection. The MMTD is powered by Smiths Detection proven and trusted IMS technology, used by the military, law enforcement and government agencies.

SABRE 4000

- Hand-held trace detector for explosives, chemical agents, toxic industrial chemicals or narcotics
- Smallest, lightest Tri-Mode (Explosives, Narcotics, CW/TICs) detector available
- Proven IMS technology for sensitivity & accuracy
- Over 40 threat substances identified in seconds
- Particle and vapor sampling

The SABRE 4000 is the only portable trace detector that can detect threats from explosives, chemical warfare agents, toxic industrial chemicals or narcotics, and can do so in approximately 20 seconds. With a start time of 15 minutes and weighing approximately 7 lbs. including the 4-hour battery, the SABRE 4000 is a small, powerful ally in the war on terror and drug trafficking. The SABRE 4000 is the smallest, lightest hand-held tri-mode trace detector available.

SABRE EXV
Feature Highlights

- Immediate alert and identification of volatile explosives including peroxides and taggants
- Simultaneous detection of both negative and positive explosives in a single sample
- Complete analysis and result in 10 seconds
- Weighs 7 lbs. with battery
- 180° screen inversion option (for fixed use)
- 3.5” color TFT displays
- Battery life up to 8 hours
- Options
- Desktop cradle for fixed use
- Protective carrying case

Common chemicals used in households cleaning products or in manufacturing processes can also be used to construct devastating Improvised Explosive Devices (IEDs). These peroxide-based explosives are extremely volatile and unstable. The SABRE EXV uses Smiths Detection's proven Ion Mobility Spectrometry (IMS) technology to detect and identify these volatile explosives substances in low ppm to ppb quantities. The operator simply holds an item such as a bag, box, or container in front of the sample nozzle and within 10 seconds, the analysis result will be shown on an easy-to-read, color display. The portable SABRE EXV system operates up to 8 hours on a fully charged battery. It can be connected to a PC for data viewing and programming using Instrument Manager (IM32) software. Although it is designed for portable use, an optional desktop cradle is available for fixed use.

Thermoses Could Be Used As Bombs

Source: http://www.nationalterroralert.com/2010/12/26/tsa-public-notice-thermoses-could-be-used-as-bombs/?utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+NationalTerrorAlertResourceCenter+%28National+Terror+Alert+Response+Center%29&utm_content=Yahoo!+Mail

Passengers may observe additional security measures related to insulated beverage containers. TSA is carefully monitoring information related to terrorist tactics and working with our international partners to share information and security best practices. The possible tactics terrorists might use include the concealment of explosives inside insulated beverage containers, so in the coming days, passengers flying within and to the U.S. may notice additional security measures related to insulated beverage containers. While such items are not being banned from travel, TSA Officers have been trained to detect a variety of threats including the concealment of explosives in common items. TSA will continue to deploy risk-based security measures and work with our international, federal, state, local and private sector partners to protect the traveling public. As always, the safety and security of the American people is our highest priority and we ask the public to remain vigilant and aware of their surroundings and report any suspicious activity to their local authorities.

FAQ's

Q. Why is TSA issuing this notice now?

A. TSA is carefully monitoring information related to terrorist tactics and working with our international partners to share information and security best practices. The possible tactics terrorists might use include the concealment of explosives inside insulated beverage containers.

Q. If there is no specific threat, why is TSA issuing a notice?

A. TSA is carefully monitoring information related to possible methods of attack. We will continue to deploy risk-based security measures and work with our international, federal, state, local and private sector partners to protect the traveling public.

Q. Are thermoses/insulated beverage containers now prohibited in carry-on or checked baggage?

A. At this time, insulated beverage containers are permitted in carry-on and checked baggage. TSA liquid policy still applies at the checkpoint.

Q. If thermoses/insulated beverage containers pose a threat, why aren't they prohibited?
A. TSA makes risk-based decisions and our officers have been trained to detect a variety of threats including the concealment of explosives in common items. We have also shared this information with our stakeholders and foreign partners.

Q. If liquids are already prohibited, why are these measures being put in place?
A. These measures apply to empty, insulated beverage containers at the checkpoint. 3-1-1 rules for liquids remain in effect.

Q. What changes can the traveling public expect?
A. Passengers traveling with insulated beverage containers can expect to see additional screening of these items using procedures currently in place, including X-ray screening, physical inspection and the use of explosives trace detection technology.

Q. Is TSA implementing new security measures related to this notice?
A. TSA is continuing to deploy risk-based security measures based on the latest intelligence to protect the traveling public. Passengers traveling with insulated beverage containers can expect to see additional screening of these items using procedures currently in place, including X-ray screening, physical inspection and the use of explosives trace detection technology.

Q. What happens if an insulated beverage container alarms while being screened?
A. As is currently the case, any item that alarms while undergoing X-ray screening will receive additional screening, to include the use of explosives trace detection technology. If TSA Officers are unable to resolve a alarm, the item will not be permitted on board the plane.

Q. How long will this measure remain in place?
A. This measure is designed to be sustainable. TSA will continuously review this measure to ensure the highest levels of security.

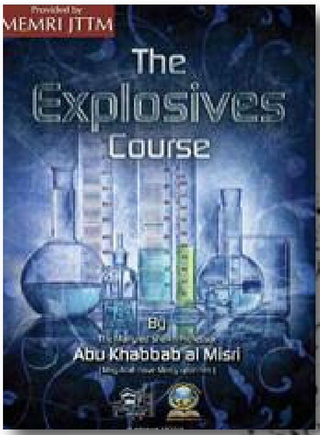
Q. Do these new measures apply to all personal liquid containers?
A. The notice is based on intelligence and specific to insulated beverage containers.

Al-Qaeda publishes explosives course in English

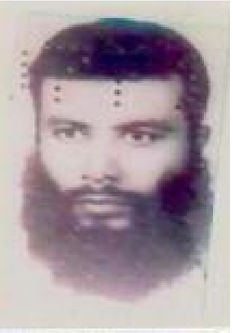
Source: http://www.memri.org/report/en/0/0/0/0/0/0/4885.htm

On December 29, 2010, the Al-Qaeda-affiliated media center Global Islamic Media Front and the Dar Al-Jabha publishing house electronically published an English-language book titled The Explosives Course. Links to download the book were posted on jihadi forums such as Shumukh Al-Islam and the Ansar Al-Mujahideen English forum, with jihadist sympathizers also posting links on Facebook.

In its introduction, the book states that it was compiled and written by students of Abu Khabab Al-Masri, the nom de guerre of Midhat Mursi Al-Sayid 'Umar, the Al-Qaeda chemistry and explosives expert who was killed in a drone attack in Pakistan in 2008. The book was approved for publication by Sheikh Ahmed Salim Sweidan, a senior Al-Qaeda operative killed in a 2009 drone attack in Pakistan.



The book is essentially a detailed, step-by-step guide to bomb manufacturing processes, replete with charts, illustrations, and diagrams. In the introduction, the authors state that their goal in writing the book was to provide: «(1) step by step guidance [in the] purification of common commercial chemicals – which are available in [local] markets and (2) the detailed practical observations/notes [of experts] in the preparation of these explosives.» Regarding their target audience, the authors wrote: «This book is [intended] for brothers [i.e., fellow mujahideen] who have a sufficient understanding of the risks [involved] in this [i.e. the manufacture of homemade bombs] – both [of] the actual sensitive task of making explosives and of its security risks [i.e. the risk of being caught and imprisoned]. It is said that in explosives 'your first mistake is your last mistake' – and this is true for both situations.»



Midhat Mursi al-Sayid Umar, aka Abu Khabab Al-Masri

The authors add that anyone who is considering carrying out an operation using the book as a guide should first obtain religious approval from an Islamic scholar and should ensure that the operation will serve the general interests of the mujahideen: «Note: ...Any operation based on this book should be based upon [shari'a] approval and maslahah [interest] of the mujahideen.»

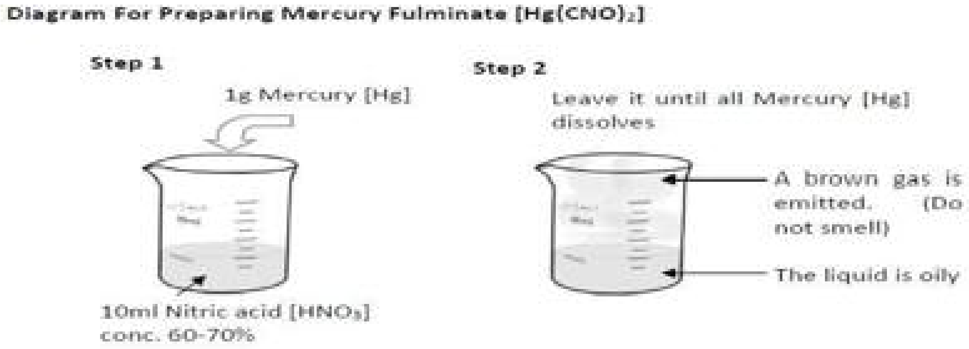


Diagram For Preparing Mercury Fulminate [Hg(CNO)₂]
Step 1
1g Mercury [Hg]
10ml Nitric acid [HNO₃] conc. 60-70%
Step 2
Leave it until all Mercury [Hg] dissolves
A brown gas is emitted. (Do not smell)
The liquid is oily

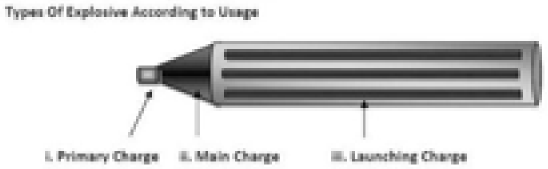
The 102-page book is divided into three main sections:

1. Laboratory: This section deals with the logistics, safety precautions, and administrative procedures of working in the explosives laboratory.

2. Chemistry: This section is essentially a 12-page crash course in chemistry, covering basic topics such as the composition of atoms, the periodic table, etc.

3. Manufacturing.

The last section comprises the core of the book and is an extensive guide to the manufacture of homemade bombs. It contains explanations of the following topics: primary charges (including detonators and fuses), main charges, launching charges, and high temperature explosives (including burning, light, and smoke bombs). The introduction to this chapter lists the various types of explosives and explains the basic principle behind building a bomb. This section also discusses where bomb ingredients can be purchased locally, or how to produce them in the laboratory. Numerous diagrams and sketches illustrate how to make various homemade explosive devices, such as Molotov cocktails, napalm bombs, thermite bombs, and smoke bombs, using readily available materials.



The book, translated from Arabic, is in fairly readable English and has undergone extensive editing and design. Abu Khabab Al-Masri is known to have written Al-Qaeda's explosives manual, and it is possible that the book is a direct translation of this manual. The book's authors claim to have carried out tests in order to verify the accuracy of the information they provide. They add that they have already developed further methods of bomb manufacture, which they intend to release in other, more detailed books in the future.

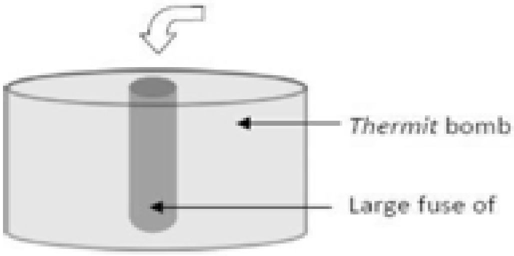


Diagram of a homemade thermite bomb

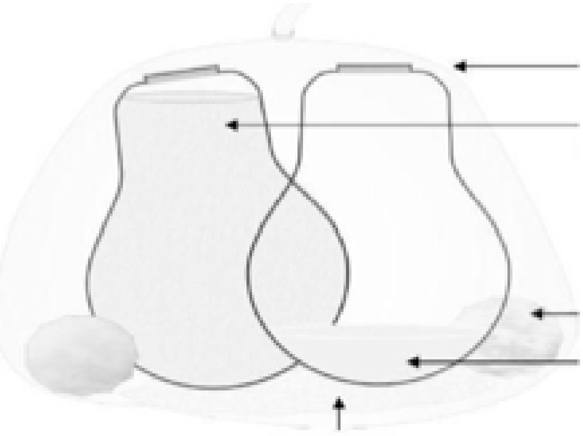


Illustration of a homemade napalm bomb

The publication of such a book in English has important ramifications. First, it is another example of the use of the Internet to disseminate terrorist methods to individuals and cells throughout the world. More significantly, the publication of this book in English marks an escalation in Al-Qaeda's efforts to encourage jihadists living in Western countries to carry out attacks there, and to provide them with the know-how needed to do so. The recent suicide-attack attempt by Swedish citizen Taimour Abdulwahab Al-Abdaly in Stockholm and the wave of arrests of suspected terrorists in Britain and the Netherlands are all evidence of the gravity of this threat.

EDITOR'S NOTE: It seems that the above edition is more modernized and specialized regarding explosives, than the older "*Encyclopedia of Jihad*" (1620 pages – Chapter 6)

The Encyclopaedia of Jihad

Source: http://www.washingtonpost.com/wp-dyn/content/custom/2005/08/05/CU2005080501351.html

The Encyclopaedia of Jihad, written in Arabic, is a lengthy textbook for jihadist-in-training, with religious messages and information on building explosive devices, conducting assassinations and communicating secretly.

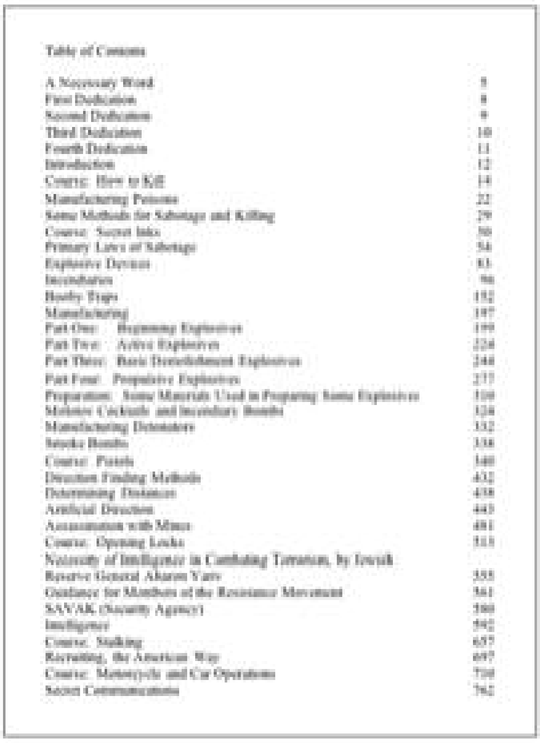
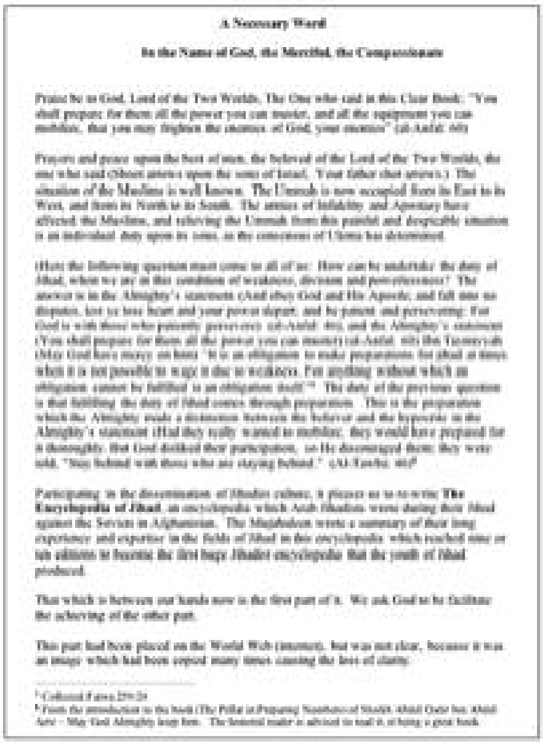


Table of Contents



A Necessary Word

In the Name of God, the Merciful, the Compassionate

Praise be to God, Lord of the Two Worlds, The One who said in this Clear Book: "You shall prepare for them all the power you can muster, and all the equipment you can mobilize, that you may frighten the enemies of God, your enemies" (al-Anfal: 60)

Prayers and peace upon the best of men, the beloved of the Lord of the Two Worlds, the one who said (Shoot arrows upon the sons of Ismail. Your father shot arrows.) The situation of the Muslims is well known. The Ummah is now occupied from its East to its West, and from its North to its South. The armies of Infidelity and Apostasy have affected the Muslims, and relieving the Ummah from this painful and despicable situation is an individual duty upon its sons, as the consensus of Ulema has determined.

(Here) the following question must come to all of us: How can he undertake the duty of Jihad, when we are in this condition of weakness, division and powerlessness? The answer is in the Almighty's statements (And obey God and His Apostle, and fall into no disputes, lest ye lose heart and your power depart; and be patient and persevering: For God is with those who patiently persevere) (al-Anfal: 46), and the Almighty's statement (You shall prepare for them all the power you can muster) (al-Anfal: 60). Ibn Taymiyyah (May God have mercy on him) "It is an obligation to make preparations for jihad at times which it is not possible to wage it due to weakness. For anything without which an obligation cannot be fulfilled is an obligation itself."[1] The duty of the previous question is that fulfilling the duty of Jihad comes through preparation. This is the preparation which the Almighty made a distinction between the believer and the hypocrite in the Almighty's statement (Had they really wanted to mobilize, they would have prepared for it thoroughly. But God disliked their participation, so He discouraged them: they were told, "Stay behind with those who are staying behind." (Al-Tawba: 46)[2]

Participating in the dissemination of Jihadist culture, it pleases us to re-write **The Encyclopedia of Jihad**, an encyclopedia which Arab Jihadists wrote during their Jihad against the Soviets in Afghanistan. The Mujahideen wrote a summary of their long experience and expertise in the fields of Jihad in this encyclopedia which reached nine or ten editions to become the first huge Jihadist encyclopedia that the youth of Jihad produced.

That which is between our hands now is the first part of it. We ask God to facilitate the achieving of the other part.

This part had been placed on the World Web (internet), but was not clear, because it was an image which had been copied many times causing the loss of clarity.

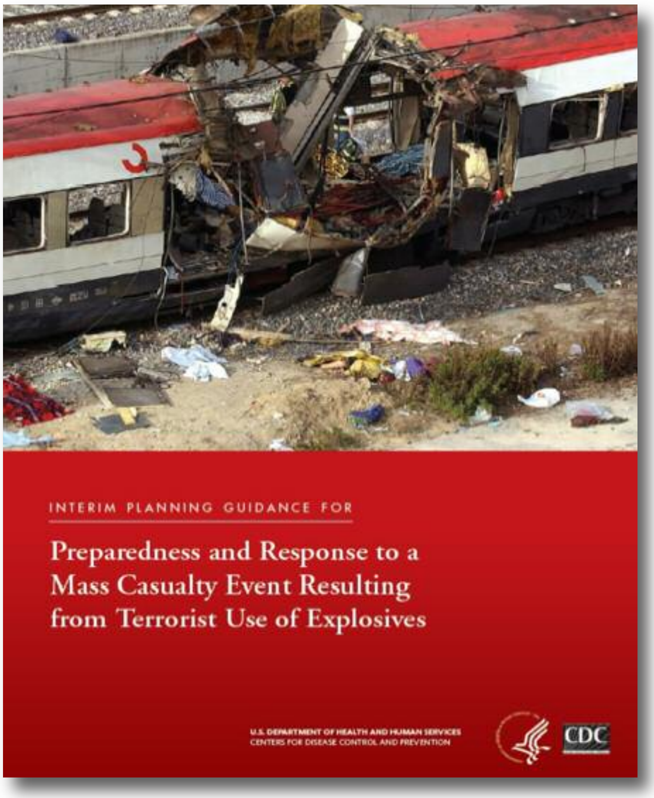
[1] Collected Fatwa 259/28

[2] From the introduction to the book (The Pillar in Preparing Numbers) of Sheikh Abdul Qadir bin Abdul Aziz – May God Almighty keep him. The honored reader is advised to read it, it being a great book.

Preparedness and Response to a Mass Casualty Event Resulting from Terrorist Use of Explosives

National Center for Injury Prevention and Control. Atlanta, GA: Centers for Disease Control and Prevention; 2010.

Explosive devices are the most common weapons used by terrorists. The damage inflicted in recent events in India, Pakistan, Spain, Israel, and the United Kingdom demonstrates the impact of detonating explosives in densely populated civilian areas. Explosions can produce instantaneous havoc, resulting in numerous patients with complex, technically challenging injuries not commonly seen after natural disasters. Because many patients self-evacuate after a terrorist attack, prehospital care may be difficult to coordinate and hospitals near the scene can expect to receive a large influx, or surge, of patients after a terrorist strike.



INTERIM PLANNING GUIDANCE FOR

Preparedness and Response to a Mass Casualty Event Resulting from Terrorist Use of Explosives

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
CENTERS FOR DISEASE CONTROL AND PREVENTION

CDC

The threat of terrorism exists at a time when hospitals in the United States are already struggling to care for patients who present during routine operations each day. Hospitals and emergency health care systems are stressed and face enormous challenges. With the occurrence of a mass casualty event (MCE), health systems would be expected to confront these issues in organization and leadership, personnel, infrastructure and capacity, communication, triage and transportation, logistics, and legal and ethical challenges.

The purpose of this interim guidance is to provide information and insight to assist public policy and health system leaders in preparing for and responding to an MCE caused by terrorist use of explosives (TUE). This document provides practical information to promote comprehensive mass casualty care in the event of a TUE event and focuses on two areas:

1. leadership in preparing for and responding to a TUE event, and

2. effective care of patients in the prehospital and hospital environments during a TUE event.

3 Interim Planning Guidance for Preparedness and Response to a Mass Casualty Event Resulting from Terrorist Use of Explosives

This guidance recognizes the critical role that strategic leadership can have on the success or failure of preparing for and responding to a terrorist bombing. It outlines important leadership strategies for successfully preparing for and managing a TUE mass casualty event, including the concept of meta-leadership. Effective meta-leaders employ influence over authority and activate change above and beyond established lines of their decision-making and control. They are driven by a purpose broader than that prescribed by their formal roles. Therefore, they are motivated and act in ways that transcend usual organizational confines, enabling them to successfully confront challenges and barriers in communication, organization and response, standards of care, and surge capacity.

The successful medical response to an MCE depends on effectively coordinating three critical areas of patient care: 1) prehospital care, 2) casualty distribution, and 3) hospital care. Critical steps must be taken throughout the response to ensure rapid and efficient patient triage, effective and appropriate distribution of patients to available hospitals and health care facilities, and proper management of the surge of patients at receiving hospitals.

Materials for fertilizer bombs not regulated

Source: http://homelandsecuritynewswire.com/materials-fertilizer-bombs-not-regulated

Mixtures of ammonium nitrate and fuel oil (ANFO) are used in about 80 percent of all explosives used in North America each year, mostly in the mining and demolition industries; they were also used by Timothy McVeigh in Oklahoma City, and in insurgents' IEDs in Iraq and Afghanistan; explosives-grade ammonium nitrate can be refined from commercial-grade fertilizers using processes readily found online; there are even YouTube videos that break down the process step by step; commercial grade fertilizers are not regulated; those states that address the issue typically require merchants to keep records of who buys what, but there are no limitations on who can buy what and no reporting requirements. Mixtures of ammonium nitrate and fuel oil (ANFO as it is known in the explosives trade) are considered high explosives in most contexts and account for approximately 80 percent of all explosives used in North America each year, mostly in the mining and demolition industries. It is also remarkably easy to produce with the proper ingredients, namely ammonium nitrate, one of the most common fertilizers found in the United States, and a fuel oil — the diesel fuel found at most gas stations being one of the most common. Neither of these items are illegal to buy, possess, or transport in the United States. For these reasons it is the explosive Timothy McVeigh loaded into his truck when he drove to downtown Oklahoma City and detonated it near the Murrah Federal Building. The resulting blast was the largest terrorist attack on the United States at the time, surpassed only by the terrorist attacks of 9/11, killing 160 people and injuring almost 700. This bombing, however, was not the first of its kind, even on U.S. soil. The same explosive was used in the 1993 bombing of the World Trade Center. More recently it is what terrorists and al Qaeda operatives often use in Iraq and Afghanistan for IEDs and truck bombs. When used in these contexts, ANFO explosives are known as fertilizer bombs. This popularity and ease of creation do not mean one can create a bomb by soaking a bag of fertilizer found at the local garden store in diesel fuel, because bombs require high grade ammonium nitrate. This explosives grade ammonium nitrate, however, can be refined from commercial grade fertilizers using processes readily found online. There are even YouTube videos that break down the process step by step. These commercial grade fertilizers are not regulated in most cases and there are no federal laws regulating their sale or purchase. While some states do choose to exercise their regulatory powers, laws can differ greatly from state to state, and some states do not have any regulation. Even in states where regulations exist, almost anyone can buy commercial grade fertilizer. Some states require vendors of commercial grade fertilizer to register with the state, but this requirement does not limit whom they may sell to. Many of the regulations only require the purchaser to show a drivers license and have the information recorded and kept on file by the retailer at the time of purchase, but this information is only helpful after an attack has occurred as there is no required reporting of sales. Fortunately

many local law enforcement agencies maintain amicable relationships with shopkeepers who will inform the police of a person they are unfamiliar with buying large amounts of commercial grade fertilizer. This, however, does depends on the shopkeeper being aware of the potential dangers and choosing to make the phone call. It can be expected that many high school or college students working part time at a retailer would not make the connection to call the police. Besides fertilizers, ammonium nitrate can be refined from the cold packs that can be bought at sporting goods or grocery stores. The concentrations of ammonium nitrate in these products, however, are low and would require approximately 450 pounds of cold packs to make a small bomb — and buying 450 pounds of cold packs would likely raise suspicions. In addition to high quality ammonium nitrate and fuel oil, an ANFO or fertilizer bomb usually requires a booster such as dynamite, to start the explosion.

Leuitant Adam Shiner of the Nassau County Emergency Services Unit Contributed to this article.

New bomb detection tool: Ferns

Source: http://homelandsecuritynewswire.com/new-bomb-detection-tool-ferns

Researchers engineered fern proteins to turn airport plants into bomb detectors; the researchers rewrite the fern's natural signaling process so the plant turns from green to white when chemicals are detected in air or soil. Professor June Medford and her team in the Department of Biology at Colorado State University, enabled a computer-designed detection trait to work in a plant by rewiring its natural signaling process so the plant turns from green to white when chemicals are detected in air or soil. This work — an important step in a long process - could eventually be used for a wide range of applications such as security in airports or shopping malls, or monitoring for pollutants such as radon in a home. "The idea to make detector plants comes directly from nature," Medford said. "Plants can't run or hide from threats, so they've developed sophisticated systems to detect and respond to their environment. We've 'taught' plants how to detect things we're interested in and respond in a way anyone can see, to tell us there is something nasty around." The research appeared yesterday in the peer-reviewed journal PLoS ONE. Financial support for the research was provided by the Defense Advanced Research Projects Agency, or DARPA, the Office of Naval Research, the Bioscience Discovery Evaluation Grant Program through the Colorado Office of Economic Development and International Trade, the National Science Foundation, Department of Homeland Security Science, and Technology Directorate and Gitam Technologies. June Medford and postdoctoral researcher Peter Bowerman analyze the emergence of the next generation of plant sentinels. "Plant sentinels engineered to detect explosives may ultimately help us protect our troops from improvised explosive devices (IEDs)," said Linda Chrisey, program officer for the Naval Biosciences and Biocentric Technology Program at the Office of Naval Research. Medford and her team also recently received a 3-year, $7.9 million grant from the Defense Threat Reduction Agency in the U.S. Department of Defense to take the discovery described in PLoS ONE from her CSU research laboratory to the "real-world." Based on research so far, detection abilities of these plants are similar to or better than those of dogs, Medford said. The detection traits could be used in any plant and could detect multiple pollutants at once — changes that can also be detected by satellite. “Dr. Medford’s research illustrates that basic changes in scientific understanding can be applied to important problems such as environmental protection and homeland security,” said Bill Farland, vice president for Research at Colorado State and formerly top scientist at the Environmental Protection Agency. Computational design of Medford’s detection trait was initially done in collaboration with Professor Homme Hellinga at Duke University and more recently with Professor David Baker at the University of Washington.

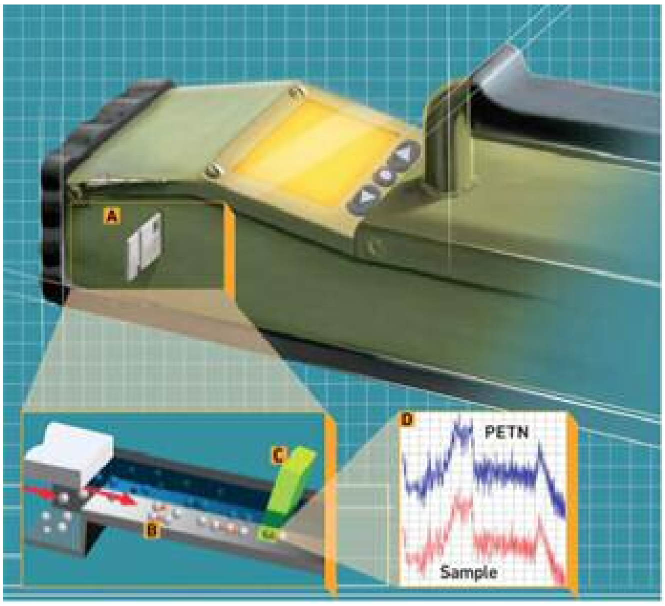
How the technology works

The Baker and Hellinga laboratories used a computer program to redesign naturally occurring proteins called receptors. These re-designed receptors specifically recognize a pollutant or explosive. Medford’s lab then modifies these computer redesigned receptors to function in plants, and targets them to the plant cell wall where they can recognize pollutants or explosives in the air or soil near the plant. The plant detects the substance and activates an internal signal that causes the plant to lose its green color, turning the plants white. Moving forward, Medford will use her team of some thirty undergraduate and graduate students and post-doctoral fellows to focus on such factors as speeding up detection time. The initial or first-generation plants respond to an explosive in hours, but improvements are underway to reduce the response time to a few minutes.

Portable bomb-sniffing device could keep explosives off planes

Source: http://homelandsecuritynewswire.com/portable-bomb-sniffing-device-could-keep-explosives-planes

The same way the aroma of freshly baked cookies fills a kitchen, a hidden bomb usually sheds trace amounts of chemicals into the air; new detection device is capable of sensing explosives’ vapor at parts per trillion; «We’re gonna give [dogs]a run for their money,» says the vice president of SpectraFluidics, the manufacturer. When the underwear bomber passed through security last Christmas, no one noticed the three ounces of PETN, one of the most reactive explosives, stuffed in his pants. Now a new portable chemical detector, capable of sensing explosives’ vapor at parts per trillion, could uncover this and other chemical threats at airports. The same way the aroma of freshly baked cookies fills a kitchen, a hidden bomb usually sheds trace amounts of chemicals into the air. Popular Science reports that the device, developed by SpectraFluidics, sucks in these telltale chemicals and traps them in microscopic water channels. A laser zaps the molecules, causing them to vibrate and reemit the light in a signature pattern, which a built-in computer compares with a library of known substances’ patterns. In addition to PETN, it can identify less than a nanogram of other explosives, such as ammonium nitrate and nitroglycerine, as well as cocaine, says Casey Hare, SpectraFluidics’s vice president of systems engineering. Future applications of the tech could include detecting roadside bombs, food contaminants and cancer markers. But currently the company is testing the device with the U.S. Army, aiming to get a



$50,000, brick-size product to the Transportation Security Administration for field-testing by early next year. “Our tool is like an incredibly effective dog nose,” Hare says. “Dogs are the best detector of airborne particles that we have, but they’re not 100 percent infallible. We’re gonna give them a run for their money.”

Hide and Seek: One of the most difficult substances to detect in air is PETN. It has a very low vapor pressure, so few particles of it evaporate and become airborne. Blanddesigns.com

How to Sniff Out Bombs

1. The security agent plugs the microfluidics chip [A], which lasts for eight hours, into the detector and turns it on.

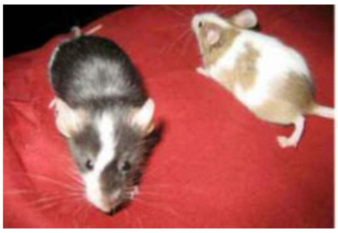
2. The agent uses the device to suck in air from around a suspicious object and run it over the chip’s water-filled microchannels.

3. Molecules dissolve in the water and bind with the metallic nanoparticles [B], which focus a laser [C] onto them. This causes the molecules to vibrate and emit light based on their unique structural properties.

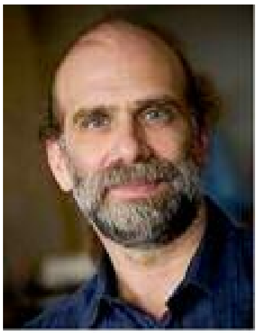
4. The spectrometer analyzes the light patterns [D], and an onboard computer matches them to known chemical signatures, flashing an alert to the agent if it senses explosives or drugs.

New explosives detectors: sniffer mice

Source: http://homelandsecuritynewswire.com/new-explosives-detectors-sniffer-mice



An Israeli company is training mice to sniff explosives; mice beat dogs for olfactory talent, and by much more than a nose: dogs have 756 olfactory receptor genes, while mice have 1,120, resulting in a more acute sense of smell; unlike dogs, which are often trained for explosives and drugs detection, mice do not require constant interaction with their trainers or treats to keep them motivated There is a new approach to explosives detection: sniffer mice. The critters are part of a bomb-detecting unit created by Israeli start-up company BioExplorers, based in Herzeliya, which claims that trained mice can be better than full-body scanners and intrusive pat-downs at telling a bona fide passenger from a terrorist carrying explosives. Eran Lumbroso conceived the mouse-based explosives detector while serving as a major in the Israeli navy. Along with his brother, Alon, he founded the company and built a device that looks much like an average airport metal detector or full-body scanner. New Scientist reports that along one side of an archway, a detection unit contains three concealed cartridges, each of which houses eight mice. During their 4-hour shifts in the detector, the mice mill about in a common area in each cartridge as air is passed over people paused in the archway and through the cartridge. When the mice sniff traces of any of eight key explosives in the air, they are conditioned to avoid the scent and flee to a side chamber, triggering an alarm. To avoid false positives, more than one mouse must enter the room at the same time. “It’s as if they’re smelling a cat and escaping,” Eran says. “We detect the escape.” Unlike dogs, which are often trained for explosives and drugs detection, mice do not require constant interaction with their trainers or treats to keep them motivated. As a result, they can live in comfortable cages with unlimited access to food and water. Each mouse would work two 4-hour shifts a day, and would have a working life of eighteen months. What is more, mice beat dogs for olfactory talent, and by much more than a nose: dogs have 756 olfactory recepto



genes, while mice have 1,120, resulting in a more acute sense of smell. Attacks such as the recent bombing of Domodedovo airport in Moscow, Russia, are fuelling interest in exploring new methods for keeping travelers safe. Low-tech alternatives may appeal to people who fear new full-body scanners are exposing them to harmful radiation and invading their privacy. “Animals’ noses are always a good solution, and the mice don’t see you naked,” says Bruce Schneier, who runs the blog Schneier on Security. Schneier adds, however, that there are drawbacks that could prevent their widespread use. For instance, their cages need regular cleaning, and new mice would have to be trained all the time because of their short working life. While useful for explosives, they could never replace current baggage scanners and metal detectors. Nonetheless, the company ran its first field test in December last year at Azrieli Center, a large shopping mall in Tel Aviv. More than 1,000 people passed through the detector, twenty-two of whom were asked to hide mock explosives in pockets or under shirts. All twenty-two packages were detected, the Lumbrosos claim, adding that the false-alarm rate was less than 0.1 percent.

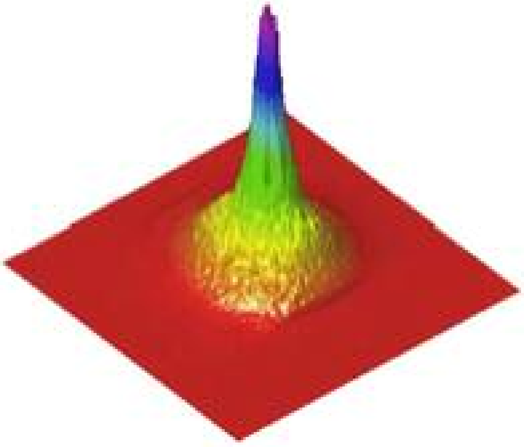
Moth in explosives detection

Moths have an exquisite sense of smell, so their ability to sniff out improvised explosive devices was recently tested by Andrew Myrick and Tom Baker at Pennsylvania State University in University Park. The team built a detector using four live moths which were immobilized in thin, aerated tubes. Different chemicals produce distinct voltages on the antennae that the moths use to sense aromas, so the team wired up the moths to record these levels. Software inferred the explosive source’s direction and distance based on the strength of signals coming from the insects. The detector was then able to home in on it to within twenty centimeters from twenty-three meters away.

Air laser will sniff bombs, pollutants from great distance

Source:http://homelandsecuritynewswire.com/air-laser-will-sniff-bombs-pollutants-great-distance? page=0,1

Princeton University engineers have developed a new laser-sensing technology that may allow soldiers to detect hidden bombs from a distance and scientists better to measure airborne environmental pollutants and greenhouse gases; the new technique differs from previous remote laser-sensing methods in that the returning beam of light is not just a reflection or scattering of the outgoing beam; it is an entirely new laser beam generated by oxygen atoms whose electrons have been «excited» to high energy levels. Princeton University engineers have developed a new laser-sensing technology that may allow soldiers to detect hidden bombs from a distance and scientists better to measure airborne environmental pollutants and greenhouse gases. “We are able to send a laser pulse out and get another pulse back from the air itself,” said Richard Miles, a professor of mechanical and aerospace engineering at Princeton, the research group leader and co-author on the paper. “The returning beam interacts with the molecules in the air and carries their fingerprints.” The new technique differs from previous remote laser-sensing methods in that the returning beam of light is not just a reflection or scattering of the outgoing beam. It is an entirely new laser beam generated by oxygen atoms whose electrons have been “excited” to high energy levels. This “air laser” is a much more powerful tool than previously existed for remote measurements of trace amounts of chemicals in the air. The researchers, whose work is funded by the Office of Naval Research, published their new method 28 January in the journal Science. Miles collaborated with three other researchers from Princeton's Department of Mechanical and Aerospace Engineering: Arthur Dogariu, a research scholar and the lead author on the paper, and James Michael, a doctoral student; and Marlan Scully, a lecturer with the rank of professor who also is a professor of physics at Texas A&M University.



The new laser-sensing method uses an ultraviolet laser pulse that is focused on a tiny patch of air, similar to the way a magnifying glass focuses sunlight into a hot spot. Within this hot spot — a cylinder-shaped region just 1 millimeter long — oxygen atoms become "excited" as their electrons get pumped up to high energy levels. When the pulse ends, the electrons fall back down and emit infrared light. Some of this light travels along the length of the excited cylinder region and, as it does so, it stimulates more electrons to fall, amplifying and organizing the light into a coherent laser beam aimed right back at the original laser. Researchers plan to use a sensor to receive the returning beam and determine what contaminants it encountered on the way back. "In general, when you want to determine if there are contaminants in the air you need to collect a sample of that air and test it," Miles said. "But with remote sensing you don't need to do that. If there's a bomb buried on the road ahead of you, you'd like to detect it by sampling the surrounding air, much like bomb-sniffing dogs can do, except from far away. That way you're out of the blast zone if it explodes. It's the same thing with hazardous gases — you don't want to be there yourself. Greenhouse gases and pollutants are up in the atmosphere, so sampling is difficult." Any chemical explosive emits various gases depending on its ingredients, but for many explosives the amount of gas is miniscule. The most commonly used remote laser-sensing method, LIDAR — short for light detection and ranging — measures the scattering of a beam of light as it reflects off a distant object and returns back to a sensor. It is commonly used for measuring the density of clouds and pollution in the air, but can not determine the actual identity of the particles or gases. Variants of this approach can identify contaminants, but are not sensitive enough to detect trace amounts and cannot determine the location of the gases with much accuracy. The returning beam is thousands of times stronger in the method developed by the Princeton researchers, which should allow them to determine not just how many contaminants are in the air but also the identity and location of those contaminants. The stronger signal should also allow for detection of much smaller concentrations of airborne contaminants, a particular concern when trying to detect trace amounts of explosive vapors. While the researchers are developing the underlying methods rather than deployable detectors, they envision a device that is small enough to be mounted on, for example, a tank and used to scan a roadway for bombs. So far, the researchers have demonstrated the process in the laboratory over a distance of about a foot and a half. In the future they plan to increase the distance over which the beams travel, which they note is a straightforward matter of focusing the beam farther away. They also plan to fine-tune the sensitivity of the technique to identify small amounts of airborne contaminants. In addition, the research group is developing other approaches to remote detection involving a combination of lasers and radar. "We'd like to be able to detect contaminants that are below a few parts per billion of the air molecules," Miles said. "That's an incredibly small number of molecules to find among the huge number of benign air molecules."

SCOTT®
RESPIRATORY
PROTECTION

DARPA's flying Hummers concept questioned

Source: http://www.popsci.com/science/article/2011-01/what-could-possibly-go-wrong-flying-hummers

DARPA proposed an innovative solution to the problem of IEDs: fly over them; if soldiers spot an IED, they push a button and the vehicle they ride in turns into a flying car; DARPA has a daunting list of specs for the Transformer: It must be able to take on small-arms fire and meet federal standards for safety and crash protection; it has got to have four-wheel drive and be able to reach an altitude of 10,000 feet; should the driver become incapacitated, it has to be able to fly itself; critics say it would be easier and cheaper to make road vehicles sturdier and better-able to withstand IEDs.

One rendering of DARPA's flying hummer // Source: laptopdrv.net

Last April DARPA proposed a novel solution to the problem of IED-strewn roads and otherwise impassable landscapes in Afghanistan and elsewhere: fly over them. The Pentagon agency's $50-million-plus exploratory program for the Transformer (TX) calls for a "robust ground vehicle" that can quickly transform into a vertical-takeoff-and-landing (VTOL) aircraft with a 1,000-pound payload capacity and a flying range of nearly 300 miles. DARPA has a daunting list of specs for any would-be contractors: It must be able to take on small-arms fire and meet federal standards for safety and crash protection. It has got to have four-wheel drive and be able to reach an altitude of 10,000 feet. Should the driver become incapacitated, it has to be able to fly itself. Popular Science notes that it is a lot to ask. The fundamental challenge of making cars fly is combining two distinct sets of optimal design characteristics into one package without sacrificing too much performance on either end. The very phrase "roadable air vehicle" sounds like a sigh of compromise. The military considered developing a hybrid in the 1950s with the ungainly Piasecki PA-59K, or "AirGeep," but then abandoned it because of cutbacks in military research. Advances in materials science and propulsion technology have lessened the trade-offs, but many challenges remain. First, weight. NASA engineer Mark Moore says that, as a rule, conventional aircraft grow roughly three pounds heavier for every extra pound of payload they are supposed to carry, whereas, "VTOL aircraft grow about five to six pounds heavier for every extra pound of weight." Now picture a VTOL aircraft that happens to be armored and packing four soldiers and their equipment. The required compact, rotorless propulsion system means, Moore says, a "hurricane-speed flow field" of rocks and debris upon takeoff. So much for stealth.

And all of this likely would do little to increase security. Transformers may be able to leap over IEDs, but insurgents can simply aim RPGs at the wings, which on one proposed Transformer design are laden with fuel tanks. Enemy combatants in Iraq have brought down Blackhawk helicopters, which are faster and more maneuverable, with small-arms fire. As for the autopilot function — nearly half of the finalists in DARPA's 2007 Urban Challenge for autonomous ground vehicles were unable to execute elemental driving tasks. "There is little reason to believe that autopiloting an inherently unstable vehicle through a battle space under hostile conditions will work better," PopSci concludes.

New clean-up method: explosives-eating sheep

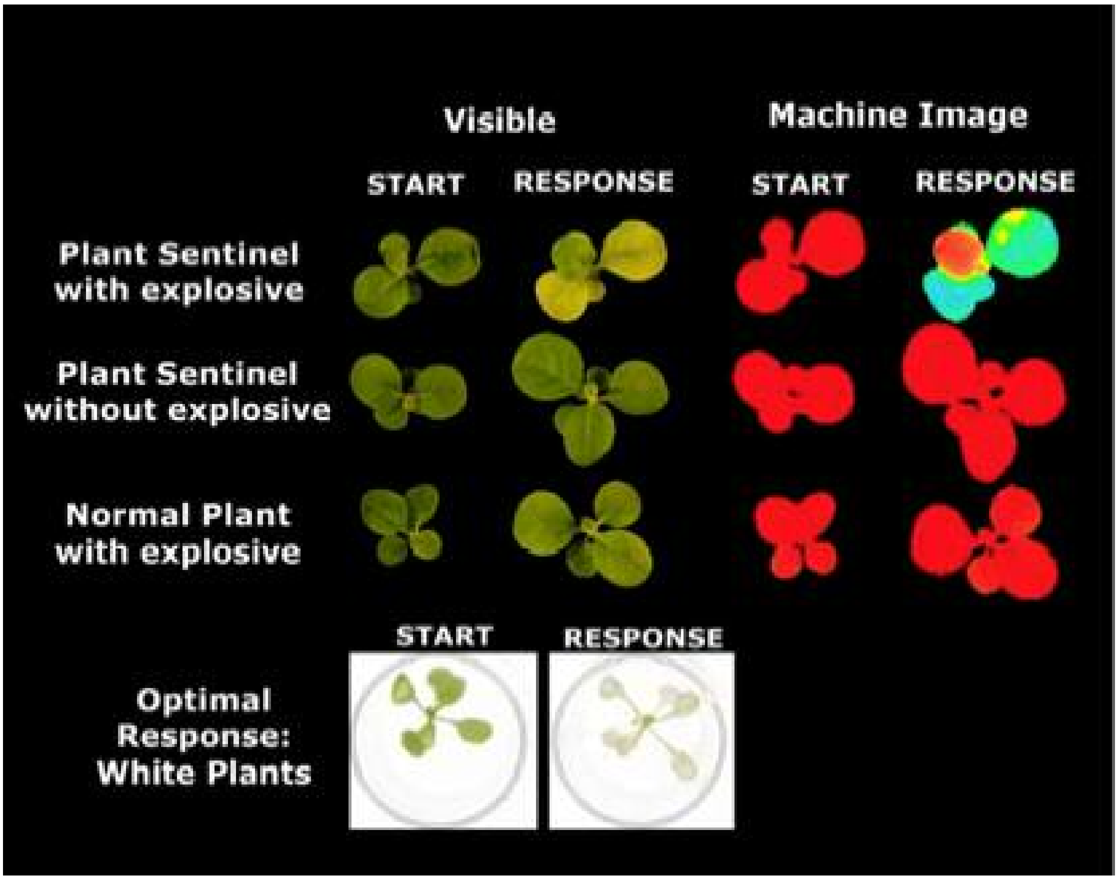
Source: http://homelandsecuritynewswire.com/new-clean-method-explosives-eating-sheep

TNT and other explosives from military munitions training and the remnants of old factories remain in the ground for decades, seeping into groundwater or poisoning plants; an Oregon State University researcher found that a bacteria in a sheep's stomach that help digest cellulose can also rapidly convert TNT into a harmless compound; the plan is to plant grasses in TNT contaminated soil to suck up the explosives, than unleash the sheep; a flock of twenty sheep could clear an acre of grass in a month, and completely rid it of munitions residue in less than three years. A team of scientists is feeding TNT to a flock of sheep. A. Morrie Craig, a veterinary scientist at Oregon State University, has found that the cud-chewing mammals can efficiently clean up explosives-contaminated soil, of which there are 1.3 million tons throughout the United States. TNT and other explosives from military munitions training and the remnants of old factories remain in the ground for decades. This residue rarely poses an immediate health threat, but officials at the Department of Defense fear that it could seep into groundwater or poison plants (which has happened before). Conventional cleanup techniques, such as incinerating the soil, are expensive and time-consuming. Sheep will work for free. PopSci reports that in 2004 Craig discovered that the bacteria in a sheep's stomach that help digest cellulose can also rapidly convert TNT into a harmless compound. In recent experiments, he and researchers from the U.S. Department of Agriculture fed sheep TNT for three weeks and found that it broke down so completely that no traces of it or any related compounds remained in the animals' feces. Craig and his colleagues plan to plant grasses in TNT contaminated soil to suck up the explosives. While the sheep munch away, the bacteria in their digestive tract take care of the rest. Craig's lab is testing the grazers on soil from a military base. He estimates that a flock of twenty sheep could clear an acre of grass in a month, and completely rid it of munitions residue in less than three years. Craig points out that even if a TNT-eating sheep's meat found its way onto a barbecue, it could never explode or cause health problems: "The ingested TNT is broken down into small molecules that are in no way similar to the original compound."

Plants That Can Detect Environmental Contaminants, Explosives

Source: http://www.medicalnewstoday.com/articles/216637.php

Someday, that potted palm in your living room might go from green to white, alerting you to a variety of nasty contaminants in the air, perhaps even explosives. The stuff of science fiction you say? Not so, says a Colorado State University biologist whose research is funded in part by Homeland Security's Science and Technology Directorate (DHS S&T), as well as by the Defense Advanced Research Projects Agency (DARPA), the Office of Naval Research (ONR), and others. Dr. June Medford and her team in the Department of Biology at Colorado State have shown that plants can serve as highly specific sentries for environmental pollutants and explosives. She's enabled a computer-designed detection trait to work in plants. How? By rewiring the plant's natural signaling process so that a detection of the bad stuff results in the loss of green color. Based on research so far, Medford says the detection abilities of some plants (tobacco is an example) are similar to, or even better, than those of a dog's snout, long the hallmark of a good detector. Best of all, the training time is nothing compared to that of a dog. «The idea comes directly from nature,» Medford said. «Plants can't run or hide from threats, so they've developed sophisticated systems to detect and respond to their environment. We've 'taught' plants how to detect things we're interested in and respond in a way anyone can see, to tell us there is something nasty around, by modifying the way the plant's proteins process chlorophyll. Our system, with improvements, may allow plants to serve as a simple and inexpensive means to monitor human surroundings for substances such as pollutants, explosives, or chemical


Visible
Machine Image
START
RESPONSE
START
RESPONSE
Plant Sentinel with explosive
Plant Sentinel without explosive
Normal Plant with explosive
START
RESPONSE
Optimal Response: White Plants

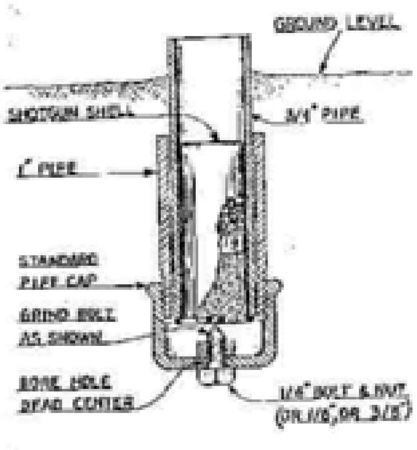
agents.» The detection traits could be used in any plant and could detect multiple pollutants at once - changes that can also be detected by satellite. While visible change in the plant is apparent after a day, the reaction can be remotely sensed within a couple of hours. A spectral imaging system designed specifically for the detection of de-greening biosensors would provide the fastest indication of a threat detected by the plants. Computational design of the detection trait was initially done in collaboration with Professor Homme Hellinga at Duke University, and more recently with Professor David Baker at the University of Washington. The Baker and Hellinga laboratories used a computer program to redesign naturally-occurring proteins called receptors. These redesigned receptors specifically recognize a pollutant or explosive. Medford's lab then modifies these computer redesigned receptors to function in plants, and targets them to the plant cell wall where they can recognize pollutants or explosives in the air or soil near the plant. Once the substance is detected, an internal signal causes the plant to turn white. Medford and her team want to speed up detection time. The initial or first-generation plants respond to an explosive in hours, but improvements are underway to reduce the response time to just a few minutes. A faster response time increases the likelihood of identifying the threat and preventing an attack. At this point in the research, it takes hours to achieve a visible change in the foliage,» says Doug Bauer, DHS S&T's program manager on the research. «Ideally, we'd want the reaction to be considerably faster.» In addition to faster response times, Bauer says, in the next generation of the research, the indicators may take place in a non-visible spectrum, such as infrared, by using color-changing methods other than the suppression of chlorophyll. That way, law enforcement equipped with the appropriate sensors would be alerted, but a terrorist would not be tipped off. A decentralized, ubiquitous detection capability could allow the early detection of bomb-manufacturing sites, instead of waiting for a potential bomber to show up at a transportation hub or other target zone. There are still many, many years of research to go before any possible deployment of plant sentinels. Once the research achieves a point where it may be possible to deploy, there are other considerations that will have to be taken into account and additional studies to be conducted. For example, USDA regulations stipulate that genetically-altered plants must go through a rigorous study on their impact to and interaction with the environment before they can be cultivated or planted in the United States. This work could eventually be used for a wide range of applications such as security in airports or monitoring for pollutants such as radon, a carcinogenic gas that can be found in basements. Harnessing plants as bio-sensors allows for distributed sensing without the need for a power supply. «One day, plants may assist law enforcement officers in detecting meth labs or help emergency responders determine where hazardous chemicals are leaking,» Bauer says. «The fact that DoD, DHS and a variety of other agencies contributed to funding this research is an indicator of the breadth of possibilities.»

A New Tool To Eliminate Improvised Land-Mines Uses Electromagnetic Energy

Source: http://www.medicalnewstoday.com/articles/216656.php

Composed of diverse elements, mostly of plastic, with little metal used, improvised explosive devices are very difficult to detect. In cooperation with two colombian universities, scientists at EPFL's Electromagnetic Compatibility Laboratory have found a solution. They have developed a device enabling the remote explosion of these mines, by using the energy from their electromagnetic impulses. This type of mine is often used by guerrillas or terrorist groups in conflict zones, and is present in many regions of the world, such as Colombia, Iraq and Afghanistan. They kill or mutilate hundreds of thousands of people every year, mainly civilians. Being themselves Colombian, and hence sensitive to this problem

Félix Vega and Nicolas Mora, doctoral students at EPFL, decide to make this project the subject of their thesis. The two researchers had to confront two main technical difficulties. Firstly, they had to find a way of inducting a current that would be strong enough to set off, at a distance, the detonators of the mines, sometimes buried deep in the ground. Secondly, they had to be sure of attaining the resonance frequencies of the various types of mines, which are all constructed in different ways. To scan the highest possible number of frequencies, it's necessary to create short impulses, with a very fast response time. In thus spanning a large spectrum of resonances, «only a fraction of the impulse we create reaches the target, and by then the current is no longer strong enough to explode the mine», explains Professor Farhad Rachidi. «We then realised that in spite of the wide diversity of these mines, they are however all in similar frequency ranges», adds Nicolas Mora. «So we developed a system that concentrates on those, and thus loses less energy.» The Electromagnetic Compatibility Laboratory tested this system in Colombia last November, using actual improvised mines provided by a team of professional bomb disposal experts, which they were able to set off at an average distance of 20 meters. This achievement is the result of two years of research work: «Now we have to develop a smaller prototype that is weather-resistant and especially easier to transport in the field», notes Félix Vega. «In Colombia, we often have to travel on small country roads.» Scheduled to run for a total of four years, the project has been undertaken with the National University of Colombia and the University of Los Andes.



Cyber News

U.S. Air Force creates powerful supercomputer out of PS3s

Source: http://homelandsecuritynewswire.com/us-air-force-creates-powerful-supercomputer-out-ps3s

The U.S. Air Force Research Laboratory (AFRL) has connected 1,760 PlayStation 3 systems together to create the fastest interactive computer in the entire Defense Department; the Condor Cluster, as the group of systems is known, is capable of performing 500 trillion floating point operations per second (500 TFLOPS). The U.S. Air Force Research Laboratory (AFRL) has connected 1,760 PlayStation 3 systems together to create what the organization is calling the fastest interactive computer in the entire Defense Department. The Condor Cluster, as the group of systems is known, also includes 168 separate graphical processing units and 84 coordinating servers in a parallel array capable of performing 500 trillion floating point operations per second (500 TFLOPS), according to AFRL Director of High Power Computing Mark Barnell. Gamasutra reports that using PS3s for the supercomputer's core allowed AFRL to construct the system for a total cost of $2 million, which Barnell estimates is five to 10 percent of an equivalent system built entirely with off-the-shelf computer parts. It will also consume one-tenth the power of other comparably powered supercomputers, officials said. After a ribbon-cutting ceremony last Wednesday, the cluster, which is housed in Rome, New York, will be used for research by Air Force service branches and centers across the country. The computer will reportedly be used for quick processing of ultra-high-resolution satellite imagery, as well as research into artificial intelligence, radar enhancement, and pattern recognition. Defense engineers worked directly with Sony and a distributor to acquire the systems, according to an interview with the Cleveland Plain Dealer. The project used the older, large PS3 units rather than new Slim models which, crucially, do not allow for the installation of Linux as an "Other OS." In 2000, it was widely reported that Iraqi dictator Saddam Hussein was planning to string then-cutting-edge PlayStation 2 systems into a defense supercomputer, though U.K. intelligence sources dismissed the claims as "nonsense." Researchers at the University of Illinois later strung 70 PS2s into a supercomputer capable of 500 billion operations per second.

Wikileaks and the Worldwide Information War

Power, Propaganda, and the Global Political Awakening

By Andrew Gavin Marshall

Source: http://www.globalresearch.ca/index.php?context=va&aid=22278

Introduction

The recent release of the 250,000 Wikileaks documents has provoked unparalleled global interest, both positive, negative, and everywhere in between. One thing that can be said with certainty: Wikileaks is changing things. There are those who accept what the Wikileaks releases say at face value, largely due to the misrepresentation of the documents by the corporate-controlled news. There are those who see the documents as authentic and simply in need of proper interpretation and analysis.

Then there are those, many of whom are in the alternative media, who approach the leaks with caution and suspicion.

There are those who simply cast the leaks aside as a 'psy-op' designed to target specific nations that fit into U.S. foreign policy objectives. Finally, then, there are those who deplore the leaks as 'treason' or threatening 'security'. Of all the claims and notions, the last is, without a doubt, the most ridiculous. This essay aims to examine the nature of the Wikileaks releases and how they should be approached and understood. If Wikileaks is changing things, let's hope people will make sure that it changes things in the right direction.

Media Propaganda Against Iran: Taking the Cables at Face Value

This perspective is perhaps the most propagated one, as it is largely influenced and undertaken by the mainstream corporate media, which present the leaked diplomatic cables as 'proof' of the media's take on major world issues; most notably among them, Iran's nuclear program. As per usual, the New York Times steps center stage in its unbridled contempt for truth and relentless use of propaganda to serve U.S. imperial interests, headlining articles with titles like, "Around the World, Distress Over Iran," which explained how Israel and the Arab leaders agree on Iran as a nuclear threat to the world, with the commentary in the article stating that, "running beneath the cables is a belief among many leaders that unless the current government in Tehran falls, Iran will have a bomb sooner or later." Fox News ran an article proclaiming that, "Leaked Documents Show Middle East Consensus on Threat Posed by Iran," and commented that, "the seismic document spill by WikiLeaks showed one area of profound agreement — that Iran is viewed in the Middle East as the region's No. 1 troublemaker."

This, it should be understood, is propaganda. Yet, we need to properly refine our understanding of propaganda in order to assess what is specifically propagandistic about these stories. While one should remain skeptical of sources and disinformation campaigns (as those who critically analyze the media have known take place time and time again), one must also consider the personal perspective of the source and decipher between authenticity and analysis. These documents, I truly believe, are authentic. In this sense, I do not adhere to the notion that these are a part of a psychological operation (psy-op) or propaganda effort, in terms of the actual release of the documents. We must keep in mind that the sources for these cables are U.S. diplomatic channels, and thus the statements within them reflect the perspectives and beliefs of U.S. diplomatic personnel. The documents are an authentic representation of their statements and beliefs, but that does not imply that they are an accurate representation of reality.

This is where the media comes in to propagandize the information within the leaks. The two above examples claim that the leaks show that there is a "consensus" on Iran, and thus, that the U.S. and indeed Israeli positions on Iran for the past several years have been "vindicated," namely in that they fear Iran is making nuclear weapons. This is nonsense. The media has essentially read and propagated the documents at face value, meaning that because U.S. diplomats, Middle Eastern and Arab leaders all agree that Iran is a "threat" and is trying to make a "nuclear weapon," it therefore must be true. This is a non sequitur. If a military general tells several soldiers to commit a raid on a house because there are "suspected terrorists" inside, the fact that the soldiers carry out the raid – and that they believe there are terrorists inside – does not make it so. In contextualizing this example with the current Wikileaks release, just because Middle Eastern and Arab leaders see Iran as a threat, does not make it so.

Again, consider the sources. What makes the Arab leaders trustworthy sources for 'unbiased' information? For example, one 'revelation' that made its way around the world was the insistence of Saudi Arabia's King Abdullah to America to "cut off the head of the snake" of Iran, and urging America to launch military strikes against Iran. This has largely been interpreted in the media as "proof" that there is a "consensus" on the "threat" posed by Iran to the Middle East and the world. This has been the propaganda line towed by the New York Times, Fox News and the Israeli government, among many others. Yet, we need to properly contextualize this information, something which the New York Times has a long record of failing to properly do (intentionally, I might add). I do not doubt the authenticity of these statements or the beliefs of the Arab leaders that Iran is a 'threat'. Iran, on the other hand, has claimed that the leaks are "mischievous" and that they serve US interests, and claimed that Iran is "friends" with its neighbours.[4] This too, is propaganda. Again, we need to contextualize.

Iran is a Shi'a nation, while the Arab nations, particularly Saudi Arabia, are predominantly Sunni. This presents a means of division among these nations in the region, at least on a superficial basis. The reality, however, is that Saudi Arabia and Iran are far from "friendly", and have not been on good terms since the Shah was deposed in 1979. Iran is Saudi Arabia's primary contender and competition for power and influence in the region, and thus Iran is, inherently, a threat to Saudi Arabia, politically. Further, the Arab states, whose claims against Iran have been widely publicized, such as those of Saudi Arabia, Bahrain, Oman, the UAE and Egypt, must be understood in their relation to the United States. The Arab states are American proxies in the region. Their armies are subsidized by the American military industrial complex, their political regimes (all of which are dictatorships and dynasties), are propped up and supported by America. The same goes for Israel, although it has at least the public outward appearance of a democracy, much like the United States, itself.

The Arab nations and leaders know that the only reason they have and maintain their power is because the United States allows them and helps them to do so. Thus, they are dependent upon America and its political, financial and military support. Going against America's ambitions in the region is a sure way to end up like Iraq and Saddam Hussein. The history of the Middle East in the modern era is replete with examples of how one-time puppets and personal favourites of the American Empire can so easily turn into new enemies and "threats to peace." American sponsored regime change takes place, and a new puppet is installed. If Arab leaders said that Iran was not a threat to peace, they would soon find themselves targets of Western imperialism. Further, many, like King Abdullah in Saudi Arabia, are so virulent in their hatred and distrust of Iran simply because they are regional competitors for influence. One thing can be said of all states and their leaders, they are inherently self-interested and obsessed with self-preservation and personal power expansion.

Saudi Arabia, in particular, is not a passive actor in the regional battle of influence with Iran. In Yemen, Saudi Arabia is involved in another American imperial war of conquest, in suppressing secessionist and indigenous liberation movements in the North and South of Yemen. Yemen, ruled by an American supported dictator, Saleh, who has been in power since 1978, is also working with the Americans to suppress its own population in order to maintain its hold on power. Much of the presentation of the conflict, however, is in propagandizing the conflict, portraying it as a regional battle for influence between Saudi Arabia and Iran. While there is no doubt, and clear admissions, of Saudi Arabia's involvement in the war, there has been no information that Iran has had any involvement, yet it is constantly accused by both Saudi Arabia and Yemen of being involved. This may be an attempt to draw Iran into a regional proxy war, if not to simply demonize the nation further. In the midst of this new Yemeni war, America made an arms deal with Saudi Arabia which broke the record as the largest U.S. arms deal in history, at $60 billion. The deal, of which it is no secret, is aimed at building up Saudi Arabia's military capabilities in order to both engage more effectively in the Yemen war, but primarily to challenge and counter increased Iranian influence in the region. In short, America is arming its proxy nations for a war with Iran.

Israel did not denounce the arms deal as it was taking place, simply because it ultimately served Israel's interest in the region as well, of which its main target is Iran. Further, Israel is left subdued to American interests, as an American proxy itself. If Israel's military financing and hardware comes from America (which it does), thus making it dependent upon America for its own military power, Israel is in no position to tell America to not arm its other regional proxies. If indeed there is a regional war against Iran in the making, which it has appeared for some time that there is, it is certainly in Israel's interest to have allies against Iran in the region.

Is Wikileaks a Propaganda Effort?

The leaders of Israel have been very adamant that the Wikileaks documents do not embarrass Israel to any extent. Prior to the release, the U.S. government briefed Israeli officials on the type of documents that would be released by Wikileaks regarding Israel.[5] Israeli Prime Minister Benjamin Netanyahu stated, "there is no disparity between the public discourse between us and Washington, and the mutual understanding of each other's positions." The Israeli Defense Minister, Ehud Barak, claimed that the documents "show a more accurate view of reality." One top Turkish politician stated that looking at which countries are pleased with the releases says a lot, and speculated that Israel "engineered the release" of documents in an attempt to advance its interests and to "pressure Turkey."

Further, the Internet and various alternative news organizations are abuzz with speculation that Wikileaks itself may be a propaganda front, perhaps even a CIA front organization, a method of "controlling the opposition" (which, historically we know, is no stranger to CIA activities). Yet, this speculation is based upon the use of the information that is released in the cables, and it strikes me as a lack of contextualizing the documents.

So, how should one contextualize this? Let's begin with Israel. Certainly, Israel is without a doubt a criminal state (as all states essentially are), but its criminality is amplified more so than most states on this planet, possibly outdone only by America, itself. Israel's ethnic cleansing of Palestinians is one of the most horrific and long-lasting crimes against humanity seen in the past 50 years, and posterity will view Israel as the vicious, war-mongering, dehumanizing and abhorrent state it is. Yet, for all that Israel is, one thing Israel is not, is subtle. When the Israeli PM states that the Wikileaks releases are not embarrassing to Israel, he is mostly correct. This is not because Israel has nothing to hide (remember, the Wikileaks documents are not 'top secret' documents, but merely diplomatic cables), but because the diplomatic exchanges Israel makes largely reflect the reality of the public statements Israel makes. Israel and its political elite are no strangers to making absurd public statements, to constantly threatening war with Iran and other neighbors, or to propagandizing their beliefs that Iran is making nuclear weapons (something which has never been proven). Thus, the leaks do not 'hurt' Israel's image, because Israel's image, internationally, is already so abysmal and despicable, and because Israeli diplomats and politicians are generally as brazen in what they say publicly as they say to each other, that Israel's image has largely remained the same. Of course, Israeli leaders – political and military – are using the leaks to suggest that it "vindicates" their perspective on Iran as a threat, which of course is an absurd propaganda ploy, the exact same technique taken on by the corporate media, in taking the cables at face value.

While Iran has slammed the Wikileaks releases as Western propaganda aimed at Iran, this statement itself should be taken as a form of propaganda. After all, Iran claimed that it is "friends" with all its neighbors, a claim which is an historical and present falsity. Iran, like all states, uses propaganda to advance its own interests. Iran is not by any means a wonderful nation. However, compared to the American favorites in the region (such as Saudi Arabia), Iran is a bastion of freedom and democracy, which isn't saying much. Those who attempt to battle the spread of misinformation and propaganda, myself included, must remain highly critical of media representations and campaigns against Iran, of which there are many. Iran is firmly in the targets of America's imperial ambitions, this is no secret. Yet, there is nothing in the current batch of Wikileaks releases that strikes me as inauthentic in relation to Iran, especially those documents pertaining to the perspectives of Western diplomats and Arab leaders in relation to Iran. No doubt, they have these perspectives simply because they reflect the policy priorities of America and the West, itself, not because they are factual in their substance. In this, we must decipher between authenticity and accuracy.

Iran stating that the Wikileaks documents are propaganda is a misnomer and is misleading. Analysts must not only critically assess the authenticity of documents (and the sources from which they come), but also, and perhaps even more importantly, they must critically analyze the interpretation of those documents. So while I do not doubt the authenticity of documents pertaining to Western and Middle Eastern perceptions of Iran (as it fits in with the wider geopolitical realities of the region), it is the interpretation of the documents that I view as active propaganda efforts on the part of Western governments and media. The methods of this propaganda effort, however, are in depicting the documents as 'factual assessments' of the on-the-ground reality, which they are not. The documents are factual in how they represent the views of those who wrote them, which does not mean that they are factual in their substance. There is a difference, and acknowledging this difference is incredibly important in both the exposure of propaganda and assessment of truth.

The Truth About Diplomacy

Craig Murray is one voice that should be heard on this issue. Craig Murray was a former British Ambassador to Uzbekistan who made a name for himself in exposing intelligence from Uzbekistan related to al-Qaeda as entirely unreliable, due to the methods of torture used to get the information (such as boiling people alive). This intelligence was passed to the CIA and MI6, which Murray said was "factually incorrect." When Murray expressed his concerns with the higher-ups in the British diplomatic services, he was reprimanded for talking about "human rights."The British Foreign and Commonwealth Office (FCO) told Murray that he had one week to resign, and was threatened with possible prosecution or jail time for revealing "state secrets." He was subsequently removed from his ambassadorial position, and has since become something of a political activist. In short, Murray is exactly the type of diplomat a person should want: honest. But he was also exactly the type of diplomat that Western imperial powers don't want: honest.

In the midst of the latest Wikileaks releases of diplomatic documents, Craig Murray was asked to write an article for the Guardian regarding his interpretation of the issue. As Murray later noted, the paper placed his article, largely reduced, hidden in the middle of a long article which was a compendium of various commentaries on Wikileaks. Murray, however, posted the full version on his website. In the article, Murray begins by assessing the claims of government officials around the world, particularly in the United States, that Wikileaks exposes the United States to "harm," that it puts lives at risk, and that they will "encourage Islamic extremism," and most especially, the notion that "government secrecy is essential to keep us all safe." Murray explains that having been a diplomat for over 20 years, he is very familiar with these arguments particularly that as a result of Wikileaks, diplomats will no longer be candid in giving advice, "if that advice might become public." Murray elaborates:

> *Put it another way. The best advice is advice you would not be prepared to defend in public. Really? Why? In today's globalised world, the Embassy is not a unique source of expertise. Often expa-*

> *triate, academic and commercial organisations are a lot better informed. The best policy advice is not advice which is shielded from peer review.*
>
> *What of course the establishment mean is that Ambassadors should be free to recommend things which the general public would view with deep opprobrium, without any danger of being found out. But should they really be allowed to do that, in a democracy?*

Murray pointedly asked why a type of behaviour that is considered reprehensible for most people – such as lying – "should be considered acceptable, or even praiseworthy, in diplomacy." Murray explained that for British diplomats, "this belief that their profession exempts them from the normal constraints of decent behaviour amounts to a cult of Machiavellianism, a pride in their own amorality." He explained that diplomats come from a very narrow upper social strata, and "view themselves as ultra-intelligent Nietzschean supermen, above normal morality" who are socially connected to the political elite. In criticizing the claims made by many commentators that the release of the leaks endanger lives, Murray pointedly wrote that this perspective needs to be "set against any such risk the hundreds of thousands of actual dead from the foreign policies of the US and its co-conspirators in the past decade." Further, for those who posit that Wikileaks is a psy-op or propaganda operation or that Wikileaks is a "CIA front", Murray had this to say:

> *Of course the documents reflect the US view – they are official US government communications. What they show is something I witnessed personally, that diplomats as a class very seldom tell unpalatable truths to politicians, but rather report and reinforce what their masters want to hear, in the hope of receiving preferment.*
>
> *There is therefore a huge amount about Iran's putative nuclear arsenal and an exaggeration of Iran's warhead delivery capability. But there is nothing about Israel's massive nuclear arsenal. That is not because wikileaks have censored criticism of Israel. It is because any US diplomat who made an honest and open assessment of Israeli crimes would very quickly be an unemployed ex-diplomat.*

Murray concluded his article with the statement that all would do well to keep in mind: "Truth helps the people against rapacious elites – everywhere."

World Order and Global Awakening

In attempting to understand Wikileaks and its potential effects (that is, if the alternative media and citizens activists use this opportunity), we must place Wikileaks within a wider geopolitical context. Our human world exists as a complex system of social interactions. As powerful and dominating as elites are and have always been, we must understand that they are not omnipotent; they are human and flawed, as are their methods and ideas. There are other forces at work in the human social world, and these various interactions created and changed the world into what it is, and will determine where it is going. In effect, nothing is preordained; nothing is exact. Plans are made, certainly, by elites, in designing ideas and reshaping and controlling society. However, society – and in the globalized world, a 'global society' – react and interact with elite forces and ideas. Just as the people must react to and experience repercussions from changes in elite processes, so too must the elite react to and experience repercussions from changes in social processes. Today, we can conceptualize this dichotomy – the geopolitical reality of the world – as '<u>The Global Political Awakening and the New World Order</u>':

There is a new and unique development in human history that is taking place around the world; it is unprecedented in reach and volume, and it is also the greatest threat to all global power structures: the 'global political awakening.' The term was coined by Zbigniew Brzezinski, and refers to the fact that, as Brzezinski wrote:

> *For the first time in history almost all of humanity is politically activated, politically conscious and politically interactive. Global activism is generating a surge in the quest for cultural respect and economic opportunity in a world scarred by memories of colonial or imperial domination.*

It is, in essence, this massive 'global political awakening' which presents the gravest and greatest challenge to the organized powers of globalization and the global political economy: nation-states, multinational corporations and banks, central banks, international organizations, military, intelligence, media and academic institutions. The Transnational Capitalist Class (TCC), or 'Superclass' as David Rothkopf refers to them, are globalized like never before. For the first time in history, we have a truly global and heavily integrated elite. As elites have globalized their power, seeking to construct a 'new world order' of global governance and ultimately global government (decades down the line), they have simultaneously globalized populations.

The 'Technological Revolution' involves two major geopolitical developments. The first is that as technology advances, systems of mass communication rapidly accelerate, and the world's people are able to engage in instant communication with one another and gain access to information from around the world. In it, lies the potential – and ultimately a central source – of a massive global political awakening. Simultaneously, the Technological Revolution has allowed elites to redirect and control society in ways never before imagined, potentially culminating in a global scientific dictatorship, as many have warned of since the early decades of the 20th century. The potential for controlling the masses has never been so great, as science unleashes the power of genetics, biometrics, surveillance, and new forms of modern eugenics; implemented by a scientific elite equipped with systems of psycho-social control.

Brzezinski has written extensively on the issue of the 'Global Political Awakening,' and has been giving speeches at various elite think tanks around the world, 'informing' the elites of this changing global dynamic. Brzezinski is one of the principle representatives of the global elite and one of the most influential elite intellectuals in the world. His analysis of the `global politicl awakening`is useful because of his repesentation of it as the primary global threat to elite interests everywhere. Thus, people should view the concept of the `global political awakening`as the greatest potential hope for humanity and that it should be advanced and aided, as opposed to Brzezinski`s perspective that it should be controlled and suppressed. However, it would be best for Brzezinski to explain the concept in his own words to allow people to understand how it constitutes a `threat`to elite interests:

> ***For the first time in human history almost all of humanity is politically activated, politically conscious and politically interactive****. There are only a few pockets of humanity left in the remotest corners of the world that are not politically alert and engaged with the political turmoil and stirrings that are so widespread today around the world.* ***The resulting global political activism is generating a surge in the quest for personal dignity, cultural respect and economic opportunity in a world painfully scarred by memories of centuries-long alien colonial or imperial domination... The worldwide yearning for human dignity is the central challenge inherent in the phenomenon of global political awakening.***
>
> *...America needs to face squarely a centrally important new global reality: that the world's population is experiencing a political awakening unprecedented in scope and intensity, with the result that* ***the politics of populism are transforming the politics of power****. The need to respond to that massive phenomenon poses to the uniquely sovereign America an historic dilemma: What should be the central definition of America's global role? ... The central challenge of our time is posed not by global terrorism, but rather by the intensifying turbulence caused by the phenomenon of global political awakening.* ***That awakening is socially massive and politically radicalizing****.*
>
> *... It is no overstatement to assert that now* ***in the 21st century the population of much of the developing world is politically stirring and in many places seething with unrest. It is a population acutely conscious of social injustice to an unprecedented degree, and often resentful of its perceived lack of political dignity****. The*

> *nearly universal access to radio, television and increasingly **the Internet is creating a community of shared perceptions** and envy **that can be galvanized and channeled** by demagogic political or religious passions. **These energies transcend sovereign borders and pose a challenge both to existing states as well as to the existing global hierarchy, on top of which America still perches**.*
>
> *... **The youth of the Third World are particularly restless and resentful**. The demographic revolution they embody is thus a political time-bomb, as well. With the exception of Europe, Japan and America, the rapidly expanding demographic bulge in the 25-year-old-and-under age bracket is creating a huge mass of impatient young people. Their minds have been stirred by sounds and images that emanate from afar and which intensify their disaffection with what is at hand. **Their potential revolutionary spearhead is likely to emerge from among the scores of millions of students concentrated in the often intellectually dubious «tertiary level» educational institutions of developing countries**. Depending on the definition of the tertiary educational level, **there are currently worldwide between 80 and 130 million «college» students. Typically originating from the socially insecure lower middle class and inflamed by a sense of social outrage, these millions of students are revolutionaries-in-waiting**, already semi-mobilized in large congregations, **connected by the Internet** and pre-positioned for a replay on a larger scale of what transpired years earlier in Mexico City or in Tiananmen Square. Their **physical energy and emotional frustration is just waiting to be triggered by a cause, or a faith, or a hatred**.*

Brzezinski thus posits that to address this new global "challenge" to entrenched powers, particularly nation-states that cannot sufficiently address the increasingly non-pliant populations and populist demands, what is required, is "increasingly supranational cooperation, actively promoted by the United States." In other words, Brzezinski favours an increased and expanded 'internationalization', not surprising considering he laid the intellectual foundations of the Trilateral Commission. He explains that "Democracy per se is not an enduring solution," as it could be overtaken by "radically resentful populism." This is truly a new global reality:

> *Politically awakened mankind craves political dignity, which democracy can enhance, but political dignity also encompasses ethnic or national self-determination, religious self-definition, and human and social rights, all in a world now acutely aware of economic, racial and ethnic inequities. The quest for political dignity, especially through national self-determination and social transformation, is part of the pulse of self-assertion by the world's underprivileged.*

Thus, writes Brzezinski, "an effective response can only come from a self-confident America genuinely committed to a new vision of global solidarity." The idea is that to address the grievances caused by globalization and global power structures, the world and America must expand and institutionalize the process of globalization, not simply in the economic sphere, but in the social and political as well. It is a flawed logic, to say the least, that the answer to these systemic problems is to enhance and strengthen the systemic flaws that created them. One cannot put out a fire by adding fuel.

Brzezinski even wrote that, "let it be said right away that supranationality should not be confused with world government. Even if it were desirable, mankind is not remotely ready for world government, and the American people certainly do not want it." Instead, Brzezinski argues, America must be central in constructing a system of global governance, "in shaping a world that is defined less by the fiction of state sovereignty and more by the reality of expanding and politically regulated interdependence." In other words, not 'global government' but 'global governance', which is simply a rhetorical ploy, as 'global governance' – no matter how overlapping, sporadic and desultory it presents itself – is in fact a key step and necessary transition in the moves toward an actual global government structure.

Conceptualizing Wikileaks

I feel that Wikileaks must be conceptualized within our understanding of this geopolitical reality we find ourselves in today. While indeed it is necessary to be skeptical of such monumental events, we must allow ourselves to remember that there are always surprises – for everyone – and that the future is nothing if not unknown. Anything, truly, can happen. There is of course logic behind the automatic skepticism and suspicion about Wikileaks from the alternative media; however, they also risk losing an incredible opportunity presented by Wikileaks, to not only reach more people with important information, but to better inform that information itself.

For those who view Wikileaks as a conspiracy or plot, as a psy-op of some kind, while indeed these things have taken place in the past, there is simply no evidence for it thus far. Every examination of this concept is based upon speculation. Many nations around the world, particularly in the Middle East and South Asia, are pointing to the Western nations as engaging in a covert propaganda campaign aimed at creating disunity between states and allies. Iran, Turkey, Pakistan and Afghanistan have made such claims. It is no surprise that most of these are nations, particularly Iran, are targets of U.S. imperial policy. Since, however, the Wikileaks releases speak heavily and negatively about Iran, Pakistan, Afghanistan, Russia, China, Venezuela, etc., one must remember that these are 'diplomatic cables', and represent the 'opinions and beliefs' of the diplomatic establishment, a social group which is historically and presently deeply enmeshed and submissive to elite ideology and methodology. In short, these are the foreign imperial envoys, and as such, they are ideological imperialists and represent imperial interests.

As has been the case both historically and presently, imperial objectives are hidden with political rhetoric. Since, politically, these are target nations of the American imperial elite, America's diplomatic representatives will focus on these nations, and adopt the same ideas and beliefs. How many people have ever been given a raise by questioning and then disregarding their superior's management technique? Thus, in their respective nations and operations, the diplomats will seek information that targets these nations or serve specific American imperial objectives. If all the information they come up with are rumours and conjectures and repeated talking points, that is what will be seen in the diplomatic cables. Indeed, that was exactly the case. The cables are full of rumours and unsupported allegations. So naturally, they would target these specific nations – deemed geopolitically significant by American imperial interests – and why there would be far less information on Israel and other allied nations. This is why it seems to me that these cables are authentic. They seem to represent the reality of the 'diplomatic social group', and thus they are a vivid exploration in the study of imperialism. We have been given the opportunity to see the 'communications' of imperial diplomacy. It is in this, that we are presented with an incredible opportunity.

Further, in regards to many Middle Eastern and Asian nations framing Wikileaks as a "Western plot," as critical thinkers we must take note of the geopolitical reality of the 'global political awakenng.' All states are self-interested, that is the nature of a state. Elites all over the world are aware of the reality and potential political power of the 'global political awakening' and thus, seek to suppress or co-opt its potential. States which are often viewed by the critical press as 'targets' by Western imperial powers (such as Iran), may seek to use this power to its own advantage. They may attempt to steer the 'global awakening' and the 'alternative media' to their favour, which gives them political power. But the alternative media must not 'pick sides' in terms of global elites and power structures, we must remain critical of all sides and all actors.

Wikileaks is receiving an incredible readership and is reaching out to new audiences, globally, in the American homeland itself, and to the youth of the world. People's perceptions are beginning to change on a variety of issues. The question is: will the alternative media ignore Wikileaks and isolate itself, or will they engage with Wikileaks, and prevent the mainstream corporate media from having a 'monopoly of interpretation', which becomes inherently propagandistic. Wikileaks is having global repercussions, and has been very good for the newspaper and mainstream news industries, which have been on a steady decline. This too, can be an issue to reach out to this new and growing audience, and to bring them to a new perspective. If we do not reach out, we are left talking to each other, further isolating ourselves, and ultimately becoming subverted and ineffective for change. We need to reach out to new audiences, and this is an incredible opportunity to do so. People are interested, people are curious, people are hungry for more.

Wikileaks and the Media

Instead of deriding Wikileaks as "not telling us anything we didn't know" before, perhaps the alternative media should use the popularity and momentum of Wikileaks to take from it the documentation and analysis that further strengthens our arguments and beliefs. This will allow for others, especially new audiences of interested people worldwide, to place the Wikileaks releases within a wider context and understanding. The reports from Wikileaks are 'revelations' only to those who largely adhere to the 'illusions' of the world: that we live in 'democracies' promoting 'freedom' around the world and at home, etc. The 'revelations' however, are not simply challenging American perceptions of America, but of all nations and their populations. The fact that these people are reading and discovering new things for which they are developing an interest is an incredible change. This is likely why the corporate media is so heavily involved in the dissemination of this information (which itself is a major source of suspicion for the alternative media): to control the interpretation of the message. It is the job of the alternative media and intellectuals and other thinking individuals to challenge that interpretation with factual analysis. The Wikileaks releases, in fact, give us more facts to place within and support our interpretations than they do for the corporate media.

We must ask why the Wikileaks releases were 'revelations' for most people? Well, it was surprising simply for the fact that the media itself has such a strong hold on the access, dissemination and interpretation of information. They are 'revelations' because people are indoctrinated with myths. They are not 'revelations' to the alternative media because we have been talking about these things for years. However, while they may not necessarily be 'revelations', they are in fact, 'confirmations' and 'vindications' and bring more information to the analysis. It is in this, that a great opportunity lies. For since the leaks support and better inform our perspectives, we can build on this concept and examine how Wikileaks adds to and supports critical analysis. For those who are newly interested and looking for information, or for those who are having their previous perceptions challenged, it is the alternative media and critical voices alone who can place that information in a wider context for everyone else. In this, more people will see how it is the alternative media and critical perspectives which were more reflective of reality than say, the mainstream media (for which Wikileaks is a 'revelation'). Thus, more people may soon start turning to alternative media and ideas; after all, our perspectives were vindicated, not those of the mainstream media (though they attempt to spin it as such).

We are under a heavy propaganda offensive on the part of the global corporate and mainstream media to spin and manipulate these leaks to their own interests. We, as alternative media and voices, must use Wikileaks to our advantage. Ignoring it will only damage our cause and undermine our strength. The mainstream media understood that; so too, must we. Wikileaks presents in itself a further opportunity for the larger exposure of mainstream media as organized propaganda. By 'surprising' so many people with the 'revelations', the media has in effect exposed itself as deeply inadequate in their analysis of the world and the major issues within it. While currently it is giving the mainstream media a great boost, we are still immersed in the era of the 'Technological Revolution' and there is still (for now, anyway) Internet freedom, and thus, the tide can quickly turn.

Like the saying goes, 'the rich man will sell you the rope to hang him with if he thinks he can make a buck on it.' Perhaps the mainstream media has done the same. No other organized apparatus was as capable of disseminating as much material as quickly and with such global reach as the mainstream media. If the leaks initially only made it into alternative media, then the information would only reach those whom are already reading the alternative press. In that, they would not be such grand 'revelations' and would have had a muted effect. In the mainstream media's global exposure of Wikileaks material (never mind their slanted and propagandistic interpretations), they have changed the dynamic and significance of the information. By reaching wider and new audiences, the alternative and critical voices can co-opt these new audiences; lead them away from the realm of information 'control' into the realm of information 'access'. This is potentially one of the greatest opportunities presented for the alternative and critical voices of the world.

Wikileaks is a globally transformative event. Not simply in terms of awakening new people to 'new' information, but also in terms of the effect it is having upon global power structures, itself. With ambassadors resigning, diplomats being exposed as liars and tools, political rifts developing between Western imperial allies, and many careers and reputations of elites around the world at great risk, Wikileaks is creating the potential for an enormous deterioration in the effectiveness of imperialism and domination. That, in itself, is an admirable and worthy goal. That this is already a reality is representative of how truly transformative Wikileaks is and could be. People, globally, are starting to see their leaders through a lens not filtered by 'public relations.' Through mainstream media, it gets filtered through propaganda, which is why it is an essential duty of the alternative media and critical thinkers to place this information in a wider, comprehensive context. This would further erode the effectiveness of empire.

With the reaction of several states and policing organizations to issue arrest warrants for Julian Assange, or in calling for his assassination (as one Canadian adviser to the Prime Minister suggested on television), these organizations and individuals are exposing their own hatred of democracy, transparency and freedom of information. Their reactions can be used to discredit their legitimacy to 'rule'. If policing agencies are supposed to "protect and serve," why are they seeking instead to "punish and subvert" those who expose the truth? Again, this comes as no surprise to those who closely study the nature of the state, and especially the modern phenomenon of the militarization of domestic society and the dismantling of rights and freedoms. However, it is happening before the eyes of the whole world, and people are paying attention. This is new.

This is an incredible opportunity to criticize foreign policy (read: 'imperial strategy'), and to disembowel many global power structures. More people, now, than ever before, will be willing to listen, learn and investigate for themselves. Wikileaks should be regarded as a 'gift', not a 'distraction.' Instead of focusing on the parts of the Wikileaks cables which do not reflect the perspectives of the alternative media (such as on Iran), we must use Wikileaks to better inform our own understanding not simply of the 'policy' itself, but of the complex social interactions and ideas that create the basis for the 'policy' to be carried out. In regards to the diplomatic cables themselves, we are better able to understand the nature of diplomats as 'agents of empire,' and so instead of discounting the cables as 'propaganda' we must use them against the apparatus of empire itself: to expose the empire for what it is. Wikileaks helps to unsheathe and strip away the rhetoric behind imperial policy, and expose diplomats not as 'informed observers', but as 'agents of power.' The reaction by nations, organizations and institutions around the world adds further fuel to this approach, as we are seeing the utter distaste political leaders have for 'democracy' and 'freedom of information', despite their rhetoric. Several institutions of power can be more widely exposed in this manner.

A recent addition to this analysis can be in the role played by universities not in 'education' but in 'indoctrination' and the production of new 'agents of power.' For example, Columbia University is one of the most "respected" and "revered" universities in the world, which has produced several individuals and significant sectors of the political elite (including diplomats). In reaction to the Wikileaks releases, Columbia University has warned "students they risk future job prospects if they download any of the material," which followed "a government ban on employees, estimated at more than two-and-a-half million people, using work computers and other communication devices to look at diplomatic cables released by WikiLeaks." The University "emailed students at the university's school of international and public affairs, a recruiting ground for the state department."[14] Good for Columbia! What do they think university is for, 'education' or something? How dare students take education into their own hands, especially students who will likely be future diplomats. This university reaction to Wikileaks helps call into attention the role of universities in our society, and specifically the role of universities in shaping the future 'managers' of the imperial apparatus.

Wiki.leaks as an Opportunity

If Wikileaks is a psy-op, it is either the stupidest or most intelligent psychological operation ever undertaken. But one thing is for sure: systems and structures of power are in the process of being exposed to a much wider audience than ever before. The question for the alternative media and critical researchers, alike, is what will they do with this information and this opportunity?

Julian Assange was recently interviewed by Time Magazine about Wikileaks, in which he explained to the inadequately informed editor of Time Magazine that organizations which are secretive need to be exposed:

> *If their behavior is revealed to the public, they have one of two choices: one is to reform in such a way that they can be proud of their endeavors, and proud to display them to the public. Or the other is to lock down internally and to balkanize, and as a result, of course, cease to be as efficient as they were. To me, that is a very good outcome, because* ***organizations can either be efficient, open and honest, or they can be closed, conspiratorial and inefficient****.*

Assange further explained some of his perspectives regarding the influence of and reactions to Wikileaks, stating that the Chinese:

> *appear to be terrified of free speech, and while one might say that means something awful is happening in the country, I actually think that is a very optimistic sign, because* ***it means that speech can still cause reform and that the power structure is still inherently political****, as opposed to fiscal. So journalism and writing are capable of achieving change, and that is why Chinese authorities are so scared of it. Whereas in the United States to a large degree, and in other Western countries, the basic elements of society have been so heavily fiscalized through contractual obligations that political change doesn't seem to result in economic change, which in other words means that* ***political change doesn't result in change****.*

In the interview, Assange turned to the issue of the Internet and community media:

> *For the rise of social media, it's quite interesting. When we first started [in 2006], we thought we would have the analytical work done by bloggers and people who wrote Wikipedia articles and so on. And we thought that was a natural, given that we had lots of quality, important content... The bulk of the heavy lifting - heavy analytical lifting - that is done with our materials is done by us, and is done by professional journalists we work with and by professional human-rights activists. It is not done by the broader community. However, once the initial lifting is done, once a story becomes a story, becomes a news article,* ***then we start to see community involvement, which digs deeper and provides more perspective****. So the social networks tend to be, for us, an amplifier of what we are doing. And also a supply of sources for us.*

As researchers, media, and critics, we must realize that our perspectives and beliefs must be open to change and evolution. Simply because something like this has never happened before does not mean that it isn't happening now. We live in the era of the 'Technological Revolution,' and the Internet has changed economics, politics and society itself, on a global scale. This is where the true hope in furthering and better informing the 'global political awakening' will need to take speed and establish itself. True change in our world is not going to come from already-established or newly-created institutions of power, which is where all issues are currently being addressed, especially those of global significance. True change, instead, can only come not from global power structures, but from the global 'community' of people, interacting with one another via the power unleashed by the 'Technological Revolution.' Change must be globally understood and community organized.

We are on the verge of a period of global social transformation, the question is: will we do anything about it? Will we seek to inform and partake in this transition, or will we sit and watch it be misled, criticizing it as it falters and falls? Just as Martin Luther King commented in his 1967 speech, Beyond Vietnam, that it seemed as if America was "on the wrong side of a world revolution," now there is an opportunity to remedy that sad reality, and not simply on a national scale, but global.

Despite all the means and methods of power and domination in this world, for every action, there is an equal and opposite reaction. As things progressively get worse and worse, as any independent observer of the world has noticed, life has a way of creating means and methods to counter these regressions. As 'globalization' has facilitated the emergence of a global elite, and several global institutions and ideologies of global power, so too has this process facilitated the 'globalization of opposition.' So while elites, globally, actively work to integrate and expand global power structures, they are inadvertently integrating and expanding global opposition to those very same power structures. This is the great paradox of our time, and one which we must recognize, for it is not simply a factual observation, but it is a hopeful situation.

Hope should not be underestimated, and it is something that I have personally struggled with in my views of the world. It is hard to see 'hope' when you study so much 'horror' in the world, and see how little is being done about it. But activism and change need hope. This is very evident from the Obama campaign, which was splashed with rhetoric of 'hope' and 'change', something that all people rightfully want and need. However, Obama's 'hope' and 'change' were Wall Street brands and patents, it was a glorious practice in the art of propaganda, and a horrific blow to true notions of 'hope' and 'change'. There is a reason why the Obama campaign took the top prizes in public relations industry awards.

Hope is needed, but it cannot be misplaced hope, as it was with Obama. It must be a hope grounded not in 'blind faith' but in 'honest analysis.' While indeed on most fronts in the world, things are getting progressively worse, the alternative media has focused almost exclusively on these issues that they have blinded themselves to the positive geopolitical developments in the world, namely the 'global political awakening' and the role of the Internet in reshaping global society. While these issues are acknowledged, they are not fully understood or explained within the wider context: that these are in fact, hopeful developments; that there is hope. Wikileaks strengthens this notion, if it is to be taken as an opportunity. A critique without hope falls on deaf ears. No one wants to hear that things are 'hopeless', so while an examination of what is wrong in the world is integral to moving forward, so too is an examination of what is hopeful and positive. This spreads the message and builds its supporters. The Internet as a medium facilitates the spread of this message, and after all, as one of the foremost media theorists, Marshall McLuhan, noted, "The medium is the message."

Appendix of 'Revelations' and 'Vindications': A Call to Action for Alternative Media

So what are some of the supposed 'revelations' which can be used as 'vindications' by the alternative media? Well, for one, the role of royalty as a relevant and powerful economic and political actor in the world today. And by this I do not simply refer to states where monarchs remain as official rulers, such as in Saudi Arabia, but more specifically to West European and notably the British monarchs. For those who have studied institutions like the Bilderberg Group and the Trilateral Commission, the relevance of European royalty in international affairs is not a new concept. For the majority of people (who haven't even heard of the Bilderberg Group or Trilateral Commission), these monarchs are largely viewed as symbolic figures as opposed to political actors. This is, of course, naïve, as all monarchs have always been political actors, however, it is a naivety that has now been challenged on a much wider scale and to a much wider audience. There was a time when I would discuss the relevance of monarchs in the modern world, and it would be a subject that would be treated by many others as an absurd notion: "but the Queen has no real power, she's a figurehead," etc. Wikileaks has exposed that notion as a falsity, and it should be an issue that is expanded upon.

For example, within the Wikileaks cables, take the British Prince Andrew, Queen Elizabeth's second son, who has been subject to many cable 'revelations.' The U.S. Ambassador to Kyrgyzstan wrote a cable regarding a meeting she attended with several British and Canadian businessmen and Prince Andrew, who is a special U.K. trade representative to the Middle East and Central Asia. At the meeting, Prince Andrew ranted against "those [expletive] journalists ... who poke their noses everywhere," and he "railed at British anticorruption investigators, who had had the 'idiocy' of almost scuttling the al-Yamama deal with Saudi Arabia," particularly "referencing an investigation, subsequently closed, into alleged kickbacks a senior Saudi royal had received in exchange for the multi-year, lucrative BAE Systems contract to provide equipment and training to Saudi security forces." When he ranted against the media – specifically the Guardian paper – for making it harder to do business abroad, the U.S. Ambassador noted that the businessmen in attendance "roared their approval" and "practically clapped." Again, evidence for how elites despise true representations of democracy and freedom.

At that same meeting, Prince Andrew made another startling claim, and one which had not been as widely publicized in the media to date. He stated that to the U.S. Ambassador that: "the United Kingdom, Western Europe (and by extension you Americans too) were now back in the thick of playing the Great Game," and, "this time we aim to win!" Further, Prince Andrew – the 'Duke of York' – "then stated that he was very worried about Russia's resurgence in the region," and referred to Chinese economic and political expansion in the region as "probably inevitable, but a menace." On the way out of the meeting, one British businessman said to the U.S. Ambassador, "What a wonderful representative for the British people! We could not be prouder of our royal family!"[20] Well, there you have it, a rich prince running around the world with rich businessmen promoting their economic interests in foreign countries and referring to it as the age-old imperial competition between Britain and Russia in the "Great Game" for dominance over Central Asia. And we call our countries 'democracies' and exporters of 'freedom'?

This is quite typical behaviour of the royal family, however, as a former South African MP and anti-corruption campaigner, Andrew Feinstein, explained, "the royal family has actively supported Britain's arms sales, even when corruption and malfeasance has been suspected," and that, "the royal family was involved in trying to persuade South Africa to buy BAE's Hawk jets, despite the air force not wanting the planes that cost two and a half times the price of their preferred aircraft. As an ANC MP at the time, I was told that £116m in bribes had been paid to key decision-makers and the ANC itself. The royal family's attitude is part of the reason that BAE will never face justice in the UK for its corrupt practices."

The British royals are also very close with Arab monarchs, which makes sense, considering it was the British Empire (and the 'Crown' behind it) that created the Arab monarchs and gave them power in the first place. Prince Andrew went on hunting trips with the King of Jordan and the Chief of Staff of the Armed Forces of the UAE. Further, Prince Charles is considered a strategic diplomatic figure in regards to Saudi Arabia, as the cables reveal. The British media headlined with the 'revelation' that Prince Charles is not as "respected" as Queen Elizabeth, but the real story was buried in the same article beneath the royal gossip, as cables revealed that Prince Charles and his wife "have helped to overcome 'severe strains' following Saudi Arabia's imprisonment and torture of five Britons from December 2001 to August 2003 and the UK's official fraud investigations of British Aerospace operations in Saudi Arabia in 2004." As one U.S. diplomatic cable explained, the British royals "helped re-build UK-Saudi ties" as "the House of Saud and the House of Windsor build upon their royal commonality." In other words, they both represent unelected and unaccountable elite dynastic power, and so they should naturally work together in 'their' own interests. How 'democratic' of them. Further, a Saudi royal threw a lavish party for Prince Charles in Saudi Arabia with the help of an unnamed British businessman.

It looks, however, like the British royals will have to again move in to "smooth out" ties with Saudi Arabia, as 'revelations' about the country and its monarch paint a picture of a not-so-helpful Western ally. In short, Saudi Arabia and its monarch have received one of the largest public relations disasters in recent history. The British monarch may be too busy cleaning up their own mess, or have too much light on them at the moment, to be able to 'gracefully' maneuver through yet another 'imperious' royal visit. What am I referring to here in terms of bad PR for the Saudis? It's quite simple, the Saudi royals, good friends of the British monarch, are incidentally the principle financiers of Sunni terrorists (which includes what we commonly refer to as 'al-Qaeda') worldwide.

While this comes as no surprise to those who have critically analyzed al-Qaeda or the "war on terror," it is indeed a 'revelation' to the majority of people. While Western governments and media propaganda machines have for years blamed terrorist financing and support on 'target' nations like Afghanistan, Iraq, Iran and more recently, Pakistan and Yemen, the Wikileaks cables 'vindicated' the historical and present reality that it is in fact the main Western allies in the region, especially Saudi Arabia, but also the other major Gulf Arab states (and their monarchs), who are the main financiers and supporters of terrorism, and most notably, al-Qaeda. A memo signed by Hillary Clinton confirmed that Saudi Arabia is understood to be "the world's largest source of funds for Islamist militant groups such as the Afghan Taliban and Lashkar-e-Taiba," as well as al-Qaeda itself. Further, three other Arab states, Qatar, Kuwait, and the United Arab Emirates are listed as other chief terrorist financiers. As the Guardian put it, "the cables highlight an often ignored factor in the Pakistani and Afghan conflicts: that the violence is partly bankrolled by rich, conservative donors across the Arabian Sea." While Pakistan is largely blamed for aiding the Taliban in Afghanistan, it is in fact Saudi Arabia as well as UAE-based businesses which are its chief financiers. Kuwait, another staunch U.S. ally, is a "source of funds and a key transit point" for al-Qaeda.

While the New York Times was busy declaring Wikileaks as providing a "new consensus" on Iran, with the Saudi King urging America to attack and "cut the head off the snake," they mentioned only in passing, how "Saudi donors remain the chief financiers of Sunni militant groups like Al Qaeda." Now, while these are indeed 'revelations' to many, we must place these facts in their proper context. This is not simply to be taken as Saudi Arabia and Arab states being responsible, alone, for support of terrorism and al-Qaeda, but that they are simply playing the role they have always played, and that diplomacy is sidelined and kept in the dark on this issue as it always has been.

What I mean by this is that the contextualization of these facts must be placed in a comprehensive historical analysis. Looking at the history of al-Qaeda, arising out of the Soviet-Afghan War, with major covert support from America and other Western allies, the center of this operation was in the 'Safari Club,' which constituted a secret network of Western intelligence agencies (such as those of France, Britain and America) and regional intelligence agencies (such as those of Saudi Arabia and Pakistan), in carrying out the financing, training, arming and operational support of the Mujahideen, and subsequently the Taliban and al-Qaeda. The 'Safari Club' was established in 1976 (with the help of CIA director at the time, George H.W. Bush, another close friend of the Saudi royals), and was designed to respond to increasing political oversight of intelligence operations in America (as a result of the Church Committee investigations on CIA operations), and so the Safari Club was created to allow for a more cove and discreet network of intelligence operations, with no oversight. Diplomats were kept in the dark about its operations and indeed its existence, while the quiet covert relationships continued behind the scenes. This network, in some form or another, exists up to the present day, as I recently documented in my three-part series on “The Imperial Anatomy of al-Qaeda.”

[In short, there is a reason that while diplomats complain quietly about Saudi and Arab financing and support for al-Qaeda, nothing is actually done: because through other avenues, the American imperial structure and apparatus supports and facilitates this process. Diplomacy is more overt in its imperial ambitions, thus the reality of the cables reflecting a focus on Iran and Pakistan, yet intelligence operations are a much more covert means of establishing and maintaining particular imperial relationships. This information again should not be taken “at face value,” but rather placed within its broader geopolitical context. In this sense, the information is not ‘disinformation’ or ‘propaganda’, but rather additional factual ‘vindication’ and information.

While Western governments and media publicly scorn Iran and accuse it of “meddling” in the affairs of Iraq, and of supporting terrorism and destabilization of the country, the reality is that while Iran certainly exerts influence in Iraq, (after all, they are neighbours), Saudi Arabia is a far greater source of destabilization than Iran is accused of being, and this is from the mouths of Iraqi leaders themselves. Iraqi government officials, reported the Guardian, “see Saudi Arabia, not Iran, as the biggest threat to the integrity and cohesion of their fledgling democratic state.” In a cable written by the U.S. Ambassador to Iraq, it was explained that, “Iraq views relations with Saudi Arabia as among its most challenging given Riyadh’s money, deeply ingrained anti-Shia attitudes and [Saudi] suspicions that a Shia-led Iraq will inevitably further Iranian regional influence.” Further, “Iraqi contacts assess that the Saudi goal (and that of most other Sunni Arab states, to varying degrees) is to enhance Sunni influence, dilute Shia dominance and promote the formation of a weak and fractured Iraqi government.” In short, that would mean that Saudi Arabia is actually doing what the West accuses Iran of doing in Iraq. So while Iran certainly has been promoting its own interests in Iraq, it is more interested in a stable Shi’a government, while Saudi Arabia is more interested in a weak and fractured government, and thus promotes sectarian conflict. One interesting fact to note that came out of the cables, is the increasing perspective among Iraqi youth rejecting foreign interference from any government, with diplomatic cables articulating that, “a ‘mental revolution’ was under way among Iraqi youth against foreign agendas seeking to undermine the country’s stability.”

It should come as no surprise, then, that one top Saudi royal (in fact the former head of Saudi Arabia’s intelligence agency and thus the man responsible for handling Saudi Arabia’s relationship with terrorists), Prince Turki al-Faisal, said that the source of the diplomatic leaks should be “vigorously punished.” Turki, who has also been the Saudi Ambassador to the U.K. and America, said, “the WikiLeaks furor underscored that cyber security was an increasing international concern.”

What other areas can Wikileaks be used to further inform and ‘vindicate’ the critical media? Well, start with Saudi Arabia’s neighbour to the south, Yemen. Whether or not most Americans (or for that matter, most people in general) are aware that America is waging a war in Yemen, just across the water from where America is waging another war against Somalia (since 2006/07). This past October, I wrote an article about the imperial war in Yemen as a war being fought under the auspices of the “War on Terror” and fighting al-Qaeda (financed by the Saudi elite); but which in reality is about America and other Western imperial powers (such as the U.K.) propping up a despotic leaders who has been in power since 1978, by supporting him in his campaign to eliminate a rebel movement in the North and a massive secessionist movement in the South. Saudi Arabia entered the conflict in August of 2009 by bombing rebel holdouts in the North along the Saudi border, as the Saudi elite are afraid of the movement spreading to disaffected groups within Saudi Arabia itself.

America inserted itself into the war by increasing the amount of money and military aid given to Yemen (in effect, subsidizing their military, as they do heavily with Saudi Arabia, Egypt, Jordan, Israel, all the Arab states, and dozens of other states around the world), as well as providing direct special forces training and assistance, not to mention carrying out missile strikes within Yemen against "al-Qaeda training camps" which American intelligence officials claimed killed 60 'militants'. In reality, 52 innocent people died, with over half of them being women and children. At the time, both Yemen and America claimed it was an al-Qaeda training camp and that the cruise missile was fired by the Yemeni government, despite the fact that it had no such weapons in its arsenal, unlike the U.S. Navy patrolling the coastline. The missile strike was carried out by America "on direct presidential orders."

Several days later, there was the bizarre "attempted terrorist attack" in which a young Nigerian man was arrested attempting to blow up his underwear (who was helped onto the plane by a mysterious Indian man in a suit who claimed he was a diplomat, according to witnesses), and who was subsequently linked to "al-Qaeda in the Arabian Peninsula" (an organization which started up not much earlier when a Guantanamo inmate returned to Saudi Arabia only to 'escape' Saudi custody, and flee to Yemen to start a new al-Qaeda branch). This provided the justification for America to dramatically increase its military aid to Yemen, which more than doubled from $67 million to $150 million, and came with increased special forces training and assistance, as well as increased CIA activity, discussing using drone attacks to kill innocent people (as they do in Pakistan), and more missile strikes.

This previous September, the Yemen government "laid siege" to a town in the South while the Obama administrations top counter-terrorism official, John Brennan, was in Yemen for 'talks' with President Saleh. The town was claimed to be a "sanctuary for al-Qaeda," but it has key strategic significance as well. It is just south of a major new liquid natural gas pipeline, and the town happened to be home to many people involved in the Southern secessionist movement. The Yemeni government "barred" any outside or independent observers from witnessing the siege, which lasted days. However, for the many who fled the conflict and "siege," they were claiming that the Islamic militants were working with the government against the rebel movement in the North and secessionist movement in the South, and according to one NPR reporter, "this is more about fighting or subduing the secessionist movement than it is about al-Qaida."

The Wikileaks 'revelations' further inform and confirm much of this analysis. In regards to the missile strike that killed innocent women and children on Obama's orders, Wikileaks cables revealed that Yemeni President Saleh "secretly offered US forces unrestricted access to his territory to conduct unilateral strikes against al-Qaida terrorist targets." As Saleh told John Breannan in September of 2009, "I have given you an open door on terrorism. So I am not responsible." Regarding the December 21 strike that killed the innocent civilians, a cable explained, "Yemen insisted it must 'maintain the status quo' regarding the official denial of US involvement. Saleh wanted operations to continue 'non-stop until we eradicate this disease," and days later in a meeting with U.S. Central Command head, General David Patraeus, "Saleh admitted lying to his population about the strikes." He told the General, "We'll continue saying the bombs are ours, not yours."

In regards to Pakistan, while it is important to be highly critical of the validity of the 'perspectives' within the cables in regards to Pakistan and the Taliban, since Pakistan is a current and escalating target in the "War [OF] Terror," there are things to keep in mind: historically, the Pakistani ISI has funded, armed and trained the Taliban, but always with U.S. assistance and support. Thus, we must examine the situation presently and so historically. Wikileaks revealed (as I mentioned previously), that Arab Gulf states help fund the Taliban in Afghanistan, so the common claim that it is Pakistan 'alone' is immediately made to be erroneous. Is it possible that Pakistan is still working with the Taliban? Of course. They have historically through their intelligence services, the ISI, and while they have never done it without U.S. support (mostly through the CIA), the ISI still receives most of its outside funding from the CIA.[29] The CIA funding of the ISI, a reality since the late 70s, picked up dramatically following 9/11, the operations of which the ISI has been itself complicit in financing. Thus, the CIA rewarded the financiers of 9/11 by increasing their funds.

The trouble with discounting information that does not fit in with your previously conceived ideas is that it does not allow for evolution or progress in thinking. This should never be done in regards to any subject, yet it is commonly done for all subjects, by official and critical voices alike. With Pakistan, we must understand that while historically it has been a staunch U.S. ally in the region, propping up every government, supporting every coup, American geopolitical ambitions have changed as a result of the changing geopolitical reality of the world. Pakistan has drawn increasingly close to China, which built a major seaport on Pakistan's coast, giving China access to the Indian Ocean. This is a strategic threat to India and the United States more broadly, which seeks to subdue and control China's growing influence (while simultaneously attempting to engage in efforts of international integration with China, specifically economically). India and Pakistan are historical enemies, and wars have been fought between them before. India and America are in a strategic alliance, and America helped India with its nuclear program, much to the distaste of the Pakistanis, who drew closer to China. Pakistan occupies an area of the utmost strategic importance: with its neighbours being Afghanistan, China, India and Iran.

American policy has changed to support a civilian government, kept weak and subservient to U.S. interests, while America covertly expands its wars inside Pakistan. This is creating an incredible potential for absolute destabilization and fragmentation, potentially resulting in total civil war. America appears to be undertaking a similar policy in Pakistan that it undertook in fracturing Yugoslavia throughout the 1990s. Only that Pakistan has a population of 170 million people and nuclear weapons. As America expands its destabilization of Pakistan, the risk of a nuclear war between Pakistan and India dramatically increases, as does the risk of destabilization spreading regionally to its neighbours of India, China, Afghanistan and Iran. The American-urged separation of the Pakistani military from official power in Pakistan (as in, it's not a military dictatorships), was designed to impose a completely U.S. dependent civilian government and isolate an increasingly frustrated and antagonized Pakistani military.

As the Wikileaks cables revealed, General Kayani, head of the Pakistani military, threatened to depose the Pakistani government in a coup in March of 2009, and he discussed this in meetings with the U.S. Ambassador to Pakistan, Anne Patterson. The cables revealed that the Pakistani Army Chief disliked the civilian government, but that they disliked the opposition even more, which was rallying people in the streets.[31] This reveals the intimate nature the U.S. has with the Pakistani military, as it always has. The U.S. did not support this proposal, as it currently favours a weak civilian government, and therefore a strong military dictatorship is not in America's (or India's) interest. Thus, there was no coup. Hence, Wikileaks can be used to further inform and vindicate analysis of Pakistan. For those who have been speaking about the destabilization of Pakistan for years, and there have been many, Wikileaks provides more resources to a critical analysis, and suddenly more people around the world might be interested in new ideas and perspectives, as Wikileaks has challenged so many of their previously held beliefs.

The list of examples surfacing from the Wikileaks cables is endless in the amount of additional information it can add in the alternative media's dissemination of information and analysis. These were but a few examples among many. Make no mistake, this is an opportunity for the spread of truth, not a distraction from it. Treat it accordingly.

__Andrew Gavin Marshall__ is a Research Associate with the Centre for Research on Globalization (CRG). He is co-editor, with Michel Chossudovsky, of the recent book, «The Global Economic Crisis: The Great Depression of the XXI Century,» available to order at Globalresearch.ca. He is currently writing a book on 'Global Government' due to be released in 2011 by Global Research Publishers.

How to Fight and Win the Cyberwar

We should think of cyberattacks as guided missiles and respond similarly—intercept them and retaliate.

Source:
http://online.wsj.com/article/SB10001424052748703989004575652671177708124.html

Several years ago, during the presidency of George W. Bush, many banks and Wall Street firms were knocked offline. The financial industry, which had long been considered to have the best safeguards against cyberinfections in the private sector, discovered its computers had been penetrated by a worm, so-called because a virus grown on one computer can worm its way to millions of others. Mr. Bush asked then Treasury Secretary Hank Paulson to examine what it would take to protect our critical infrastructures. The upshot was that steps were taken to strengthen the security of the military networks, but little else was done.

The major shock about the mischievous WikiLeaks—even more than the individual headline items—is that it dramatizes how vulnerable we still are. Digitization has made it easier than ever to penetrate messages and download vast volumes of information. Our information systems have become the most aggressively targeted in the world. Each year, attacks increase in severity, frequency, and sophistication. On July 4, 2009, for instance there was an assault on U.S. government sites—including the White House—as well as the New York Stock Exchange and Nasdaq. There were similar attacks that month on websites in South Korea. In 2008, our classified networks, which we thought were inviolable, were penetrated. Three young hackers managed to steal 170 million credit-card numbers before the ringleader was arrested in 2008.

The Internet was originally intended for thousands of researchers, not billions of users who did not know and trust one another. The designers placed a higher priority on decentralization than on security. They never dreamed the Internet could be used for commercial purposes or that it would eventually control critical systems and undergird the world of finance. So it is not surprising that the Internet creators were comfortable with a network of networks rather than separate networks for government, finance and other sectors.

A symbol to many of the open communication of American culture, the Internet has thus evolved into a two-edged sword. Our extensive systems facilitate control of pipelines, airlines and railroads; they energize commerce and private banking. They give us rapid access to medical and criminal records. But they also offer a growing target for terrorists and thieves.

Most people who experience “malware” have been victims of so-called phishing, whereby criminals pretending to be bank employees, for example, trick the gullible into revealing account numbers and passwords. But cyberwarriors can do damage on a much larger scale, as former White House counterterrorism czar Richard Clarke points out in his revealing book “CyberWar,” published earlier this year. They can tap into these networks and move money, spill oil, vent gas, blow up generators, derail trains, crash airplanes, cause missiles to detonate, and wipe out reams of financial and supply-chain data. Havoc can be created at the blink of an eye from remote locations overseas. Criminal groups, nation-states, terrorists and military organizations are at work exfiltrating vast amounts of data from the U.S. public and private sectors.

Another worrisome threat is the distributed denial of service attack, a deluge of Interne traffic specifically intended to crash or jam networks. Hackers using malicious computer code can mobilize a "botnet," or robotic network, of hundreds of thousands of machines that simultaneously visit certain websites to shut them down.

More recently, a virus that targets special industrial equipment has become widely known as the "Stuxnet" attack. This is the worm that this fall reportedly infiltrated the computers controlling Iran's nuclear centrifuge facilities, thereby delaying or even destroying its nuclear-weapons program (the one Iran denies it has). It is the world's first-known super cyberweapon designed specifically to destroy a real-world target.

Similarly, many believe that the immobilization of hundreds of key sites in independent Georgia in 2008 was a Russian government operation accompanying its kinetic war in support of breakaway regions in the former Soviet republic. In a cyberattack on South Korea last year, an estimated 166,000 computers in 74 countries flooded the websites of Korean banks and government agencies, jamming their fiber optic cables.

Mr. Clarke argues in his book that China is one of the key players in developing a cyberwar capability. The Chinese use private hackers to engage in widespread penetration of U.S. and European networks, successfully copying and exporting huge volumes of data. That's on top of their capacity to attack and degrade our computer systems and shut down our critical networks. He believes that the secrets behind everything from pharmaceutical formulas, bioengineering designs, and nanotechnologies to weapons systems and everyday industrial products have been stolen by the Chinese army or private hackers who in turn give them to China.

The United States has done little to enhance the safety of the networks that bolster our economy. We urgently need to develop defensive software to protect these networks and create impermeable barriers to the profusion of malware. Network convergence—transporting all communications over a common network structure—increases the opportunities for and the consequences of disruptive cyberattacks. Hackers and cyberwarriors are constantly devising new ways to trick systems.

Not many people realize that all of our nation's air, land and sea forces rely on network technologies that are vulnerable to cyberweapons, including logistics, command and control, fleet positioning and targeting. If they are compromised or obliterated, the U.S. military would be incapable of operating. It does not help that there is a disproportion between offense and defense. The average malware has about 175 lines of code, which can attack defense software using between 5 million and 10 million lines of code.

It is currently incredibly challenging to figure out the source of an attack, and this in turn inhibits our capacity to prosecute the wrongdoers or retaliate. Malicious programmers are always able to find weaknesses and challenge security measures. The defender is always lagging behind the attacker.

The task is of such a scale that it needs nothing less than a souped-up Manhattan Project, like the kind that broke the scientific barriers to the bomb that ended World War II. Our vulnerabilities are increasing exponentially. Cyberterrorism poses a threat equal to that of weapons of mass destruction. A large scale attack could create an unimaginable degree of chaos in America.

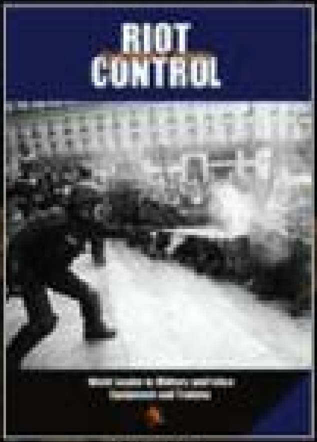
We should think of cyberattacks as guided missiles and respond similarly—intercept them and retaliate. This means we need a federal agency dedicated to defending our various networks. You cannot expect the private sector to know how—or to have the money—to defend against a nation-state attack in a cyberwar. One suggestion recommended by Mr. Clarke is that the government create a Cyber Defense Administration. He's right. Clearly, defending the U.S. from cyberattacks should be one of our prime strategic objectives.

Few nations have used computer networks as extensively as we have to control electric power grids, airlines, railroads, banking and military support. Few nations have more of these essential systems owned and operated by private enterprise. As with 9/11, we do not enjoy the luxury of a dilatory response.

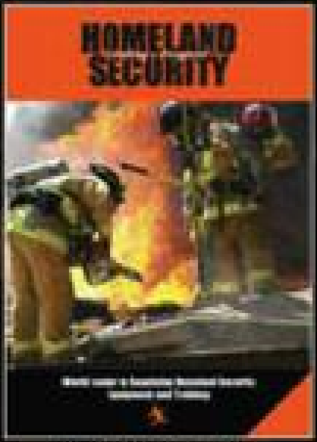
Mr. Zuckerman is chairman and editor in chief of U.S. News & World Report.

ONE STOP SHOP

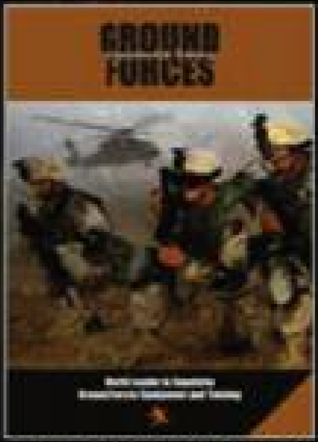
E



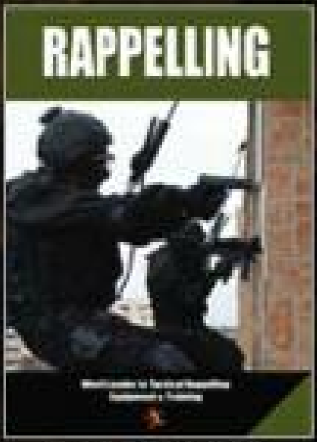
RIOT CONTROL



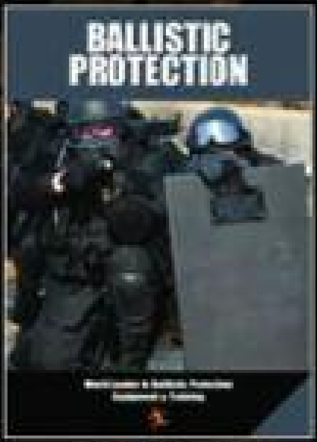
HOMELAND SECURITY



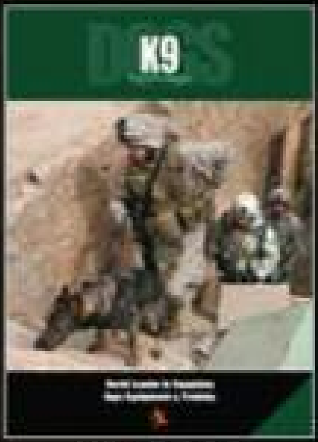
GROUND FORCES



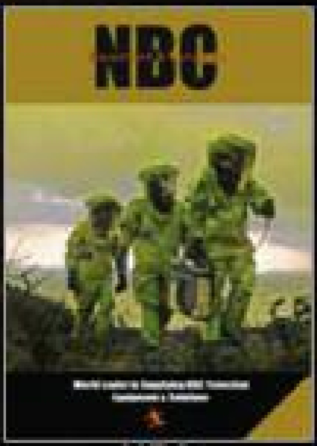
RAPPELLING



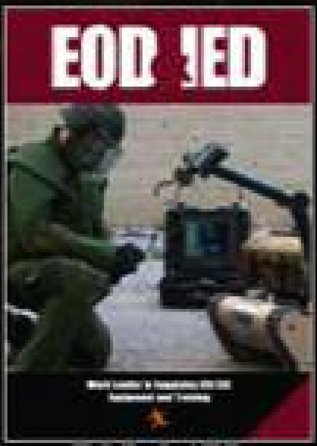
BALLISTIC PROTECTION



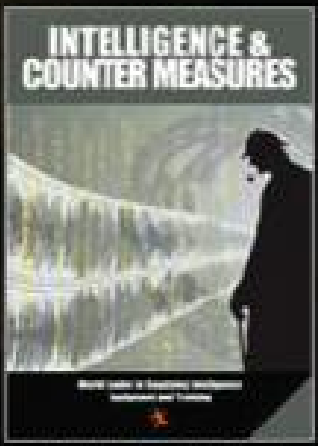
K9 - DOGS



NBC

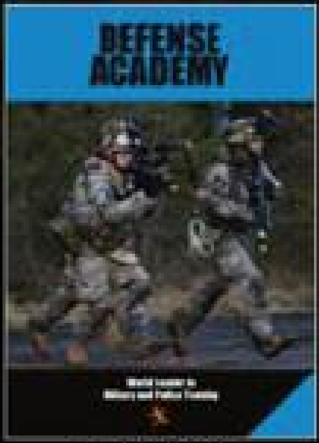


EOD & IED

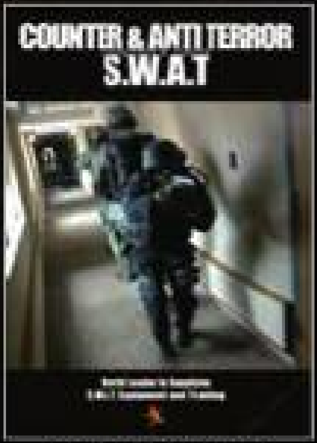


INTELLIGENCE

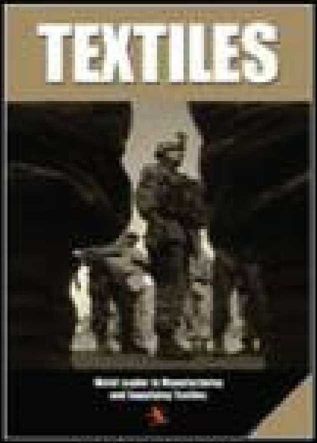
TAR
Ideal Concepts Ltd.
3, Maavar Yabok St., Tel-Aviv 67440 Israel
Tel: +972-3-6914564
Fax: +972-3-6914567
www.tarideal.com



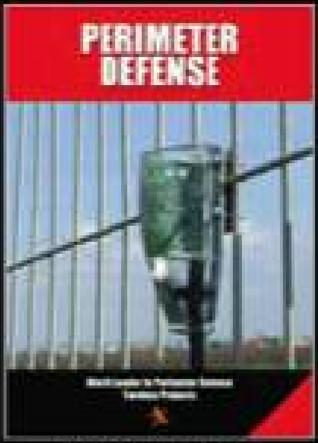
DEFENSE ACADEMY



ANTI-TERROR S.W.A.T.



TEXTILES



PERIMETER DEFENSE

Android phones more vulnerable to cyber attacks than Apple iPhone

Source:http://homelandsecuritynewswire.com/android-phones-more-vulnerable-cyber-attacks-apple-iphone

Android smart phones are more susceptible to hacking and viruses than Apple’s iPhone; the Android operating system is open source, allowing hackers to understand the underlying code; Apple iPhone may have a safer operating system, but it is not impervious to attacks; McAfee warns that 2011 will see hackers increasingly target mobile devices like Android phones, iPads, and iPhones. Android smart phones may be more susceptible to hacking and viruses than Apple’s iPhone. According to Steve Chang, chairman of Trend Micro Inc., the Android operating system is based on open source coding which allows programmers greater flexibility and ease in disseminating apps, but also makes it vulnerable to hackers with malicious intent. The open source code allows hackers to understand the underlying architecture and source, enabling them easily to design harmful software. controls its software more tightly and follows a stricter app approval process. Before an app can be sold in Apple’s app store, it must be approved by Apple. Android allows programmers freely to disseminate their apps. Apple’s iOS software, used in its iPhone, iPad, and other mobile devices, also contains built-in security measures. “Apple has a sandbox concept that isolates the platform, which prevents certain viruses that want to replicate themselves or decompose and recompose to avoid virus scanners,” Chang said. Google’s Android platform for smart phones was introduced in 2008 in conjunction with various hardware and software developers including Intel, HTC, ARM, Motorola, and Samsung as part of the Open Handset Alliance. The Open Handset Alliance embraces elements of open source computer culture which believes in giving free access to a product’s source code. The goal is to unleash the creative energies and harness the collective power of programmers around the world to create better software, applications, or programs. Other major open source projects include the Linux operating system for computers. While comparatively safer than the Android operating system,Apple’s operating system is not entirely impervious to hackers. “Apple’s iOS isn’t fully immune to security threats and may be hit with so-called social-engineering attacks, which trick users into authorizing the download or installation of malicious software,” Chang said. McAfee Inc. warns that Apple’s iPhone and other mobile devices will be the target of hackers in 2011. The increasing popularity of such technology and the relative lack of consumer awareness for safety leave these devices at risk for data and identify theft. Currently RIM dominates the U.S. smart phone market with 33 percent, while Google’s Android is second with 26 percent and Apple’s iOS trails with 17 percent in third. Google’s Android has rapidly gained market share since it was first introduced, leaping from 3.8 percent of the U.S. market in 2009 to its current 26 percent. Based on its rapid growth, some predict that the Android will gain market dominance in the U.S in as little as three months.

Globalization?

Source: http://en.wikipedia.org/wiki/VeriChip

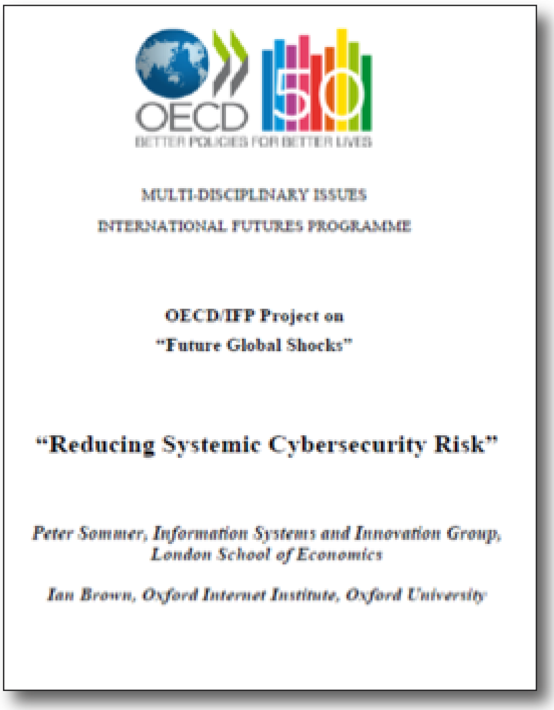
VeriChip is the only Food and Drug Administration (FDA)-approved human-implantable radio-frequency identification (RFID) microchip. It is marketed by VeriChip Corporation, a subsidiary of Applied Digital Solutions, and it received United States FDA approval in 2004. About twice the length of a dime, the device is typically implanted between the shoulder and elbow area of an individual's right arm. Once scanned at the proper frequency, the VeriChip responds with a unique 16 digit number which could be then linked with information about the user held on a database for identity verification, medical records access and other uses. The insertion procedure is performed under local anaesthetic in a physician's office. As an implanted device used for identification by a third party, it has generated controversy and debate.

EDITOR'S NOTE: It is very interesting to Google the chip and read the Internet philology on this contra versus issue…

Fears of cyberwar exaggerated

Source: http://homelandsecuritynewswire.com/fears-cyberwar-exaggerated-report

New report says that analysis of cyber-security issues has been weakened by the lack of agreement on terminology and the use of exaggerated language; the report says online attacks are unlikely ever to have global significance on the scale of, say, a disease pandemic or a run on the banks; the authors say, though, that «localized misery and loss» could be caused by a successful attack on the Internet's routing structure, which governments must ensure are defended with investment in cyber-security training. When the writer of a notorious book for hackers says we should stop panicking about cyberwar, it is probably time to sit up and take notice. "Governments should take a calm, disciplined approach and evaluate the risks of each type of attack very carefully rather than be swayed by scare stories," says Peter Sommer of the London School of Economics. Under the pseudonym "Hugo Cornwall," Sommer published the Hacker's Handbook in 1985. Since then he has become a noted security researcher and expert witness. Now he has co-authored a report for the Organization for Economic Co-operation and Development (OECD) which warns governments against swallowing wholesale stories about "cyberwar" and "cyberweapons". New Scientist reports that in Reducing Systemic Cybersecurity Risk, published yesterday, Sommer says that a true cyberwar would have the destructive effects of conventional war but be fought ex-



OECD
BETTER POLICIES FOR BETTER LIVES

MULTI-DISCIPLINARY ISSUES
INTERNATIONAL FUTURES PROGRAMME

OECD/IFP Project on
"Future Global Shocks"

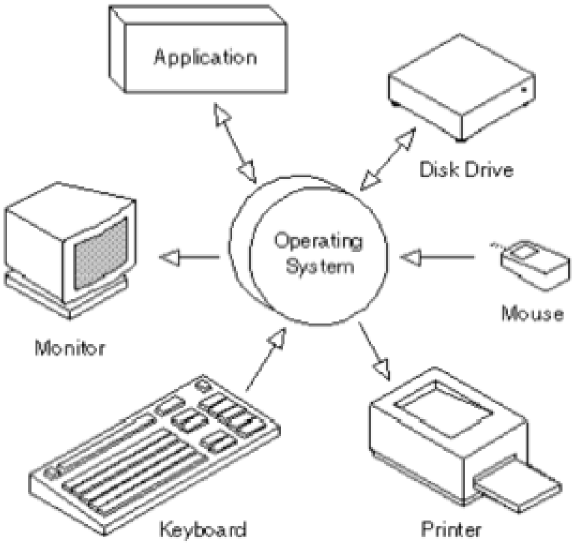
"Reducing Systemic Cybersecurity Risk"

Peter Sommer, Information Systems and Innovation Group, London School of Economics

Ian Brown, Oxford Internet Institute, Oxford University clusively in cyberspace — and as such is a "highly unlikely" occurrence. "Analysis of cyber-security issues has been weakened by the lack of agreement on terminology and the use of exaggerated language," the report says. "Cyber-espionage is not a few keystrokes away from cyberwar, it is a method of spying." Controversially, the OECD advises nations against adopting the Pentagon's idea of setting up a military division — as it has under the auspices of the U.S. Air Force's Space Command — to fight cybersecurity threats. While vested interests may want to see taxpayers' money spent on such ventures, says Sommer, the military can only defend its own networks, not the private-sector critical networks we all depend on for gas, water, electricity, and banking. Co-authored with computer scientist Ian Brown of the Oxford Internet Institute in the United Kingdom, the report says online attacks are unlikely ever to have global significance on the scale of, say, a disease pandemic or a run on the banks. They say, though, that "localized misery and loss" could be caused by a successful attack on the Internet's routing structure, which governments must ensure are defended with investment in cyber-security training. Jay Abbott, a security manager at the consultancy PricewaterhouseCoopers, agrees that the routing structure is indeed vulnerable. "Short of physically cutting the wires, it's the best way to take down a country from the internet," he says.

Protect Operating Systems From Attack

Source: http://news.ncsu.edu/releases/wmssolihinos/



The operating system (OS) is the backbone of your computer. If the OS is compromised, attackers can take over your computer – or crash it. Now researchers at North Carolina State University have developed an efficient system that utilizes hardware and software to restore an OS if it is attacked. At issue are security attacks in which an outside party successfully compromises one computer application (such as a Web browser) and then uses that application to gain access to the OS. For example, the compromised application could submit a "system call" to the OS, effectively asking the OS to perform a specific function. However, instead of a routine function, the attacker would use the system call to attempt to gain control of the OS. "Our goal is to give the OS the ability to survive such attacks," says Dr. Yan Solihin, an associate professor of electrical and computer engineering at NC State and co-author of a paper describing the new system. "Our approach has three components: attack detection; security fault isolation; and recovery." The concept is to take a snapshot of the OS at strategic points in time (such as system calls or interrupts), when it is functioning normally and then, if the OS is attacked, to erase everything that was done since the last "good" snapshot was taken – effectively going back in time to before the OS attack. The mechanism also allows the OS to identify the source of the attack and isolate it, so that the OS will no longer be vulnerable to attacks from that application. The idea of detecting attacks and re-setting a system to a safe state is a well-known technique for restoring a system's normal functions after a failure, but this is the first time researchers have developed a system that also incorporates the security fault isolation component. This critical component prevents the OS from succumbing to the same attack repeatedly. The concept of taking snapshots of the OS and using it to replace the OS if it is compromised was previously viewed as impractical, since taking these snapshots and running such a system significantly slowed computer operating speeds. "But we've developed hardware support that allows the OS to incorporate these survivability components more efficiently, so that they take up less time and energy," Solihin says. The researchers say the survival system takes up less than 5 percent of the OS's operating overhead.

The study abstract follows.

"Architectural Framework for Supporting Operating System Survivability"

Authors: Xiaowei Jiang and Yan Solihin, North Carolina State University

Presented: Feb. 16, 2011, at the IEEE International Symposium on High-Performance Computer Architecture in San Antonio, Texas

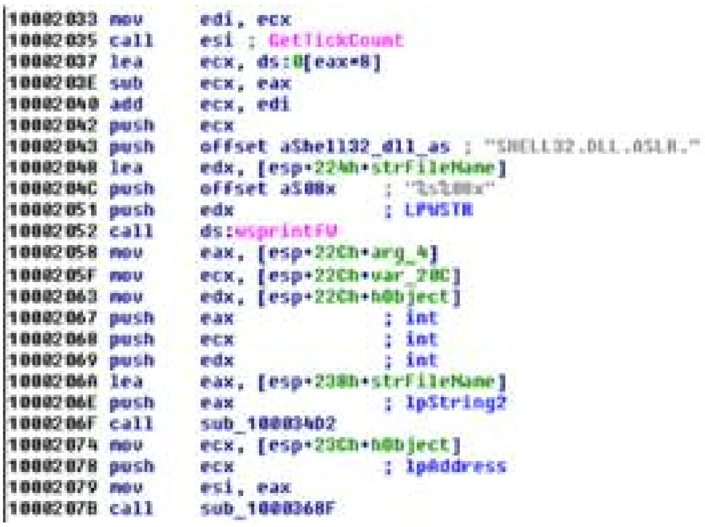
Abstract: The ever increasing size and complexity of Operating System (OS) kernel code bring an inevitable increase in the number of security vulnerabilities that can be exploited by attackers. A successful security attack on the kernel has a profound impact that may affect all processes running on it. In this paper we propose an architectural framework that provides survivability to the OS kernel, i.e. able to keep normal system operation despite security faults. It consists of three components that work together: (1) security attack detection, (2) security fault isolation, and (3) a recovery mechanism that resumes normal system operation. Through simple but carefully-designed architecture support, we provide OS kernel survivability with low performance overheads (<5% for kernel intensive benchmarks). When tested with real world security attacks, our survivability mechanism automatically prevents the security faults from corrupting the kernel state or affecting other processes, recovers the kernel state and resumes execution.

Hackers release Stuxnet's decompiled code online

Source: http://homelandsecuritynewswire.com/hackers-release-stuxnets-decompiled-code-online

The Stuxnet worm was a cybermissile designed to penetrate advanced security systems; it was equipped with a warhead that targeted and took over the controls of the centrifuge systems at Iran's uranium processing center in Natanz, and it had a second warhead that targeted the massive turbine at the nuclear reactor in Bushehr; security experts say it is the most sophisticated cyberweapon ever designed; now, a group of anonymous «hacktivists» hacked the computers of a U.S. security company and stole a decrypted version — the decompiled code — of the malware, and put it on the Web; security experts are anxious: «There is the real potential that others will build on what is being released,» says one; this will not lead to an immediate threat, but it could lead to something soon, he added; «Weeks wouldn't surprise me».

The group of anonymous "hacktivists" that made headlines for online cyberattacks in December just released a bombshell online: a decrypted version of the same cyberworm that crippled Iran's nuclear weapons program. The ones and zeroes that make up the code called the Stuxnet worm — described as the most sophisticated cyberweapon ever created — were reportedly found when the faceless group hacked into the computers of HBGary, a U.S. security company that the anonymous collective viewed as an enemy, Fox News reported. Security experts said the leaked code was serious cause for concern. “There is the real potential that others will build on what is being released,” Michael Gregg, chief operating officer of cybersecurity firm Superior Solutions, told FoxNews.com. Gregg was quick to clarify that the group has not released the Stuxnet worm itself, but rather a decrypted version of it HBGary had been studying — which could act almost like a building block for cybercrooks. “As an attacker you need to understand how something works. The better you understand how it works the easier it is to build something similar that serves the same purpose,” Gregg explained. The “decompiled” code the group made available is in that sense akin to a recipe book for disaster, he said.



```
10002033 mov     edi, ecx
10002035 call    esi ; GetTickCount
10002037 lea     ecx, ds:0[eax*8]
1000203E sub     ecx, eax
10002040 add     ecx, edi
10002042 push    ecx
10002043 push    offset aShell32_dll_as ; "SHELL32.DLL.ASLR."
10002048 lea     edx, [esp+224h+strFileName]
1000204C push    offset aS08x      ; "%s%08x"
10002051 push    edx               ; LPWSTR
10002052 call    ds:wsprintfW
10002058 mov     eax, [esp+22Ch+arg_4]
1000205F mov     ecx, [esp+22Ch+var_20C]
10002063 mov     edx, [esp+22Ch+hObject]
10002067 push    eax               ; int
10002068 push    ecx               ; int
10002069 push    edx               ; int
1000206A lea     eax, [esp+238h+strFileName]
1000206E push    eax               ; lpString2
1000206F call    sub_10003402
10002074 mov     ecx, [esp+23Ch+hObject]
10002078 push    ecx               ; lpAddress
10002079 mov     esi, eax
1000207B call    sub_1000368F
```

A snippet of the Stuxnet source code // Source: data0.net

“With the right tools — and these guys have shown themselves more than once to be a fairly technical bunch of individuals — then it gives others a cookbook to start modifying,” he said. Careful examination of the Stuxnet worm by armies of security analysts have shown it to be a cybermissile designed to penetrate advanced security systems. It was equipped with a warhead that targeted and took over the controls of the centrifuge systems at Iran’s uranium processing center in Natanz, and it had a second warhead that targeted the massive turbine at the nuclear reactor in Bushehr. Stuxnet was designed specifically to take over those control systems and evade detection, and it apparently was very successful. Dave Aitel, CEO of Immunity Inc., painted a firm line between the version of the worm that destroyed Iran’s nuclear plant and the code released by Anonymous. “What they’ve released is essentially incomprehensible,” he said, saying that what the group found was far removed from the raw worm that has been “travelling around Iran destroying nuclear things.” “This is essentially just a translation. HBGary took the worm in the wild and translated it into a slightly easier to read format,” Aitel said. He notes that Stuxnet is still a threat, however, and the more dangerous raw version of the worm — or the “binary” version — is still easily accessible for those wishing to use it maliciously. “The stuxnet binary is widely available,” Aitel told FoxNews.com. “The people who would use the binary would know how to find it.” Orla Cox, a security operations manager at Symantec, told the Guardian that it was “very difficult to tell” how dangerous Anonymous’ copy of Stuxnet is. “It would be possible [for Anonymous to use Stuxnet in an attack],” Cox said. “But it would require a lot of work; it’s certainly not trivial.” A hacker would need to repurpose the single-minded code and retarget it, a likely challenge, experts said. The Anonymous group released the Stuxnet code on 13 February, after finding it in a database of e-mails it stole from HBGary. “First public Stuxnet decompile is to be found here,” one representative of the group wrote over Twitter. Anonymous claims the hacking was a response to HBGary’s purported efforts to penetrate the group and identify its members. The reasons for releasing the Stuxnet code are unclear, be they malicious or merely anarchist. The ramifications, experts say, are far less obscure. “Now that pieces of that code become available, it’s not a far step to others developing their own attack kits, Gregg told FoxNews.com. “Just because they don’t have malicious intent with it doesn’t mean others wouldn’t.”

This will not lead to an immediate threat, but it could lead to something soon, Gregg said. “Weeks wouldn’t surprise me.”

Stuxnet worm's true origins are exposed

Source: http://www.worldsecuritynetwork.com/showArticle3.cfm?article_id=18540&topicID=33

It's breaking dawn by a beachside command center for Hezbollah. But already, the commander has been up for hours in anticipation of the day's work – the simultaneous annihilation of revered European cultural sites and the inner border of Israel. The former attack sites have been indiscriminately chosen to garner world attention. The latter would be retribution for, well, for just being. All the commander needs to do now is give the word.

- **Virus intended as «weapon of peace»**
- **Origins date back over 30 years, not 2009 as estimated**
- **U.S., KGB, Israel, Canada, Australia and others have all had earlier versions**
- **Proliferation may continue undetectable with experts only having solved «false flags»**
- **Changes landscape of modern warfare as we know it**

He picks up the receiver of his impenetrable, mega-million-dollar communications system installed to withstand all but a nuclear war. But the receiver is silent, no dial tone. Dead. Impatient but unperturbed, he turns to his cell phone. No service. By now, he is on a rampage, waking up the entire installation with shouts of ineptitude. Others come to his aide, aimed at restoring lines. But they too encounter silence. No phones, no fax, no Internet. Back to the Middle Ages. There will be no war today. No missiles fired. Without communication, there is no relaying of orders. The best laid plans of sabotage gone astray.

An event like this did happen this past fall in the Mid-East, according to two deep, inside sources of mine. Except that there were actually five command centers, and all five went down simultaneously. There was still worse chaos, 40 minutes later, explosions ratcheting the air like a blitzkrieg, underground weapons caches exploding in place. The command centers knew the explosions were close, but with no communications, knew not where – they couldn't relay offensive orders, deploy defensive actions, or even discern what was going down.

A neighboring nation came to the rescue, their radar detecting enemy jets over Lebanon skies and scrambling its fighter jets. Except in truth, there were no enemy jets to be found, just sunny, cloudless skies. Much like communications at the command center, that neighboring air force's radar had been manipulated.

Off in a different country, in the land of an enemy combatant, there were wry smiles among those in the know. This had all been a long time coming. Not just years, but decades. Because they knew survival might come down to just such a day. And so they had planned well for their Trojan horse, the smallest, most microscopic of masquerades. The malware worm, Stuxnet.

Nineteen hours later, all communications order was miraculously restored in Beirut and radar resumed working. But there was then another type of silence at command and air control centers because one player in this game of chess had showed that it could start and stop all communications at the drop of a hat, and turn them back on at whim. A message that to others might be subtle is not subtle to a trained eye in war.

As they might say in War College, "We choose the time, the place, and the element." The element, in this case, was the worm, Stuxnet. And the message was clear: Any time, any place. Our choosing.

To some, the worm is a noble weapon, to the recipient, ignoble.

Some might find a noble weapon an oxymoron. But let me relay comments of Geir Lundestad, Secretary of the Norwegian Nobel Committee at an Oslo presentation attended by an associate of mine. Lundestad said the esteemed Nobel Peace Prize is sometimes awarded not for accomplishments toward peace, but as a deterrent to war. "The prize can actually influence outside events," he said. Lech Walesa said that he would not have achieved Solidarity's victory in Poland in 1989, had he not earlier received the Nobel Peace Prize. Likewise, East Timor winners said their prize in 1996 helped that country become independent. Lundestad said the Committee had "adapted the definition of peace. The Nobel Peace Prize is also a protective device." He said Committee members ask themselves, "What can we actually do for peace?"

And so now we have the worm opening undetectable doors not visible to the naked eye. But like the Nobel Peace Prize, the doors opened are with the ultimate goal being to deter war and maintain peace. The goal is to fight and win a war with no bloodshed, with few if any human casualties.

The worm, Stuxnet, is a Trojan horse said to have disabled Iran's nuclear weapons program. The New York Times said late last year, «Meanwhile, the search for other clues in the Stuxnet program continues — and so do the theories about its origins.»

The Times updated their take on January 15, 2011 calling Stuxnet, "the most sophisticated cyberweapon ever deployed…experts who have picked apart the computer worm describe it as far more complex — and ingenious — than anything they had imagined when it began circulating around the world, unexplained, in mid-2009."

Other major news outlets report it as an attack that was the perfect storm leaving no fingerprints, or that it should have won "Person of the Year" for its impact on world events. Still others at first tried to decipher cryptic language within the worm, supposedly tied to this or that chapter of the bible. In other words, no one has much clue as to the true Stuxnet origin. That's because no one has been looking back far enough. As Santayana said, "Those who cannot remember the past are doomed to repeat it."

No one is looking back to a time in the mid-70s, when an obscure program called Promis first reared its head. Promis, according to sources, is at the root of Stuxnet. Promis was a computer program that promised to help US prosecutors track criminals and legal maneuverings through the system, "Prosecutor's Management Information System." The people-tracking software was later marketed by a firm named Inslaw, under the auspices of William Hamilton, a former NSA officer who still markets a version of the product today.

The Department of Justice became intrigued by Promis, seeing its potential for exorbitant legal case-management and provided funding for improvements. As Promis morphed, its capabilities refined, its natural alternative applications became self-evident: the worlds of intelligence, terrorists and targets.

Rafi Eitan, head of the Israeli Defense Ministry's Lekem in the early 1980s, a clandestine, scientific and technological intelligence unit, attended a presentation of Promis under an assumed name. He was so impressed with

«This is a big worry for the future," warns Scott Borg, Director and Chief Economist of U.S. Cyber Consequences Unit, an independent, non-profit research institute. "We are entering a completely new defense era. If you have the tools like Stuxnet, why would you bother with missiles? Why bother invading with an army? The whole relationship between the military and society is going to have to be re-thought."

it that he obtained a copy – how, and whether legally, is another story. Suffice it to say that he especially saw its potential for tracking the spidery web of PLO installations around the world, at the time under Yasser Arafat, as well as tracking the leader himself. Eitan, however, wanted a "trapdoor", a built-in chip so that if Promis was later sold to other organizations, Israeli intelligence could track the information for which those entities might search. Big brother tracking little brother, or intelligence tracking of intelligence.

Boldly, Eitan then arranged for Arafat himself to buy the Promis program for his security needs, this according to author Gordon Thomas. But the trapdoor instead allowed Israeli intelligence to follow Arafat's aliases on the lam. You can run, but you can't hide from Promis. And here's where it gets really interesting.

By the late 1980s, Promis programs had been sold to Britain, Australia, South Korea and Canada. Allies harmless enough, right?

But then up next was the KGB. There are multiple claims as to who sold Promis to the Russians. Several, including a source of mine, said it was newspaper mogul Robert Maxwell in assistance to Israel. Another acquaintance, former double agent David Dastych (Polish intell working for the CIA during the Cold War) said that an American intelligence officer admitted to him, "Yes, we gave Promis to the Russians and Chinese to back door their intel. Worked like a charm." Both claims may overlap.

In fact, the KGB is said to have used Promis for over 15 years. At first, there was nothing to suspect since malicious malware had not really been coined. Few back then understood the power of the computer, and so the Trojan horse entered the realms of international espionage, the microscopic spy.

As former US Attorney General Elliot Richardson later said on Australia's TV show, A Current Affair, in 1990 regarding Promis, "The US Government had through clandestine means planted software on foreign intelligence agencies so the US would be better able, the phrase goes, to read their mail."

The only problem was the "blowback", David Dastych reported. "As we gave it to our enemies in order to back door them through the trap door in Promis, we left 64 federal agencies open in the US Government who also used Promis."

That's a big, "Whooops." An intelligence contact I know recently noted, "We opened all the cans of worms rather than just the right can of worms."

At least according to Dastych about that not-slight mishap, the information obtained far outweighed the damage done.The importance of the program's role was also pointed out in a WIRED expose in the '90s. It quoted an ex-Israeli spy, Ari Ben Menashe, as saying "PROMIS was a very big thing for us guys, a very, very big thing….The whole form of intelligence collection changed."

So you ask, what does all of this twisted espionage in the 1980s have to do with today's malware worm called Stuxnet? It is said of some nations and their causes that they do not plan for this generation or the next, but for hundreds of years, especially true if they are fighting for existentialism. Stuxnet is just such a case.

The malware worm may have started out as a logistical program, Promis. Then it morphed into an "Enhanced Promis" for intelligence work. It was subsequently altered for specific situations, given different names and sold to perhaps a dozen countries, worming its way around the world. In the process, rather than burrowing, the worm became like a centipede with hundreds of legs regenerating in different sizes and shapes, taking direction from its owners regarding objectives.

At issue, however, is who that current "owner" might be. Most fingers point to nations intent on halting Iran's nuclear weapons facilities, the US and Israel. But there is no dearth of suspects given the program's piracy over the years.

Both Russia and China have sold high-tech systems and weapons to Iran for years, and could have unwittingly been modern-day Typhoid Mary's carrying the worm to their recipients. In a game of highly sophisticated Clue, for example, Israel might have sold Promis to the KGB; the KGB or its successors later sold critical systems to Iran; and then Iran built operations with a Trojan horse in place. Likewise, Chinese scientists tapped by Iran could have brought that country Promis, the gift that keeps giving.

It’s a scintillating game of Clue with no sure culpability, no one to shoot, a war with no casualties. Nobel Peace Prize potential. Half of the world’s computer security experts are still scratching their heads opining on this new worm, not realizing that Stuxnet is not “new” at all.

Said one publication, it was “like the arrival of an F-35 into a World War I battlefield.” Another, “The timing is intriguing because a time stamp found in the Stuxnet program says it was created in January [2010], suggesting that any digital attack took place long before it was identified and began to attract global attention.” Long before is an understatement.

One man who spends his days worrying about such worms is Scott Borg, Director and Chief Economist of U.S. Cyber Consequences Unit, an independent, non-profit research institute that assesses cyber attacks and counter-measures. He says that the phrase “worms” is grossly outdated.

“We’re so far beyond worms,” says Borg. “We’re into big, complicated creatures.”

He likens Stuxnet to the Velociraptor dinosaurs from Jurassic Park, intelligent, cunning, capable of hunting in groups till they find their prey. “Modern malware — like Stuxnet — will use any channel available to spread and search out its prey. If the target system isn’t connected to the internet, the malware will migrate from device to device until it reaches the system it is looking for.”

Once planted, the Stuxnet bosses never have to talk to it again; it operates totally on its own. Somewhere, someone just watches and waits. And, in the case of Iran, Stuxnet’s target was very precise — automation control facilities. Not just any control systems, but nuclear. So Stuxnet wormed its way around the world until as Borg says, “When it finds the system it meant to destroy, it will destroy it.”

Some think Stuxnet was spread by international contractors moving between facilities. But they don’t know about Promis.

What’s odd to Borg, for example, is that Stuxnet included some features to help it avoid being detected, but not others. Stuxnet was designed to erase itself after each copy made four additional copies on different devices. In effect, Stuxnet was designed to have a limited number of children and to kill itself after its quota of kids. This would eliminate copies that had reproduced, but hadn’t reached their target so that Stuxnet’s trail would be minimized. But there was no limit on later descendants, so Stuxnet would eventually spread and almost certainly be detected. Why didn’t its creators make Stuxnet eventually die, so it could covertly be used again in a different situation?

Borg offers some theories: the “attacker” was fairly desperate to reach the intended target; could not release Stuxnet very close to its intended target, hence the extra children produced; had resources to burn; and, didn’t care if Stuxnet were detected and received a great deal of attention.

“Sometimes we know who carried out an attack,” adds Borg, “but it’s usually from other intelligence.”

One highly placed intelligence source I know, says we’ve hardly seen the last of Stuxnet, i.e. Promis. Sure, computer security experts found its vulnerabilities and have supposedly closed those exposures. But posed this source, “How do you know Stuxnet didn’t show those vulnerabilities on purpose, a ‘false flag’, so everyone would go ‘solve’ those problems while Stuxnet moved on?” That source winked, Gotcha. Maybe in fact, Stuxnet’s grandchildren are roaming the streets of the information superhighway as I write, ready to pounce on their next prey.

Dr. Peter Vincent Pry, a former CIA officer, now President of EMPACT America, a non-profit focused on electromagnetic pulse threats (EMPs) which have the potential to down power grids, thinks cyber threats are overblown at the risk of more probable, and more damaging, EMPs. Simply put, EMPs create a radio-frequency shockwave that zaps electronic fields of energy, burning out electrical systems such as computers, power grids, weaponry and communications. There’s been some tug-of-war going on in Washington as to which threat is worse, EMPs or “cybergeddon”.

Russia, for one, addressed significant cyber-risk by throwing out Promis with the bath water, choosing to re-construct their computer systems from scratch a decade or so ago, I’m told, rather than worry about generous gifts that keep giving.

But Stuxnet has also shown the civilized world the dangers of copycats. With the attention now drawn to the “good” that can be done by the likes of a Stuxnet, come the possibilities of future versions that might harm. The enormous physical power harnessed by some industrial facilities, for example, if unleashed in the wrong way by a worm could be astounding. Think of the dangers of opening a dam that should have been shut, or an oil pipeline backwashed into the sea. Nuclear reactors are just the half of it.

“There’s no reason to keep the secret from the American people, or our own allies, because the bad guys are on to it. This is a big worry for the future,” warns Borg. “We are entering a completely new defense era. If you have the tools like Stuxnet, why would you bother with missiles? Why bother invading with an army? The whole relationship between the military and society is going to have to be re-thought.”

Without a doubt, it is a new day of warfare. And cybergeddon aside, Stuxnet remains at the forefront, one of the most amazingly sophisticated pieces of malware ever publicly recognized; it always did have promise.

So do we have to worry about world powers attacking each other’s power grids with Stuxnet tools any time soon? Hardly, says Borg. “The last thing China or Russia wants is for our economy to take another dive. No one wants destabilization. But that doesn’t mean they haven’t planted malware programs for possible use at a future date.”

And that’s exactly what was done several decades ago with a promising new people-tracking program intended to stave off war, not start it. That brings us back to this weapon of peace, ever the more important as the Mid-East cracks at the seams. It also brings us back full circle to Beirut last October. Promis aka Stuxnet was at the core of the communications shutdown at command centers in Lebanon that day. This, confirmed by two extremely reliable, unrelated sources.

But Stuxnet only cleared the way in Beirut. The blasting of underground weapons caches that followed were achieved through electromagnetic pulses. The radar that went on the blink? Also electromagnetic pulses. So Stuxnet’s purpose was like clearing obstructive land mines before doing battle.

A Tehran journal a decade ago put it this way, “…today when you disable a country’s military high command through disruption of communications you will, in effect, disrupt all the affairs of that country.” Sounds like wording for a Stuxnet how-to-manual.

Regardless, Stuxnet and EMPs make it exceedingly clear that in any future major war, there may be no images of Patton charging across Europe in tanks, no massive armies forging rivers. The war will be fought below the radar, both literally and figuratively, with a new era of weapons.

As for Stuxnet, the “newest» weapon in that arsenal — or oldest depending how much you know – right now it could be on its way to a target near you. Jeffrey Carr, author of Inside Cyber Warfare acquiesces that possibility. “No one has a product that would have stopped the Stuxnet worm.”

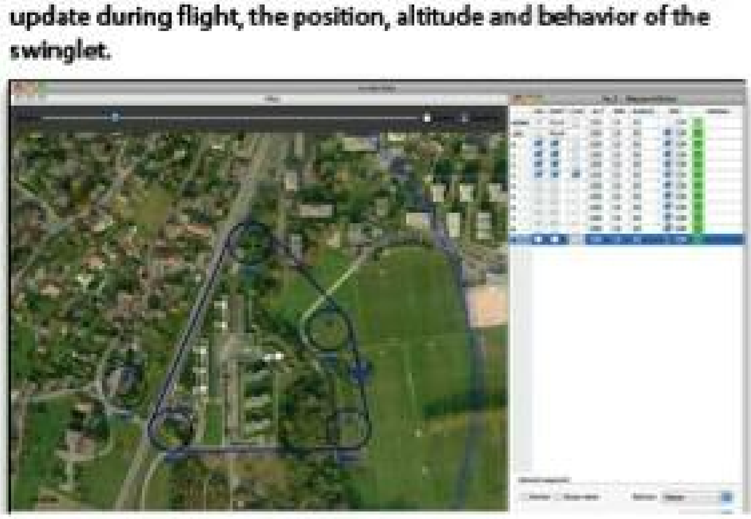
On that, Carr is undoubtedly correct. Because in one of the greatest whodunits in modern history, I know all the sleuths are looking in the wrong places. Rather than looking at where Stuxnet visited, they should be looking at where it came from, Promis. I just hope that the people that have Stuxnet are reasonable, either that, or they’re our friends.

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

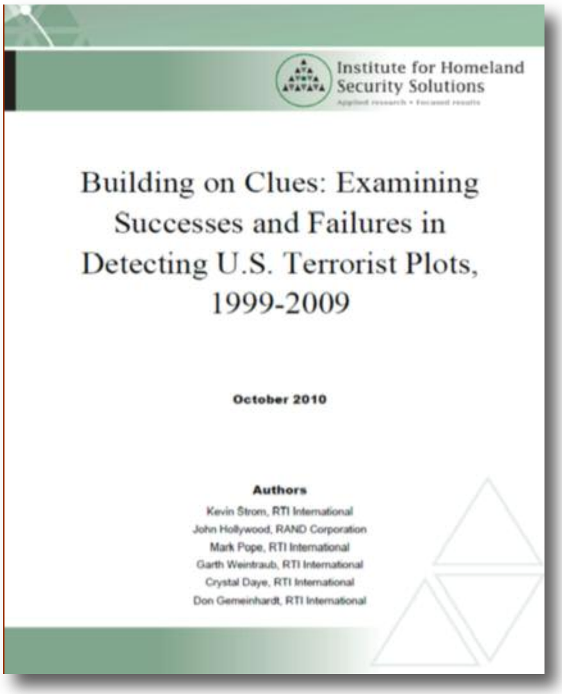
senseFly – chemin de la Raye 13 – 1024 Ecublens – Switzerland – www.sensefly.com

Terror News

Building on Clues

Institute for HMS Solutions - USA

Since 2001, the intelligence community has sought methods to improve the process for uncovering and thwarting domestic terrorist plots before they occur. Vital to these efforts are the more than 17,000 state and local U.S. law enforcement agencies whose role in the counterterrorism process has become increasingly recognized. As part of an on-going study for the Institute for Homeland Security Solutions (IHSS), this report examines open-source material on 86 foiled and executed terrorist plots against U.S. targets from 1999 to 2009 to determine the types of information and activities that led to (or could have led to) their discovery. Our findings provide law enforcement, homeland security officials, and policy makers with an improved understanding of the types of clues and methods that should be emphasized to more reliably prevent terrorist attacks, including the need to:



Institute for Homeland Security Solutions
Applied research • Focused results

Building on Clues: Examining Successes and Failures in Detecting U.S. Terrorist Plots, 1999-2009

October 2010

Authors
Kevin Strom, RTI International
John Hollywood, RAND Corporation
Mark Pope, RTI International
Garth Weintraub, RTI International
Crystal Daye, RTI International
Don Gemeinhardt, RTI International

1) Recognize the importance of law enforcement and public vigilance in thwarting terror attacks. More than 80% of foiled terrorist plots were discovered via observations from law enforcement or the general public. Tips included reports of plots as well as reports of suspicious activity, such as pre-operational surveillance, para-military training, smuggling activities, and the discovery of suspicious documents.

2) Continue to investigate Al Qaeda and Allied Movements (AQAM), but do not overlook other groups, and pay particular attention to plots by "lone wolves". Less than half of U.S. terror plots examined had links to AQAM, and many non-AQAM plots, primarily those with white supremacist or anti-government/militia ties, rivaled AQAM plots in important ways. Additionally, plots by single actors ("lone wolves") have proven particularly successful, reaching execution nearly twice as often as plots by groups.

3) Ensure processes and training are in place that enable law enforcement personnel to identify terrorist activity during routine criminal investigations. Almost one in five plots were foiled "accidentally" during investigations into seemingly unrelated crimes. Training is needed to recognize when ordinary crimes may be connected to terrorism.

4) Work to establish good relations with local communities and avoid tactics that might alienate them. Approximately 40% of plots were thwarted as a result of tips from the public and informants. Establishing trust with persons in or near radical movements is jeopardized by tactics such as racial, ethnic, religious, or ideological profiling. Support quality assurance processes to ensure initial clues are properly pursued and findings shared. Investigating leads and sharing infor

mation across agencies led to foiling the vast majority of terrorist plots in our sample. Similarly, breakdowns in these basic processes led to lost opportunities to thwart some of the worst attacks, including 9/11.

5) Expand the federal standards for categorizing suspicious activity reports (SARs). A large majority of the initial clue types we identified, including public and informant tips, as well as law enforcement observations made during routine criminal investigations, are only indirectly referenced in the current national SAR standards. Expanding them would enable more comprehensive reporting and greater information sharing of potential terrorist activity.

Safeguarding the Rails: Four Avenues for Increasing Security

Source: http://www.emergencymgmt.com/infrastructure/Safeguarding-Rails-Security.html

Railroads have been vulnerable since the first Transcontinental Railroad was built in 1869. Then and now, teenagers armed with rocks or guns see boxcars as tempting targets. Derailment, from both deliberate acts and accidents, is a constant threat — and sabotaging trains has a long history as part of warfare. "We've been doing rail security since Jesse James was robbing trains," said Thomas L. Farmer, assistant vice president of security for the Association of American Railroads, which represents major freight carriers and Amtrak. For a long time, the primary concern was people wanting to steal a freight train's contents, shoot the crew or rob the passengers. The United States' post-9/11 focus on security, however, is shining a new spotlight on other hazards surrounding railroads. "It's a vulnerable target," said Charles Peña, a senior fellow at the Independent Institute, who writes on national security and foreign policy. "There are good reasons [to] be concerned about it." But the desire to protect the railroads, their employees and passengers must be balanced, Peña said, "by what you can really do given that you're trying to move large numbers of people." Railroad security — whether for passenger rails, commuter lines or freight trains — is a complicated endeavor. The entities that own most railroads — from both the public and private sectors — have done much work, especially since 9/11, to increase security. But coordination challenges, the number of people involved and the rail network's vastness make it a difficult task. Although the 9/11 attacks made security experts increase planning for terrorist attacks on a train or station, terrorist attacks on rail transportation isn't new. "Unfortunately bringing explosives into train stations is a terrorist tactic that's been going on for generations," Farmer said. The attacks — in recent years in London, Madrid and Mumbai, India, for example — have generally happened outside the U.S. But that doesn't mean the U.S. is immune.

A Complicated Problem

After 9/11, the newly created U.S. Department of Homeland Security (DHS) focused much attention on airline travel, which was understandable, said Dan Goodrich, a research associate at the Mineta Transportation Institute at San Jose State University in California. “Anything that can be put into motion — a car, bus, plane, ship — can all be used as weapons,” Goodrich said. “Air is a real issue because of its flexibility; [planes] can go literally anywhere.” It’s also easier to control access to commercial planes, so increasing security seemed more feasible. With rail and other modes of transportation, the infrastructure is much broader and more difficult to secure. With miles of rail, “it becomes a complex issue of how to address security,” Goodrich said. “We only have a finite amount of resources.”In addition, rail security is further complicated by the number of public and private entities involved. The federal government, state governments, counties, cities and transportation authorities can all play a role in rail transport. These entities have their own elected officials, budgets and concerns. Many also have their own law enforcement and emergency response teams. A single freight train carrying hazardous material may travel on tracks owned by different companies and through numerous jurisdictions to reach its destination. “You can see how this can get complex,” Goodrich said.The result is that the security of rail passengers and trains is essentially a public-private partnership. “A substantial amount of effort has gone into building partnerships between federal, state and local governments and operators,” Farmer said. Experts point to a number of avenues for increasing rail security, although they all have drawbacks.

First, screen passengers and luggage. When the government needed to increase security for airports, it increased security screenings and restricted access to boarding areas. Passengers take off their shoes, and their bags are scanned. But more people travel on trains and subways than on planes. If you try to screen all of them, it ceases to be mass transit, Peña said. “It brings the system to a complete, grinding halt.” Even if passengers and bags could be screened and moved efficiently, hiring all the people necessary would be expensive. “That’s a huge amount of manpower if every station has to have people who are patting people down,” he said. Another issue is access at stations in less populated areas. “People just walk up onto platforms,” Peña said. “You don’t have control points.” One possibility is to institute random screenings, said Lawrence Mann, a Washington, D.C. attorney who has worked on rail safety issues for 40 years. “That would at least mitigate a person thinking he can get away with it.” Major rail carriers like Amtrak could also institute screening without too many problems, he said. There are no easy answers, however. “People are used to being able to show up and board within 10 minutes,” Goodrich said. “You have to balance these things [with] what the customer is willing to put up with.”

Second, reinforce trains. Windows of locomotives and passenger trains are required to be bulletproof, but only for .22-caliber rifles. “Major damage can be done with high-caliber arms,” Mann said. Efforts also are under way to improve tanker cars so they’re more resistant to attacks and accidents.

Third, air condition locomotives. When locomotives aren’t air conditioned, crews in hot areas have no choice but to ride with windows and even doors open, said James Stem Jr., national legislative director of the United Transportation Union, which represents tran sit, rail and other workers. “It’s impossible to secure the cab when it’s 100 degrees outside,” Stem said. “That is probably the most outrageous rail security issue today.”

Fourth, safeguard hazardous materials during transport. Much of the attention in rail security has focused on passenger trains and subway systems — with good reason. Attacks on heavily populated passenger systems allow terrorists to achieve “casualties, damage and the laserlike attention of the international media,” Farmer said. They make rail passengers worldwide worry if such an attack could happen to them. Attacks on freight trains also can potentially be deadly and attention-getting, especially if they hit trains transporting hazardous material through a heavily populated area. “Throughout the country, hazardous materials are transported more on trains than any other mode of transportation,” Mann said. “There’s no real protection against someone just taking a shotgun and shooting it. That’s a major problem.” But freight trains’ schedules and cargo are unpredictable, Farmer said, making such an attack “not nearly so easy.” Some attacks on freight trains turn out to be fairly similar to an accidental derailment — a problem, but not the sort of catastrophe that gets international headlines. Although freight trains may not be as attractive targets as passenger trains, “the freight railroads have been very attentive to the new realities after 9/11,” Farmer said. Within weeks of the attacks, safety and security officials assessed the risks and created a security plan. The transport of hazardous materials got particular attention, both from railroads and government. Focusing particularly on transported material that can be toxic when inhaled, the Transportation Security Administration (TSA) created a plan to ensure that those materials are kept secure, especially in heavily populated areas.

A Partnership

Because securing both freight and passenger rail systems is so complex, those in charge are turning to an old strategy: enlisting the public to report suspicious activity. “Terrorists are looking for what’s easy to do,” Peña said. If security efforts and the sharp eyes of the public make it more difficult, terrorists are less likely to try in the first place. In July, DHS Secretary Janet Napolitano announced an expansion of the department’s “See Something, Say Something” campaign, as well as a partnership with Amtrak to share information as part of the department’s Suspicious Activity Reporting program. “See Something, Say Something” teaches the public what types of activities law enforcement would like to know about. The DHS is creating educational materials and advertisements to nationally expand the program, which started with New York’s Metropolitan Transit Authority. The basic idea behind the program is sound and old — think of Neighborhood Watch programs, for example, Goodrich said. “They’re looking for a new way of getting through to people that this is an issue and they need to be aware of it,” he said. The idea is that terrorist plots require planning, surveillance and information-gathering in advance. If alert citizens call law enforcement when they see something suspicious, it will be much more difficult for plots to form. The government has numerous other programs as well. Although it’s not always easy to calculate how much money goes specifically to rail — since rail is one component of larger programs like port security — the federal government has given grants to transit systems nationwide to enhance their security, Farmer said. This includes canine teams, intrusion detection technology and expanded police forces. “Working together, the government, railroads, subways and local law enforcement are expanding their capabilities to do random, unpredictable security activities that are essential to deterrence,” Farmer said. However, some say even more could be done. “Rail security has taken a backseat to the security of other modes of transportation,” Mann said. Stem said he sees a stronger role for the federal government: “When you deal with transit and rail security, those issues are national in scope.” Stem also said although he understands that the TSA needed to focus first on the airline industry, it’s past time for the TSA to work with other parties to improve training for rail employees. In addition to training employees who deal with the public so they can better look for suspicious activities, Stem said the government also should work with railroads to establish better perimeter criteria — ensuring the cars are shielded and access is restricted when there's hazardous cargo.

A Balancing Act

Any security program requires trade-offs. How much are passengers and taxpayers willing to pay to secure the railways? How much are passengers willing to be inconvenienced and have their privacy invaded? "Security versus accessibility: Invariably it's going to be a compromise between the two," Goodrich said. It can even be difficult for the public to tell how much is being done. "You must have a certain degree of anonymity for a lot of security programs to function effectively," Goodrich said. "The more people know about them, the more difficult it is for them to do their jobs. But we live in an open society: Where are my tax dollars going? How do I know it's successful, appropriate and not violating my rights or anybody else's?" The unpleasant fact, Peña said, is that "at some point, you have to accept risk. But politicians don't get re-elected and government bureaucrats don't advance their careers by telling the public there's a certain amount of risk you have to take." And even the most robust security systems aren't perfect. "Hindsight is 20/20 when it comes to security," Goodrich said. "In reality, there are gaps in all security programs."

K Margaret Steen is a writer in Los Altos, Calif., who writes frequently about business and management.

Lessons Learned: Mass Casualties and Communication Gaps

Source:http://www.domesticpreparedness.com/Commentary/Viewpoint/Lessons_Learned:_Mass_Casualties_and_Communication_Gaps/

Emergency communications is key to incident management – and critical, both during and following, mass-casualty incidents (MCIs). On 7 July 2005, four suicide bombers detonated bombs between 8:50 a.m. and 9:47 a.m. on three underground commuter trains and a street bus in central London. Those bombings broke down the below-ground communications infrastructure, making it impossible to communicate with passengers trapped underground and extremely difficult to communicate with incident command agencies, and hospitals, in close proximity to the mass casualty incident. The first bomb was detonated at 8:50 a.m. on the eastbound Circle Line train travelling from Liverpool Street to Aldgate station. One minute later, the second bomb exploded on a westbound Circle Line train leaving Edgware Road station for Paddington station. At approximately 8:53 a.m., the third bomb detonated, on a southbound Piccadilly Line train traveling between the King's Cross and Russell Square stations. The fourth bomb exploded at 9:47 a.m. on the top deck of a double-decker bus at Tavistock Square. The four attacks caused 52 deaths and an estimated 700 injuries. London's primary emergency response organizations began responding to the incident by evacuating and rescuing victims at the four bombing sites. However, there were a number of passengers trapped inside the underground tunnels who could not be reached immediately because the explosions had so severely damaged the trains' communications systems. Many passengers were totally unaware, of course, of what actually had happened and did not know if emergency responders were aware of the situation and/or if they were on their way to help. Smoke coming from the bombed compartments created additional fears among the surviving passengers. The overall confusion and panic was exacerbated considerably by the fact that the train drivers could not immediately communicate with the passengers or issue evacuation instructions.

Follow-Up Actions & Recommendations

According to a well researched follow-up report (Emergency Communications: Improving Communications with Train Passengers Trapped Underground following a Mass Casualty Incident – a Lesson Learned available only on Lessons Learned Information Sharing [LLIS.gov]), the London Assembly investigated the bombings and later recommended that Transport for London (TfL) – the principal transport service agency managing London's entire transport network – update its train communications systems to help station staff and emergency responders provide critical information to train passengers much more quickly following a mass casualty incident. In any emergency incident, of course, communications should be initiated as soon as possible to alleviate confusion among victims and emergency responders. In mass-casualty incidents, hospitals in the vicinity also should be quickly alerted so that they will be ready to respond and receive incoming patients as soon as possible. Incident Management: Alerting Hospitals in Close Proximity to a Mass Casualty Incident – another Lesson Learned exclusive to LLIS.gov – further elaborates on the London Assembly's recommendations that all hospitals in close proximity to a mass casualty incident be notified about the incident much more quickly, even those hospitals that have not been specifically designated as «receiving hospitals.» Following the London bombings, the National Health Service (NHS), the United Kingdom's largest public healthcare provider, quickly alerted all designated receiving hospitals in London to increase their readiness, but did not formally notify specialist and non-acute care hospitals relatively close to the incident sites – apparently because those hospitals were not on the official list of receiving hospitals. Unfortunately, many specialty hospitals located in close proximity to each of the casualty sites – e.g., the Great Ormond Street Hospital (GOSH), a specialty children's hospital – did not know about the train bombings until paramedics arrived at the hospital asking for equipment and other assistance. Nonetheless, even though the GOSH staff had not been fully aware of what had happened, they were able to quickly set up a field hospital and to help emergency responders rescue and treat a number of injured victims. Staff members later commented that they would have benefited from NHS guidance on how to respond to the incident had they been notified at the same time as the staffs on the original list of receiving hospitals. The London Assembly's report recommends that London's emergency plans be amended to provide early notification to all hospitals in the vicinity of a major incident, even those hospitals not designated as possessing major accident and emergency departments. Mass casualty incidents, whether caused by terrorist attacks or natural disasters, usually happen very quickly, and communications infrastructure is critical in maintaining the discipline and order mandatory for incident-command and emergency-response situations. Taking to heart the lessons learned from the July 2005 bombings and applying them to local and state operations plans will and should help mitigate miscommunication problems in future incidents and eliminate other communication gaps that may already exist.

For additional information on these Lessons Learned and on mass casualty incidents, log into LLIS.gov at www.llis.dhs.gov.

Sophia Paros is an outreach analyst for Lessons Learned Information Sharing (LLIS.gov), the U.S. Department of Homeland Security/Federal Emergency Management Agency's national online network of lessons learned, best-practices, and innovative ideas for the nation's homeland-security and emergency-response communities. She received a dual bachelor's degree in Computer Information Systems and Business from the College of Notre Dame of Maryland and is currently working on an M.S. in Information Security from The George Washington University.

Swedish Rescue Training Centre

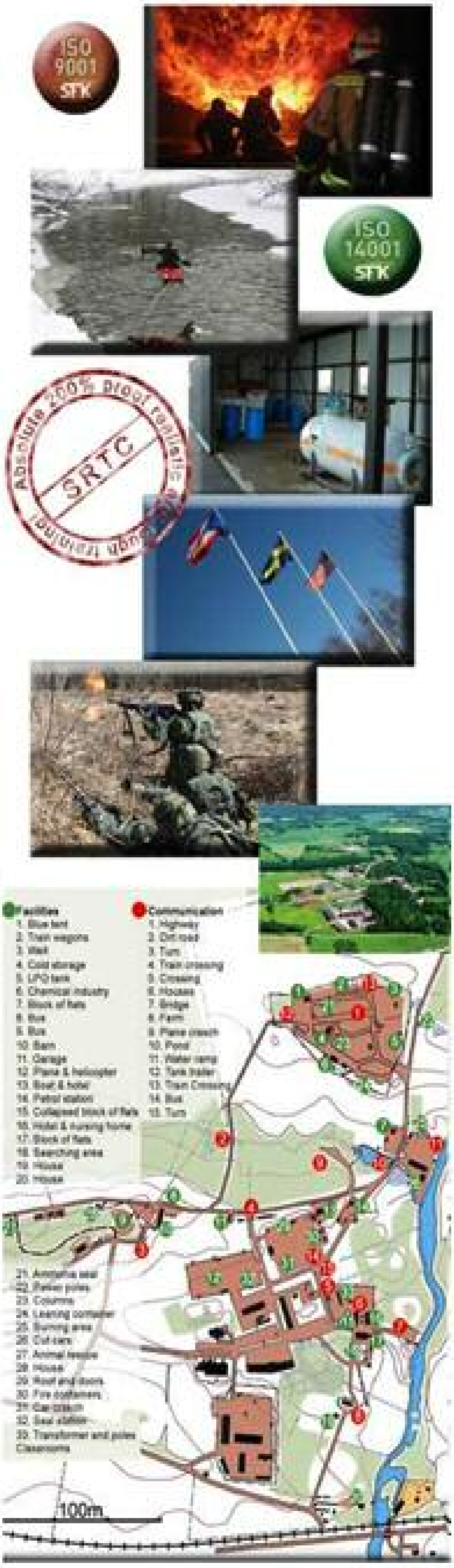
Swedish Rescue Training Center in Skövde AB (**SRTC**), the hub for risk and safety training, a company of **The Autokaross Group**. We formed in 2009 by former school **Swedish Rescue Service Agency Skövde** (**SRSA**) which later was named **Swedish Civil Contingencies Agency** (**MSB**).
Our intention is to provide Swedish and foreign rescue services, businesses, governments, organizations, etc. a wide range of training courses and exercises in risk and security.
We are approved as an official supplier to the authority, **Swedish Civil Contingencies Agency** (**MSB**), training and exercises at our training ground in Skövde. As a result, four training courses have been completed in autumn 2009, approximately 130 participants.

On the international market, we are now deeply cooperating with companies in Germany, Holland and USA, we also see collaborations in other parts of the world in the near future. However, our main objective is that You, as customer, receive the training You require and therefore we offer tailor-made concepts, based on Your actual needs and demands. In the Products link in the menu, we report a sample of our training opportunities. Whether you choose to educate You with us, in our miniature society, or at Your home, we tailor a complete training package. Together with You we want to identify your needs, in order to supply and fulfill Your requests.

Our instructors and service personnel have a broad competence. In addition to our own staff, we can also invite personnel from rescue services, authorities and organizations to participate in the operation of the school. This guarantees that we have a solid foundation of experience in education, development and pedagogy from basic to specialist level within all areas of training.

The **Swedish Rescue Training Centre** in Skövde is environmentally and quality certified according to ISO 14001 and ISO 9001.

http://www.srtc.se/english/index.html



Islamists raise fears of violent 'clash of cultures' in Europe

Source: http://www.msnbc.msn.com/id/40336911/ns/world_news-europe/

'It's a mathematical certainty there will be a successful attack ... at some point,' expert warns

Anjem Choudary, center, achieved notoriety in Britain after announcing an Islamist parade through the town of Wootton Bassett, where local people have taken to lining the streets to pay respects to dead soldiers as they return home through a nearby air force base.

It is a Sunday night in London's East End and the self-styled «most hated man in Britain» is holding court, reveling in his vision of a Taliban victory over America and a world under Islamic Shariah law. The crowd of about 250 listens intently as Anjem Choudary issues a call to arms in the pristine surroundings of the newly refurbished art deco conference center, built to host weddings and business meetings. «There are many battlefields,» he says calmly into a microphone. «There's a battlefield outside 10 Downing Street [home to Britain's prime minister] and in the mountains of the Tora Bora [in Afghanistan].» Any man who fails to fight, he warns, will face difficulty when the «angel of death» arrives and he is forced to explain to Allah why he did not raise his hand «against the oppressor» out of fear. «Allah will say to him, 'Am I not more worthy to be feared than them?'» Choudary says. «Allahu Akbar!» the men shout out in unison, as if a war cry, during his speech. «Allahu Akbar.» God is great. A group of women, all heavily veiled and sitting in a screened-off area, remain quiet throughout. As former leader of the banned Islamist organizations al-Muhajiroun and Islam4UK, Choudary was kept off the bill and appeared as the surprise star speaker at the rally. His groups may be outlawed but, unlike his female followers, Choudary will not be silenced. His message is one that echoes across Europe, which experts say is home to thousands of people who would wholeheartedly support Choudary's «ultimate objective» — the «domination of the world by Islam.» The majority of Muslims are not Islamists, who believe in a society based on Islamic law, and not all of the latter are seeking world domination or are willing to use violence. But fear of another Islamist-inspired atrocity after Madrid in 2004 — 191 dead — and London in 2005 — 53 dead — remains high.

Suicide bombers targeting London's public transit system killed 53 people on July 7, 2005. Four men detonated devices hidden in knapsacks aboard three subway trains and a double-decker bus, seen here. Rightly so, according to Dr. John J. Le Beau, a former CIA officer and now professor of strategy and security studies at Germany's George C. Marshall European Center for Security Studies. «It's a mathematical certainty there will be a success-

ful attack in Europe at some point,» he told msnbc.com. «The amount of attempted plots we see is not decreasing. I think what we have seen is a ... strengthening of attempted attacks that in some cases have come pretty close.» Le Beau, who cautioned that putting a figure on the number of Islamists was a «soft science,» estimated there were between 5,000 and 10,000 people in Europe «willing to engage in violence.» In 2007, the German Central Institute Islam Archive said there were 53.7 million Muslims living in Europe. A backlash is growing. Support for the far-right in normally liberal countries like Sweden and the Netherlands is on the rise. French lawmakers voted for a ban on full face veils. Protest groups, such as the English Defense League which has been linked to soccer hooligans, have made headlines. Le Beau warned of «an incipient clash of cultures.» The consequences of another terrorist spectacular — intelligence reports recently warned an al-Qaida-linked group was planning to hit Western Europe_with a commando-style raid like that on Mumbai, India — could be profound, he suggested. «I could see that leading to a spontaneous violent reaction on the part of others. Could this spin out of control? Sure,» he said. «I think that would be very dangerous because ... it runs the risk of sectarianizing or 'Balkanizing' Western Europe.» Europe is home to ancient conflicts. The Balkans, which includes the former Yugoslavia, has been the scene of intermittent religious strife stretching back to the fall of Constantinople, now Istanbul, to the Muslim Ottoman Empire in 1453. After the fall of Yugoslavian Communism, a resurgence of ethnic tensions led to the 1992-1995 Bosnian War, during which 8,000 Bosnian Muslim men and boys were massacred by Bosnian Serb forces in a single act of genocide. The U.K., far removed from such turmoil, has a long tradition of tolerating other countries' dissidents. In the 19th century, political philosopher Karl Marx took refuge in London after outraging authorities in his native Germany and France. But that tradition has been frayed by the increasingly vocal presence of Islamists in the U.K.

'Crazies' flock to 'Londonistan'

In the 1990s, the city became so popular for Islamists fleeing authorities in Muslim countries that some commentators dubbed it «Londonistan.» Citing the WikiLeaks cables, the Guardian newspaper last week reported that the future U.K. Prime Minister David Cameron told an American official in April 2009 that the former Labour government had «let in a lot of crazies and did not wake up early enough» to the danger posed by Muslim extremists. Le Beau said while Choudary and others like him were unlikely to fight themselves, they were helping to recruit people to the cause who would. «These groups are not the terrorist cells that are going to launch an attack,» he said. «These are the groups that radicalize individuals and put them in the frame of mind where they might engage in an attack.» Richard Reid, the so-called «shoe bomber» who attempted to blow up a flight from Paris to Miami in December 2001, was radicalized after meeting extremists at mosques in London, his father Robin tearfully told BBC News. Umar Farouk Abdulmutallab, a Nigerian dubbed the «underwear bomber» after being accused of trying to blow up a Detroit-bound flight on Christmas Day last year, studied at University College London. Yemeni officials told the BBC he became an Islamist in the U.K., although the British government has denied this. And London's Finsbury Park Mosque, now renamed after a takeover by moderates, was once the power-base of radical cleric Abu Hamza, a former nightclub bouncer who organized a conference praising the 9/11 attackers. He was later sentenced to seven years in prison for inciting murder and racial hatred.

A reformed Islamist

Ghaffar Hussain once counted himself among London's Islamists. His reaction to the Sept. 11 attacks was «well, so what?» «I felt it was kind of redressing some of the imbalance,» Hussain said. «'They've done this to the Palestinians by supporting the Israelis, this is the price you pay.'» However, he now battles the Islamist ideology as head of outreach at a British counter-extremism think tank, the Quilliam Foundation. «London is like the heart of the Arab world,» Hussain said. «The political dissidents are all based here.» In the 10 years before 9/11, foreign Arab dissidents «set up shop and carried on doing what they were doing in their own countries: Preaching violent jihad,» he explained. They found a ready-made constituency of young, disaffected, second-generation Muslims who had «experienced racism when they were younger.» «Merge those two together and you have a recipe for disaster,» Hussain said. «I was caught up in that ... and became active in my own area, doing speeches, giving out leaflets for about three years. «I abhor any kind of extremism, anything that takes innocent life. I look back with surprise at the things I used to believe.» His «wild guess» on the number of Islamists in Europe was «less than 5,000 hardcore activists» with a further 20,000 to 30,000 people who are «broadly sympathetic at times.» Al-Qaida's propaganda gives an indication of where they believe support is strongest, Hussain said, as they tend to publish only in English and German, not French, Spanish or Dutch. Fears of a terrorist attack may have recently gripped Germany , but Hussain said authorities there had not done enough to minimize the risk. Many of the 3 million Muslims there came as «guest-workers» and he said there had been little attempt to integrate them into society. «Germany is a bit of a basket case. Those communities are very hard to penetrate. Guessing, I'd say it's probably not as bad as the U.K., but nobody really knows,» he said.

Angry young men

As for Choudary, «he's got about 50 followers, all young men — I know some of them personally — very, very ill-informed,» Hussain said. «All they know is they are angry about something.» Choudary has achieved infamy in Britain, particularly after announcing an Islamist parade through the town of Wootton Bassett, where local people have taken to lining the streets to pay respects to dead soldiers as they return home through a nearby air force base. The event, which would have seen the Islamists carrying empty coffins to symbolize Muslims «mercilessly murdered» in Afghanistan, did not take place but still sparked public anger. Given his rhetoric, some in Britain question Choudary's right to freedom of speech. And the European Union is taking steps to limit the flow of Islamist propaganda, putting itself at odds with the U.S. and its adherence to the First Amendment. Gilles de Kerchove, the EU's counterterrorism coordinator, said legislation would soon be implemented which would allow «even 'free speech' member states to shut down websites, to bring people to court when they cross the line.» «That's where we have a problem with the U.S.,» he told msnbc.com. «Most of the neo-Nazi and most radical Islamist websites are hosted by U.S. servers.» The EU has invested millions of dollars on research to develop programs capable of monitoring the internet for the «automatic detection of threats and abnormal behavior or violence,» the Sunday Telegraph reported. According to de Kerchove, collecting more information about flights, passengers and cargo and using computer programs to analyze this data could prevent terrorist attacks. The attempt to send bombs hidden in printers from Yemen to Chicago in October was detected by Saudi Arabian intelligence. However, a surveillance program might have red-flagged the shipment as a U.S. synagogue was likely to purchase office equipment closer to home. «It's stupid to send a printing machine from Yemen to a synagogue in Chicago,» de Kerchove said. «That does not make sense.» He insisted the danger to Europe remained real, despite the lack of a major attack since London in 2005. «That's not because there's no threat. It's because the security services have been very effective,» de Kerchove said, highlighting recent arrests in connection with an alleged plot to kill the moderate head of a Paris mosque. Like Le Beau, he thought it likely that a significant attack would eventually slip through. «Since the threat is becoming more ... diverse and complex, it's not that risky to speak like this and say, 'It's not if, but when,'» he added.

Choudary, who rose to prominence in 1999 when media reports described him as a key figure in the recruitment of fighters for Islamist forces around the world, insists that his beliefs did not mean «I'm going to kill you.»

'There will always be wars'

The mild-mannered Choudary told msnbc.com that some «battlefields» were merely «ideological» ones. The former lawyer said he «cannot have a friendship» with a non-Muslim but different religions could live side by-side «peacefully.» «As long as my life and wealth is protected in Britain, I do not target the life and wealth (of people here),» Choudary said, citing a passage from the Quran to that effect. However, he cautioned this stance was a matter for legitimate religious debate. «There are many Muslims who do not believe that,» he said. «(London suicide bomber) Mohammed Siddique Khan didn't believe that.» And he appeared almost to relish the prospect of ethnic violence. «There will always be wars. The conflict will continue always. I think it's a matter of time before another 9/11 takes place and another 7/7 (London bombings),» Choudary said. «I think we are on the brink of many more operations in the West. This is going to be very, very nasty ... The Muslims engaged in jihad are not going to stop. People will declare jihad in Britain and America. I don't think you can stomach something like that.»

Egypt: Sinai shark attacks orchestrated by Israel

Source: http://homelandsecuritynewswire.com/egypt-sinai-shark-attacks-orchestrated-israel

The sandy resort of Sharm el-Sheikh, at the tip of the Sinai Peninsula, is popular with European tourists and attracts more than three million visitors a year; two shark attacks in as many weeks — a fatal shark attack on a German tourist Sunday, which followed a similar attack which mauled four Russian tourists earlier last week — now threaten the region's tourism industry; Egyptian officials now say the attacks may have been orchestrated by Israel to damage Egypt's economy; Israel says the accusations are too ludicrous for comment

Egypt runs the risk of giving conspiracy theories a bad name: Egyptian officials say they have not ruled out the possibility that a fatal shark attack in Sinai on Sunday could have been a plot by the Mossad. "What is being said about the Mossad throwing the deadly shark [in the sea] to hit tourism in Egypt is not out of the question, but it needs time to confirm," South Sinai governor Muhammad Abdel Fadil Shousha was quoted as saying by the Egyptian state news site egynews.net. Israeli officials said the claims were too ludicrous to comment on. Israel has issued an advisory warning against travel to Sinai due to plots against Israelis by terrorist groups linked to al Qaeda. The Jerusalem Post reports that the fatal shark attack in the Red Sea off the coast of the resort town of Sharm e-Sheikh killed a German tourist, just days after four Russians were mauled by sharks and Egypt declared that the waters were safe. Experts said that despite announcements that Egypt had caught the shark, the one actually responsible for the mauling was still on the loose. Sunday's attack happened at Nama Bay when a shark bit off the arm of a snorkeling German tourist. The woman reportedly died immediately, reports said. The general manager of the Sharm e-Sheikh Marriott Hotel in Nama Bay, Nagy Arafat, told the Media Line that they closed the beaches until further notice. "This is something I've never seen before. I have never had any sightings of sharks in the area and if we ever did, it was in the deep waters and not up on the beach," Arafat said. He stressed that the mood was "calm and cool." "We don't see it af-

fecting the tourism industry in any big way," Arafat said. Aviv Levy, a shark expert and the curator of the Underwater Observatory Marine Park in Eilat, said the Egyptians usually engaged in "smoke screening" when it came to shark attacks. "Something is very strange here. The Egyptians are trying to hide it," Levy told the Media Line. "This is very bad news for the sharks. It was strange after the first attacks last week and now even more so." Egyptian authorities launched a hunt for sharks after four Russian swimmers were mauled at the Red Sea resort last week. Over the weekend, government conservation officials released photos of two captured sharks: an oceanic whitetip and a mako. The mayor of Sharm e-Sheikh had announced that the beaches were reopened after authorities deemed that the sharks no longer posed a threat and that it was safe to go back into the waters. The sandy resort at the tip of the Sinai Peninsula is popular with European tourists and attracts over three million visitors a year. Shousha speculated that the sharks in the deep sea could have become frenzied after a ship transporting livestock dumped dead sheep into the waters. Levy said they were more likely becoming bolder after over-fishing forced them closer to shores. "They are taking away their fishing places and there are less fish so they are spreading their range of searching for food. This is when the sharks and humans meet," Levy said. "But sharks usually recognize a person and turn around." According to Levy, attacks in the Gulf of Aqaba happen only once every couple of years and are very rarely fatal. "When I heard they were going out to catch the sharks, I thought to myself that it'll now be open season on sharks. It's going to be difficult for them now. As it is, the shark population has been dwindling and we don't see the big ones we used to anymore," he said.

N
Sainai
Dahab
Ras Nasrani
Tiran Island
Shark Bay
El Tur
Sharm El Skeikh
Turtle Bay
Ras Umm Sid
Ras Ghozlani
Strait of Gubal
Ras Mohammed
Small Gubal Is.
Big Gubal Is.
Shadwan Is.
Red Sea
Main Road
Reef

New York City's leaders urge Congress to close «Terror Gun Gap»

Source: http://homelandsecuritynewswire.com/new-york-citys-leaders-urge-congress-close-terror-gun-gap

In the United States, the fact that you are on the terrorist watch list does not disqualify you from purchasing an AK-56 assault rifle (if your immigration status is unclear, you are disqualified); FBI data showed that between 2004 and February 2010, a total of 1,228 background checks were conducted for purchases of firearms and explosives attempted by people on the U.S. terrorist watch list; of those purchases, 91 percent were allowed to proceed, while a total of 109 were denied.

Mayor Michael Bloomberg and other high officials from the New York City metro-area called on Congress Wednesday to close the "terror gun gap" that they argue makes a Mumbai-style attack against an American city easier for terrorists. The hearing before the Senate Committee on Homeland Security and Government Reform, held just days after the arrest of suspected Times Square bomber Faisal Shahzad, examined whether people on the terrorism watch list should be legally prevented from purchasing firearms and explosives (note that Shahzad was not on the terrorist watch list). "The threat is all too real. Terrorists with semi-automatic and high-powered weapons can inflict heavy casualties (.pdf) in seconds," said committee chairman Senator Joseph Lieberman (I-Connecticut), citing the November 2009 massacre at Fort Hood, Texas, and the June 2009 murder of an Army recruiter in Arkansas as examples. "The more we can do to deny would-be terrorists access to these weapons, the safer we will be," said New York police commissioner Raymond W. Kelly, reminding lawmakers that "a small team of operatives using AK-56 assault rifles" had paralyzed Mumbai, India, for nearly 60 hours and killed approximately 170 people. Matthew Harwood writes that the Government Accountability Office (GAO) found that between 2004 and February 2010, FBI data showed that 650 individuals on the terrorist watch list had background checks conducted on them while attempting to purchase firearms and explosives. Overwhelmingly, the transactions were allowed to proceed, testified Eileen R. Larence (.pdf), the GAO's director for homeland security and justice, because "no prohibiting information was found — such as felony convictions, illegal immigrant status, or other disqualifying factors." The GAO reported that over the six-year period a total of 1,228 background checks were conducted for purchases attempted by people on the watch list. Of those purchases, 91 percent were allowed to proceed, while a total of 109 were denied. The government did not start tracking the reasons for denials until April 2009. They have since included "felony conviction, illegal alien status, under indictment, fugitive from justice, and mental defective," said Larence. The bipartisan witnesses from the New York City metropolitan area argued Congress must close this loophole quickly. "When gun dealers run background checks, should FBI agents have the authority to block sales of guns and explosives to those on the terror watch lists — and deemed too dangerous to fly?" Republican Mayor Bloomberg asked (.pdf). "I believe strongly that they should." Last year, Senator Frank Lautenberg (D-New Jersey) introduced a bill to do just that. The bill (S. 1317) would give the U.S. attorney general the ability to deny a gun transfer or a gun or explosives license to a person reasonably suspected of terrorism ties. People denied the right to purchase a firearm could then challenge the attorney general's decision. Testifying before the committee, Lautenberg said his bill is "not anti-gun—it's anti-terrorist" (pdf.). Representative Peter King (R-New York), who recently introduced similar legislation in the House, described the law as "an issue of common sense" (pdf.) Harwood notes that not everyone agreed. Senator Lindsay Graham (R-South Carolina) cautioned the law could deny a U.S. citizen on the terrorist watch list their Second Amendment rights. He also asked the witnesses whether anyone on the terrorist watch list that purchased guns had ever been prosecuted for a terrorist offense. No one knew. Bloomberg, however, told Graham that it is reasonable that if someone on the No-Fly List cannot fly, then that person should not be able to own a gun. Graham was unmoved, later stating that there is no constitutional right to fly but there is a constitutional right to bear arms. Attorney Aaron Titus, privacy director for the Liberty Coalition, called Senator Lautenberg's legislation an unconstitutional violation of due process and lampooned it. "In short, S. 1317 should be re-named the 'Gun Owners Are Probably Terrorists Act,'" Titus said, "because it gives the attorney general the discretion to deny someone the enumerated constitutional right to bear arms (pdf.), based on 'suspicion' and 'belief' of terrorist inclinations." Lautenberg's legislation is currently before the Senate Judiciary Committee.

Chinese variants of the AK-56 // Source: uzitalk.com

Journal of Bioterrorism & Biodefense

http://omicsonline.org/jbtbdhome.php

OMICS Publishing Group

An Open Access Publisher for the Advancement of Science & Technology

Open Access

ISSN: 2157-2526

FAA's Missing Plane Info Leads to Terror Concerns

Source: http://newyork.cbslocal.com/2010/12/10/faas-missing-plane-info-leads-to-terror-concerns/
From: wcbsmark

The Federal Aviation Administration is missing key information on who owns one-third of the 357,000 private and commercial aircraft in the U.S. – a gap the agency fears could be exploited by terrorists and drug traffickers. The records are in such disarray that the FAA says it is worried that criminals could buy planes without the government's knowledge, or use the registration numbers of other aircraft to evade new computer systems designed to track suspicious flights. It has ordered all aircraft owners to re-register their planes in an effort to clean up its files. About 119,000 of the aircraft on the U.S. registry have "questionable registration" because of missing forms, invalid addresses, unreported sales or other paperwork problems, according to the FAA. In many cases, the FAA cannot say who owns a plane or even whether it is still flying or has been junked. Already there have been cases of drug traffickers using phony U.S. registration numbers, as well as instances of mistaken identity in which police raided the wrong plane because of faulty record-keeping. Next year, the FAA will begin canceling the registration certificates of all 357,000 aircraft and require owners to register anew, a move that is causing grumbling among airlines, banks and leasing companies. Notices went out to the first batch of aircraft owners last month. "We have identified some potential risk areas, but I think we're trying to eliminate as much risk as possible through the re-registration process," said FAA spokeswoman Laura Brown. The FAA says security isn't the only reason it needs an up-to-date registry. Regulators use it to contact owners about safety problems, states rely on it to charge sales tax and some airports employ it to bill for landing fees. Also, rescuers use the database to track down planes that are missing. But the FAA has emphasized the security and law enforcement angle as the new measure has moved through the rule-making process over the past two years. The agency says the paperwork gap is becoming a bigger problem as authorities increasingly rely on computers to tighten aviation security in the wake of 9/11 and other terrorist plots. There have already been cases of criminals using U.S. registration numbers, also known as N-numbers or tail numbers, to disguise their airplanes. In 2008, Venezuela authorities seized a twin-engine plane with the registration number N395CA on the fuselage and more than 1,500 pounds of cocaine on board. Soon afterward, airplane owner Steven Lathrop of Ellensburg, Wash., received a call from a reporter. "He sort of started the conversation with, `Do you know where your airplane is? … Your airplane's in a jungle in South America,"' Lathrop said. Lathrop's Piper Cheyenne II XL was locked safely in its hangar at the Ellensburg airport. The smugglers had apparently chosen his tail number because the model was similar to their plane. "Anybody with a roll of duct tape can put any number they want on an airplane," Lathrop said. Federal law requires all U.S. aircraft owners to register their planes with the FAA and carry the registration certificate on board. The registration number — all U.S. registrations start with the letter N – is painted on the fuselage or tail. The numbers are used on flight plan forms and by air traffic controllers to communicate with aircraft in flight. The amount of missing or invalid paperwork has been building for decades, the FAA says. Up to now, owners had to register their planes only once, at the time of purchase. The FAA sent out notices every three years asking owners to update their contact information if needed, but there was no punishment for not doing so. As of 2008, there were 343,000 airplanes on the registry. By 2010, the number had risen to 357,000. The U.S. registry includes 16,000 aircraft that were sold but never updated with the names of the new owners, and more than 14,000 aircraft that have had their registrations revoked but may still be flying because the FAA has not canceled their N-numbers. Other registrations are outdated because the owners have died or the planes were totaled in crashes. Some planes are simply derelicts corroding in barns or junkyards. As a result, there is a "large pool" of N-numbers "that can facilitate drug, terrorist or other illegal activities," the FAA warned in a 2007 report. The problem became more acute after the government launched a new computer system for tracking flights called the Automatic Detection and Processing Terminal, or ADAPT, the FAA says. The system combines dozens of databases, from a list of stolen aircraft to the names of diplomats. It flags suspicious flights in red on a map. Unreliable data in the system has led to cases of mistaken identity. Pilot Pierre Redmond said his Cirrus was searched by Customs and Border Protection agents in fatigues and bulletproof vests last year in Ramona, Calif. They told him his tail number had been confused with that of a wanted plane in Florida. In August, police in Santa Barbara, Calif., detained flight instructors John and Martha King at gunpoint after federal authorities mistook their Cessna for a plane that was stolen in 2002. The Kings are famous in aviation because they produce and star in a popular series of test-preparation videos for pilots. The error in the Kings' case was eventually traced to a law-enforcement database that is cross-referenced with the FAA's registry, not to the registry itself. But Brown of the FAA called it an example of the real-world consequences of bad recordkeeping. "It's very, very scary," Martha King said. "If this keeps happening to people, somebody's going to get shot." To update the FAA registry, the agency will cancel all aircraft registrations over the next three years. Owners will have three months to re-register. In addition, the FAA will do away with its one-time registration certificate and adopt one that has to be replaced every three years. Those who fail to re-register will lose their certificate, and the plane must be grounded. "We're trying to model it more closely on some of the programs that are in effect for automobiles," Brown said. "With the more regular renewal process, you will capture bad data much more frequently." Airlines, leasing companies, charter operators and banks agree there is a problem but have complained about having to repeatedly re-register planes. The Air Transport Association of America, which represents airlines, warned in 2008 that the measure "had the potential to wreak havoc on the commercial air transportation system." On Tuesday, ATA spokesman David Castelveter said airlines are still gauging the potential effect of the new rule. Other groups noted that most of the aircraft with paperwork problems are smaller planes that pose little terrorist threat. "I don't think we're going to see a tremendous security benefit as a result of this," said Doug Carr, a vice president of the National Business Aviation Association. Banks and finance companies that hold loans used to buy planes will be among those hardest hit, said David Warner, general counsel for the National Aircraft Finance Association. A bank's claim to an aircraft is often tied to the FAA registration, so lenders are having to hire more staff and buy computer systems to track hundreds of aircraft registrations, Warner said. He said the FAA has exaggerated the danger. "The threat of people wanting to do us harm is very real, but the focus on re-registration or stale registration data on aircraft is not where the risk is likely to be," Warner said.

Al Qaeda's M&A Strategy

Is franchising a successful way to build a global terror network?

Source: http://www.foreignpolicy.com/articles/2010/12/07/al_qaedas_m_and_a_strategy

On Sept. 11, 2006, al Qaeda celebrated the fifth anniversary of its marquee terrorist attack by announcing that it had signed up hundreds of new members — an impressive growth spurt for an organization whose membership is often estimated by American counterterrorism analysts to be in the low thousands.

But al Qaeda hadn't so much recruited its new members as acquired them: They were from the Salafist Group for Preaching and Combat (GSPC by its French initials), a jihadist group that for years had almost exclusively targeted the ruling regime in Algeria. "The Salafist Group for Preaching and Combat has joined the Al Qaeda organization," Ayman al-Zawahiri, al Qaeda's No. 2, crowed. "May this be a bone in the throat of American and French crusaders, and their allies, and sow fear in the hearts of French traitors and sons of apostates." A few months later, the GSPC adopted the moniker "al Qaeda in the Islamic Maghreb" (AQIM). A minor-league guerrilla operation had rebranded itself as a franchise of the biggest name in Islamist terrorism.

AQIM is not alone in going from a local to a global focus. The popular image of al Qaeda is of an organization that draws its membership from disillusioned Muslims who, infuriated by U.S. support for Israel or intervention in the Muslim world — and beguiled by the idea of a universal caliphate — go off to join the fight. But in fact, much of al Qaeda's growth in the last decade has been the kind of expansion that any American businessman would recognize: They've systematically tried to absorb regional jihadist start-ups, both venerable and newly created, and convince them that their struggle is a component of al Qaeda's sweeping international agenda — and vice versa. Zawahiri himself was once head of one such organization, Egyptian Islamic Jihad (EIJ), which he led from an exclusive focus on toppling the Egyptian regime to an embrace of al Qaeda's anti-American and pan-Islamic agenda. Al Qaeda branches have since popped up in Iraq and the Arabian Peninsula, and the organization is making inroads with groups in Pakistan, Somalia, and elsewhere.

Consider last year's Christmas Day bombing plot, in which a Nigerian recruit to the Yemen-based al Qaeda in the Arabian Peninsula (AQAP) almost blew up a passenger airplane landing in Detroit. Yemen has long hosted al Qaeda-linked jihadists, but for most of the last decade they focused on local and regional targets. In 2009, however, jihadists in Yemen and Saudi Arabia announced a merger under the AQAP banner and took on a more global focus: one that included the Detroit plot and this October's plan to blow up two cargo planes as they neared U.S. cities.

The attacks emerging from Yemen have led some U.S. officials to believe al Qaeda's affiliates are more dangerous than the organization's core, isolated as it is in the Pakistani hinterlands. Making sense of this network is key to understanding the threat of terrorism today — and how best to respond to it.

How Do I Sign Up?

Formally joining al Qaeda is a complex process and one that can take years. It is often difficult to tell when a true shift has occurred, in part because al Qaeda does not demand sole allegiance; it supports local struggles even as it pursues its own war against the United States and its allies. So group members can be half-pregnant: both part of al Qaeda's ranks and loyal fighters in their local organization. Zawahiri, for instance, had been part of al Qaeda since its founding in 1988, but for almost a decade he saw EIJ, not al Qaeda, as his primary charge. It took 10 years for Zawahiri to fully sign on to Osama bin Laden's "International Islamic Front for Jihad on the Jews and Crusaders," and three more years for his group to fully integrate with al Qaeda. For Algeria's GSPC, the process took at least four years, and the integration is still incomplete.

During this prolonged courtship, groups often straddle their old and new identities, trying to keep up the fight against the local regime while also attacking more global targets. Often this is a time of infighting, with key leaders pulling the group in different directions. Some seek to stay the course and continue to fight the local regime, while others are attracted by what al Qaeda has to offer. Somalia's al-Shabab, for instance, appears to be in such a phase today. Some parts of the organization cooperate with al Qaeda, with foreign jihadists playing leading roles in tactics and operations. But others within the movement — probably the majority, in fact — oppose the foreigners' control, with some even publicly condemning terrorism and even working with international humanitarian relief efforts. Al-Shabab could become "al Qaeda of the Horn of Africa," but this is not yet a done deal. And if it happens, it could split the group.

After a merger happens, command relationships between the affiliate and al Qaeda's central leadership vary. When al Qaeda of the Arabian Peninsula began attacks on Saudi Arabia in 2003, they were done at the direction of al Qaeda's central leadership, which was eager to strike at the kingdom. But groups like AQIM retain a high degree of independence, working with al Qaeda's core more as partners than as proxies. Many AQIM attacks still target the Algerian regime, particularly its security forces — an aim more in keeping with the group's past priorities than al Qaeda's.

But even these somewhat independent partners change both their targets and methods as they move closer to joining al Qaeda. On the road to becoming AQIM, for instance, the GSPC expanded its primary focus to include France as well as the Algerian regime. When it took on the al Qaeda label, the group struck U.N. and Israeli targets and went after Algeria's energy infrastructure, none of which were a priority in the past. Suicide bombings, hitherto one of the few horrors the GSPC did not inflict, grew more frequent, along with Iraqi-style car bombs. In Pakistan, where al Qaeda's influence has spread since 9/11, there were two suicide attacks in 2002; by 2009, there were almost 60.

The Rewards of Association

For al Qaeda's leaders, the appeal of gathering affiliates is manifold. New franchises are both confirmation of the wisdom of their mission — to throw out the Westerners and establish a true Islamic government throughout the Muslim world — and a means of extending its influence. Al Qaeda seeks not only to change the Islamic world, but also to shift the orientation of jihad from the local to the global. Historically, most jihadi resistance movements have focused on their own territory. Even Zawahiri, during his EIJ days, once wrote that "the road to Jerusalem goes through Cairo" — meaning that destroying Israel, ostensibly the ultimate sacred cause for jihadists, must wait until there is an Islamic government at home. If jihadists did have a foreign focus, it was usually on throwing out foreign troops: for example, fighting the Russians in Afghanistan and, later, Chechnya. But bin Laden has successfully convinced groups that striking the United States and its allies is more important to this victory than fighting more proximate enemies.

Affiliates offer al Qaeda many practical rewards: hundreds or even thousands of fighters, donors, smuggling networks, and sympathetic preachers who offer religious legitimacy. Before the creation of al Qaeda in Iraq (AQI) in 2004, bin Laden and his coterie seemed irrelevant to the struggle against the United States there; it was Abu-Musab al-Zarqawi and his supporters in the Monotheism and Jihad Group who garnered recruits, money, and publicity. Al Qaeda affiliates also offer access to immigrant and diaspora communities — a group like Somalia's al-Shabab, with its connections to the Somali-American population, would be a prize asset. (Mohamed Osman Mohamud, the alleged Portland, Ore. bomb plotter arrested in November, doesn't appear to have any connection to al-Shabab, but demonstrates the potential that such groups see in immigrant communities.)

What do al Qaeda franchises get out of the deal? Most concretely, money — either directly from al Qaeda or from elsewhere in its network. After all, jihad isn't cheap. Buying explosives, paying salaries, providing stipends for the families of imprisoned fighters, arranging travel, and handing out bribes to local governments — it all adds up. (In 1999, EIJ was so broke that Zawahiri blasted a cell member for buying a new fax machine without authorization when the organization's staff was on half salary.) Al Qaeda also has web and media specialists who produce recruitment and fundraising videos, recruiters who try to identify potential new members at mosques and other locations, trainers who teach how to use small arms and make improvised explosive devices, and other experts in its global Rolodex, all available to help a new local franchise. For example, Saleh Ali Nabhan, an experienced al Qaeda commander linked to several attacks in Africa, reportedly trained al-Shabab members in Somalia.

An al Qaeda label is also a potential recruiting boon — it may help a group attract new members who hate the West and the United States but were not motivated by the group's past, more local, rhetoric. Less tangibly, the al Qaeda brand also can give credibility to groups struggling at home. Groups like al-Shabab often have an inchoate ideology; al Qaeda offers them a coherent — and, to a certain audience, appealing — alternative.

A Risky Play

But the post-merger relationship is not all IEDs and roses. Gaining affiliates may raise al Qaeda's profile and extend its reach, but it also poses risks for the group's core. The biggest is the lack of control. Maintaining effective command from remote parts of Pakistan was always difficult; the U.S. drone campaign has made it even harder. Nowhere was this more apparent than in Iraq. As early as 2005, al Qaeda core leaders tried to push Iraqi fighters waging guerrilla war under the banner of al Qaeda in Iraq not to slaughter Shiite Muslims, and especially not Sunni civilians, but to no avail. As the bloodshed rose, al Qaeda funders and supporters pointed their fingers not only at AQI leaders, but also at al Qaeda's core. This left the top al Qaeda officials in a bind: Should they denounce their most popular affiliate for its excesses, or risk being tarred with its bloody brush? In 2008, years after the merger, Zawahiri was still defending the al Qaeda cause against accusations of brutality and excess. Sayyid Imam al-Sharif (known better as Dr. Fadl), a one-time key EIJ ideologue who has since turned against al Qaeda, excoriated the group this year for the "unprecedented atrocities committed … against the Iraqi people."

But joining up with al Qaeda is even more risky for the affiliates. By taking on new enemies at al Qaeda's behest, a group gets — well, new enemies. When AQIM declared its intention to take jihad beyond Algeria, the Moroccan government — long hostile to Algiers — became much more willing to cooperate with its neighbor, and French counterterrorism support for states in the region also picked up. The United States, of course, is the biggest new enemy. Even short of drone strikes, Washington can offer its allies intelligence, financial support, paramilitary capabilities, and other vital forms of assistance, creating new headaches for groups that have plenty of them already.

When groups embrace al Qaeda's "far enemy" logic, they are also embracing strategic absurdity. Terrorist groups that succeed politically, like Hezbollah and Hamas, are firmly anchored in local realities and politics, and their success comes in part because their ambitions are limited. Not so with al Qaeda. Al Qaeda may preach that the regimes in Riyadh, Cairo, and Algiers are held in place by U.S. troops and influence, but the reality is that these governments have their own ruthless security services and means of buying off rivals that help them ensure their grip on power even if Washington abandons them.

Because of these risks, the decision to join al Qaeda often angers more sensible group members who retain local ambitions. One of Zawahiri's EIJ compatriots declared the merger a "great illusion," and in 2001 another member criticized joining bin Laden as a "dead end," fuming, "Enough pouring musk on barren land!" The dissenting comrade had it right: EIJ's cause is dead in Egypt today, and the decision to go global was the nail in the coffin.

It's not surprising, then, that not everyone in the jihadi camp signs up with al Qaeda. Samir Saleh Abdullah al-Suwailem, a Saudi fighter known as Khattab and for many years the most prominent Arab commander in Chechnya, shared many of al Qaeda's goals but rejected a formal relationship. At the time, he believed that he was close to defeating the Russians in Chechnya, and that taking on the United States or other new foes would be a distraction. Prominent groups in Egypt, Palestine, and elsewhere also have refused to entertain closer ties to al Qaeda, or have even rejected the organization publicly.

Handle with Care

All this suggests that for all the danger al Qaeda's growing network of affiliates poses to the West, it also offers opportunities for counterterrorism. Atrocities committed by one branch of al Qaeda can be used to discredit the core, as has happened with AQI. Ties to foreigners can alienate many insurgents, who are often motivated more by nationalism than religion. For example, AQI suffered when it declared its intention to make Iraq an Islamic state: Many of its potential Sunni supporters there came to see AQI as more of a threat to their independence than the United States. Even Somalis — who would seem immune to atrocity and bloodletting after years of conflict — were outraged by the spate of suicide bombings in recent years, blaming foreigners for it and thus undermining al-Shabab's legitimacy in the country.

Nor are all jihadi groups necessarily as professional as bin Laden's inner circle. The al Qaeda core represents an unusual set of leaders and operatives: Most are highly skilled, dedicated, well-trained, and meticulous about operational security. Affiliate members, however, are frequently less careful — their organizations often were born amid civil wars, and accordingly have focused more on maintaining a continued insurgency rather than focusing on pulling off a limited number of high-profile terrorist attacks. Years of fighting in the mountains of Algeria or the wastes of Yemen are not good preparation for infiltrating and attacking targets in the West.

That's the good news. The bad news is that counterterrorism success against locally focused groups can have unforeseen pitfalls. The United States should, of course, want its allies in the Muslim world to triumph over jihadists; even governments like Algeria's, which are hardly close friends, deserve support. But, as was the case for EIJ and GSPC, local failure may prompt some group members to go global, increasing the risk of anti-U.S. terrorism. Counterterrorism is not zero sum, but it would be naive and dangerous to assume that crushing local opponents won't encourage some cells to split off and join al Qaeda.

The most vexing dilemma for U.S. counterterrorism policy, however, concerns groups that may be moving toward al Qaeda but have not yet made the leap. Many al Qaeda affiliates always hated the United States and its allies, but their focus was local for many years. Because the groups had some ties to al Qaeda, George W. Bush's and Barack Obama's administrations began to target them and encourage others to do so. As a result, the groups became more anti-American, creating a vicious circle.

Consider Ethiopia's U.S.-supported 2006 invasion of Somalia, which intended to remove Islamists from power, and in the process splintered them into smaller groups. Al-Shabab emerged from one of the more radical fragments and has since become far more powerful. Angered by U.S. involvement in the invasion and the targeting of al Qaeda-linked individuals in Somalia, the group has become far more anti-American than its Islamist predecessor ever was. In short, U.S. administrations are often damned either way. Ignoring the group allows potential threats to grow worse and risks an attack from out of the blue. But taking them on may mean driving some deeper into al Qaeda's fold — and making the terrorist threat all the more dangerous.

There is no one-size-fits-all strategy. U.S. intelligence and other counterterrorism assets should continue to focus on the core of al Qaeda, which — both alone and in combination with affiliates — remains highly dangerous. For some affiliates — AQAP, for instance — the United States should rely first and foremost on local allies. In other cases, simply cultivating better relations with states at risk — such as Algeria, Mali, Mauritania, and others threatened by AQIM — is the wisest strategy. In Somalia, the best that can be hoped for may be simply containing the problem. In all these cases, however, the United States should strive to separate the locals from the al Qaeda core. The organization's merger strategy is a double-edged sword: Al Qaeda has gained from its acquisitions, but it can also be hurt by them.

Daniel Byman is a professor in the Security Studies Program at Georgetown University and a senior fellow at the Saban Center at the Brookings Institution. His forthcoming book is A High Price: The Triumphs and Failures of Israeli Counterterrorism.

Thirteen Georgia dams could be reclassified as high risk

Source: http://homelandsecuritynewswire.com/thirteen-georgia-dams-could-be-reclassified-high-risk

The number of dams designated high risk under Georgia's Safe Dams Act could more than double in two counties in the state, but a backlog in state enforcement because of budget cuts could drag the reclassification process out years longer than scheduled. The number of dams designated high risk under Georgia's Safe Dams Act could more than double in Richmond and Columbia counties, but a backlog in state enforcement because of budget cuts could drag the reclassification process out years longer than scheduled. The 1978 law, enacted after a dam failure in Toccoa killed thirty-nine people, requires state officials to inspect annually all Category I high-risk dams where loss of life could occur in the event of a failure; and to re-inspect lesser "Category II" dams at least every five years in case new development warrants re-designation to Category I. The Augusta Chronicle reports that currently, there are six high-risk dams in Augusta and three in Columbia County, but at least thirteen additional Category II dams have been identified for reclassification studies, said Tom Woosley, the manager of the Georgia Environmental Protection Division's Safe Dams Program. Those thirteen dams are among about 520 statewide, and the list continues to grow. "The list is backlogged," he said. "We can knock out maybe 30 to 40 a year, but in recent years we were adding more dams than we could get studied." The Safe Dams Program once had twelve employees but has shrunk to eight, making it difficult to reinspect all Category II dams every five years.

One of the **Category I dams** identified decades ago is at Woodbridge subdivision in Evans (photo), where homeowners are under a state mandate requiring improvements that could cost up to $250,000. The 33-acre lake, built in 1973, was modified after the Safe Dams Act was adopted. "There was a lot of work done to bring it up to the standards back then, but those standards changed over time, and now we are being forced to bring it up to newer standards," said Joe Wheeler, the vice president of the Woodbridge homeowners association, which has spent $30,000 on engineering work and is awaiting state approval for construction plans. Although a Category I designation is labeled high risk, it does not mean a dam is poorly built or improperly maintained, he said. Rather, it means the structure is held to standards designed to prevent the dam from getting into a condition where it could fail. "They've never come out and said our dam is in danger of breaching or anything like that," he said. "But all the things they are requiring are safeguards against that." Although owners of Category I dams are working to comply with state rules and finance needed improve-

ments, the delay in re-evaluating other dams could help their owners escape such scrutiny for years, Wheeler said. "We're being held to overly onerous requirements, while others go by without even falling into their area of responsibility."

The newspaper notes that one of the **Category II dams** awaiting reclassification studies is on a much larger lake just three miles away, at Windmill Plantation subdivision. The dam's Category II status, which exempts it from stricter rules, was adopted years ago, before development crept into the then-vacant land just across William Few Parkway from the base of the earthen structure. Today, several homes are in that zone — in addition to the Greenbrier preschool and day care center, which — according to its Web site — opened in late 2005 and tends to about 200 children. Woosley would not identify all 13 local dams awaiting possible reclassification but acknowledged Windmill as one of them because of the development in its downstream path. "That one is a Category II at least for today," he said. "People are building things all the time, so it's very common to find new hazards below an older dam." Although state officials are backlogged on inspections, local authorities also keep watch over dams and flood-prone areas, said Pam Tucker, Columbia County's emergency operations director.

"With all the state budget cuts, they're having a harder time than they used to have, and they've always been understaffed," she said. "The program doesn't really get the attention it should."

Media Attention to Terrorist Attacks: Causes and Consequences

Source: Institute for Homeland Security Solutions – Dec 2010

Political movements that engage in terrorism typically have too few material resources—personnel, funds, or territory under their control—to achieve their goals through legitimate political action or large-scale organized violence (Fromkin, 1975). Terrorist attacks are part of an indirect strategy for achieving their political objectives by influencing an audience (Crenshaw, 1981). These terrorist groups differ in the audiences that they seek to influence and in the messages they seek to communicate to their chosen audiences (Kydd & Walter, 2006). Some use terrorism to convince opponents to concede to their demands. Other terrorist groups seek to provoke authorities into engaging in indiscriminate repression, which will undermine support for the government and justify the use of terrorist violence. Some use violence to demonstrate to current and potential supporters a capacity to deliver powerful blows against their opponents. Media attention is an important vehicle by which terrorists communicate with their audiences, and thus a central goal of many terrorist groups is to influence the scale and tone of media attention to their attacks (Hoffman, 2006; Jenkins, 1975; Nacos, 2002).

However, terrorist attacks vary widely in the amount of media attention they receive. Most terrorist attacks receive no attention from major media outlets. Others, such as those in New York and Washington, DC, in 2001, London in 2005, and Mumbai in 2008, received heavy coverage (Kern, Just, & Norris, 2003, p. 40). This research brief summarizes the current understanding of factors influencing the decisions of media outlets to devote attention to terrorist attack and discusses how such coverage influences potential sympathizers and supporters.

RESEARCH BRIEF

Institute for Homeland Security Solutions
Applied research • Focused results

Understanding media attention to terrorism can inform homeland security policy in at least four ways.

First, the fact that most terrorist attacks receive no or little media attention suggests that terrorist groups vary substantially in their ability to design attacks to garner media attention. It is not easy for terrorists to manipulate the media coverage they receive. Knowledge of why some terrorist attacks succeed and others fail to attract media attention could provide important insights into the political goals, media savvy, and organizational capacity of the perpetrators.

Second, a better understanding of the motivations of and constraints facing media outlets could inform the design of media relations and public diplomacy strategies of agencies responsible for counterterrorism. As discussed in greater detail below, some argue that media outlets have incentives to provide overly extensive coverage of terrorist attacks. This coverage can provide terrorists with a vehicle for conveying their political messages to mass audiences, and it can also distract from public understanding of the difficulty of preventing terrorist attacks and the steps that the authorities take to achieve this objective. Research in this area has begun to explore, in a systematic manner, the conditions under which the media are more or less likely to devote considerable coverage to terrorist attacks rather than other topics or other aspects of counterterrorism.

Third, the structure and competitiveness of the news industry appear to influence media attention to terrorism. As the media environment becomes more decentralized and competitive, news outlets may try to maintain market share by devoting more attention to terrorist attacks that employ novel tactics or that are particularly violent. Such a development could pose new challenges for the media relations of homeland security agencies by giving the public a distorted picture of the threat from terrorism and reducing the ability of the authorities to explain their policies and to put the problem of terrorism in an appropriate context.

Fourth, existing research is beginning to explore how the tone with which the media covers terrorism influences the attitudes and behaviors of mass publics, including voters, as well as potential sympathizers with terrorist movements. There is considerable evidence that coverage of terrorism increases fear and anxiety and that these emotional changes influence the preference of some members of the public for counterterrorism policies that rely on force. This may make it more difficult for authorities to respond to terrorist attacks with other types of policies, even if these policies might produce superior results. It is sometimes claimed that terrorists are effective in manipulating media coverage to convey their message to a mass audience and to gain sympathizers and supporters (e.g., Hoffman, 2006). However, systematic research in this area is in its infancy, making it difficult to draw definitive conclusions about how terrorists' narratives influence their level of public support.

There are notable limitations in existing research on media attention to terrorism. Most studies have focused on elite Western media outlets. Much less is known about the attention to terrorism from more popular media outlets, which have very large audiences. Also, little is known about how terrorism is covered by the press in non-Western countries. Such countries experience a considerable amount of terrorism, and some are of particular concern to U.S. foreign policy. Many plausible explanations of media attention have not yet been systematically explored. There is a particular need to better understand how media attention influences the attitudes and behaviors of individuals, other terrorist groups, and government authorities. At the same time, technological developments such as easy access to media outlets through the Internet and advanced tools for sophisticated automated analysis of media content promise to open up new areas for investigation in the future.

IATA unveils plan for airport security tunnels

Source: http://homelandsecuritynewswire.com/iata-unveils-plan-airport-security-tunnels

The International Air Transport Association unveiled a plan to replace lengthy and sometimes intrusive passenger security checks at airports with a new system aimed at finding «bad people, not bad objects»; under the project, an early version of which could be in place within 2-3 years if governments cooperate, travelers would be directed down one of three security tunnels depending on profiles based on biometric data and flight booking data; the IATA plan would eliminate the need for nearly all intrusive screening as well as routine scanning and searches of carry-on luggage; IATA says the system would not be based on racial or ethnic profiling

The airline industry body IATA unveiled a plan on Tuesday to replace lengthy and sometimes intrusive passenger security checks at airports with a new system aimed at finding “bad people, not bad objects.”

Under the project, an early version of which could be in place within 2-3 years if governments cooperate, travelers would be directed down one of three security tunnels depending on profiles based on biometric data and flight booking data. “The current sy

A solution for intrusive searches // Source: silent-gardens.com stem of putting everyone through the same procedure — taking off shoes, pulling out laptops — is an incredible mess. It is causing longer and longer delays," said IATA director-general Giovanni Bisignani. "With today's terror threats, we need to be able to find bad people, not bad objects. We can only do that by assessing passengers for risk with appropriate security checks to follow," he told journalists at the body's Geneva headquarters. Air Transport World reports that Bisignani was speaking at a media briefing held every year by IATA, the 230-member International Air Transport Association, at which he announced the industry would return to profit this year and next at higher levels than expected. Airport security has mushroomed since the 9/11 attacks on U.S. targets by al Qaeda militants using hijacked passenger planes and subsequent attempts by suicide bombers to detonate inflight explosives, including a failed attempt by a Nigerian man on a U.S.-bound plane last Christmas Day. Anger at stepped-up airport security procedures — including full-body scanners and "pat-down" manual body searches, widespread in the United States — has spilt over recently with traveler revolts against the systems. The procedures have also caused diplomatic incidents, as when the Indian ambassador in Washington was subjected earlier this month to an airport pat-down in Mississippi and her government complained. The IATA plan — which Bisignani said had been in the works for some time before the U.S. passenger revolts — would eliminate the need for nearly all such screening as well as routine scanning and searches of carry-on luggage. After checking in heavy bags and passing passport controls, travelers would identify themselves at security with a fingerprint, biometric passport or mobile phone boarding pass, and be checked electronically against their stored profile. They would then be automatically assigned to one of the tunnels — one for registered "known travelers" where checks would be light, one where checks would be at "normal security" level, and the third an "enhanced security" lane. In the first two tunnels, most passengers would walk with hand luggage past sophisticated electronic detector devices and into the departure lounge if nothing unusual is registered. Bisignani said the profile would be based on details travelers provide when buying their ticket, including whether they had paid by cash or credit card, and would be checked by national security or intelligence services. IATA global security director Ken Dunlap said, however, that the system would not be based on racial or ethnic profiling. "We are completely opposed to checking people by the color of their skin or by their nationality," he added. Dunlap said IATA was discussing the plan with governments, which would have to finance it. If an intermediate version were in place by 2014 in key airports, a full one could be working within seven to ten years.

Underground security tech to revolutionize border security

Source: http://homelandsecuritynewswire.com/underground-security-tech-revolutionize-border-security

The University of Arizona College of Engineering is testing an invisible border monitoring system that could revolutionize the way the U.S. conducts homeland security; the border-monitoring system, known as Helios, consists of laser pulses transmitted through fiber-optic cables buried in the ground that respond to movements on the surface above; a detector at one or both ends of the cable analyzes these responses; Helios is sensitive enough to detect a dog and can discriminate between people, horses, and trucks.

A unique underground surveillance system tested by University of Arizona researchers could be used to watch the entire U.S.-Mexico border continuously. The border-monitoring system, known as Helios, consists of laser pulses transmitted through fiber-optic cables buried in the ground that respond to movements on the surface above. A detector at one or both ends of the cable analyzes these responses. Helios is sensitive enough to detect a dog and can discriminate between people, horses, and trucks. The system can be set to avoid being triggered by small animals and can also tell if people are running or walking, or digging, and in which direction. **Zonge**, a geophysical engineering company based in Tucson, Arizona, recently installed a Helios test system in the desert near Tucson. The University of Arizona's Lowell Institute for Mineral Resources is leading the project to evaluate Helios as a tool for border surveillance, assisted by the UA National Center for Border Security and Immigration. This is not new technology. Such systems are known as smart sensors and are already used to monitor large engineering works such as dams, pipelines, bridges and highways for cracks or seismic damage and other unseen strain forces at work deep within structures. The Helios system consists of fiber-optic cables, lasers and detectors and is more accurately described as a "distributed acoustic sensor." It relies on the physics phenomenon of "optical backscattering" for its operation and is made by the British company Fotech Solutions. "It's all a matter of scale," said Scott Urquhart, Zonge president and senior geophysicist, talking about the shift from detecting seismic events to measuring tiny subsurface vibrations caused by desert wildlife, both two- and four-legged. "When very small vibrations hit the fiber-optic cables, the cables are slightly distorted," Urquhart said. "This distortion creates a unique signature change in the laser pulses, which can be detected by the Helios unit." Urquhart said the Zonge team buried several types of cable at the desert test location. "Each had different properties in terms of flexibility or type of shielding," he said. "The advantage of a Kevlar cable, of course, versus a steel cable, is that the Kevlar cable cannot be found with a metal detector." Nor does digging up the cable and cutting it clean through stop the system working, provided a Helios unit is connected to both ends of the cable, Urquhart said. "We can detect people digging up the cable, and even if theycut it the signal doesn't stop flowing from the cut back to the Helios unit," he said. The resolution of the cable can be set to one-meter intervals, which means that the location of a cut cable, or people, or vehicles, can be pinpointed instantly to within one meter along a section of cable up to fifty kilometers long. Moe Momayez, associate professor of mining and geological engineering at the UA Lowell Institute for Mineral Resources, is co-author of a report detailing the recent Helios tests. "We can install cables up to 50 kilometers in length with only one Helios detector," he said. "Because the 50-nanosecond laser pulses travel at the speed of light, we can detect any event virtually instantaneously and deploy the appropriate resources to that location." These 50-kilometer cable lengths, each with a Helios detector, can be strung together indefinitely to cover vast distances. For example, the border between the United States and Mexico is 1,969 miles, or 3,169 kilometers. Although the extreme topography of some border areas would make cable deployment difficult, dividing the border length into 50-kilometer segments equates to approximately sixty-four cable sections and detector units. It is envisaged that Helios might be integrated into a larger system that includes mobile surveillance vehicles, such as those currently used by border patrol agents. For this and many other reasons it is too soon to name the cost of monitoring the U.S.-Mexico border, but all on the project agree it would be significantly lower than the ineffective barriers deployed to date, such as steel fences, disconnected grids of sensors, or hi-tech virtual fences. Momayez's report co-author is Kevin Moffitt, a research scientist at the UA National Center for Border Security and Immigration. They conclude in the report that "with sufficient training, an observer could reasonably differentiate between events triggered by a group of people, cattle, horses, digging tunnels, cars or even 'stealthy' border crossers." Fotech is already working on automating Helios operation. Once a database of signals has been built up over an extended period of time, advanced pattern-recognition software could be employed to automatically identify events detected by the Helios system. The system would generate an alert if the software determined that a border crosser was being detected. Zonge and Fotech have signed a two-year agreement to develop a border security application. The next step, according to the report, is a limited deployment along a stretch of border with a known high volume of border-crossing traffic. Zonge is seeking funding for this extended field trial, results from which would most likely be released at the discretion of the funding agency. Zonge is considering working with a technical partner that could provide large-scale analysis and storage of the volumes of data that the test system will gather. Representatives from a major defense contractor were present at the tests, as was an observer from the office of Rep. Gabrielle Giffords. Because Helios can detect if people are digging in or moving through underground tunnels, the system has great potential for perimeter security — prisons, for example – and mine safety. If such a system were installed in a network of mine shafts and tunnels, a trapped miner could just tap on the rock wall and the system could pinpoint his location to within a couple of feet.

Organized Crime vs. Terrorism

Source: http://www.stratfor.com/theme/video_dispatch

Analyst Reva Bhalla uses the Mexican drug cartel war to examine the differences between an organized criminal group and a terrorist organization. Mexican lawmakers recently passed legislation defining punishment for acts of terrorism. The most interesting aspect of this law is what was encompassed in that definition of terrorism, which could apply to cartel-related activities. This could be an emerging tactic by the Mexican government to politically characterize cartel-related activities as terrorism and use that as a way to undermine popular support for organized criminal activity in Mexico. There are some very clear distinctions between organized crime and terrorism. Organized criminal groups can engage in terrorist tactics. Terrorist groups can engage in organized criminal activity. These two sub state actors have very different aims, and these aims can place very different constraints on each.

An organized crime group cannot exist without an extensive peripheral network. In that peripheral network that will involve the bankers, politicians and police; basically the portals into the illicit world that protects the core of the organized crime group, which revolves around business activity. In this case being drug trafficking that the Mexican cartels are engaged in. With such a network territorial possessions come into play, and again, popular support is needed. That doesn't necessarily mean population condones the violence committed by the cartels but it does mean that the cartels can effectively intimidate the population to tolerate activity and allow business to go up on as usual.

By contrast a terrorist group does not need to rely on as extensive network. By definition terrorism is primarily driven by political aims. The financial aspect of their activities is a means to an end, so this place is very different constraints on the terrorist group and allows the terrorist group to engage in much bolder, riskier and violent acts then an organized crime group would. What's important about a terrorist act is that it's used to draw attention to their political objectives. Essentially terrorism is theater.

An interesting dynamic that we haven't seen quite play out yet in Mexico is when an organized crime group starts to adopt terrorist tactics. We have seen examples of where some cartels have engaged in beheadings and IED usage but not to a degree yet where there's been a big public backlash. In fact, in Mexico we've seen the population and major business groups come out against the government calling on the government to stop the offensive against the cartels and to allow business to go on as usual.

We have seen international examples of where this line has been crossed. For example, in 1992 the Sicilian Mafia La Cosa Nostra crossed a big line when they launched a massive car bombing against an important official. That unleashed a huge wave of public backlash. We also saw this in Colombia with Pablo Escobar and the huge IED campaign that swept across Colombia and that eventually turned people against the cartel dominance and resulted in intelligence sharing that led to the downfall of some of those key cartels. What we may be seeing here is a more subtle tactic by the Mexican government to deal with the cartels.

Despite the very important distinctions between organized crime groups and terrorist groups, the branding of an organized crime group like the Mexican cartels as terrorists could be a way to undermine the public tolerance for a lot of their activity in the country. Again, we have not seen this line crossed in Mexico and I don't think we're quite there yet but it will be interesting to see how the Mexican government attempts to re-brand the cartel war.

Two Faces of High-Seas Crime

Source: http://www.usni.org/magazines/proceedings/2010-07/two-faces-high-seas-crime

Maritime piracy and maritime terrorism must be tackled with a unified effort. Piracy off Somalia and the Horn of Africa is again the focus of attention due to a steep increase in the frequency of attacks that ave grown more violent and aggressive. These attacks have shifted to the high seas, even beyond the established naval patrol corridor in the Gulf of Aden. In 2009, piracy in this region has gone up by 126 percent.1 This increase has occurred despite a host of measures, including the passage of four resolutions by the United Nations in 2008, the deployment of multinational naval forces by more than a dozen countries, improvements in reporting systems of merchantmen, and establishing of a safety corridor for transit of merchant ships. And in a trouble spot such as Somalia, where terrorism and piracy flourish concomitantly, the symbiosis between the two is cause for concern. The world today faces a dual threat of global terrorism and maritime piracy, and yet, surprisingly, these are still being dealt with as separate and distinct problems. A 9/11-style attack at sea cannot be ruled out if terrorism and piracy are not addressed together in this region. Piracy not only poses a threat to global commerce and human safety at sea, but also encourages the use of sea routes for the spread of terrorism. Because piracy can be used as a complementary form of terrorism, the international community needs to attack both issues in a unified effort at their roots in Somalia and extend the global war on terrorism to this region.

Piracy, Terrorism: Same Coin, Different Sides?

Terrorism at sea needs to be accepted and addressed as a problem intertwined with piracy. Contrary to the belief that pirates operate with the sole objective of financial gain, many of today's pirates, like terrorists, have an ideological mindset and a broad political agenda. Meanwhile, many terrorist organizations have sought to develop maritime capabilities so they can exploit the sea to further spread terrorism. Terrorist groups known to operate at sea using pirates' techniques are:

- the Liberation Tigers of Tamil Eelam-Sri Lankan separatists also known as the Tamil Tigers
- the Palestine Liberation Organization
- the Free Aceh movement-Sumatran separatists
- the Moro Islamic Liberation Front, Moro Liberation Front-related Filipino militant

Islamic groups

- Jemaah Islamiyah-Southeast Asian militant Islamic group
- al Qaeda
- Hezbollah.

Similarities exist between piracy and terrorism, namely their methods of deployment and targeting, with both groups threatening life and economic activities at sea or in ports. According to Stephanie Hanson, who writes on African issues for the Council on Foreign Relations, there are two key areas in which piracy and terrorism overlap. The first is legal, wherein both groups, being non-state actors, divorce themselves from their nation-states and form extraterritorial enclaves. They conduct acts of homicide and destruction against civilians for private ends. The second area of overlap is financial, with pirates known to fund Islamic terrorist organizations in Somalia and Indonesia. Obviously, there are differences as well. In their purest forms, piracy and terrorism have divergent motives and (because their motives differ) each pursuit has a different attitude toward publicity. Piracy is mostly undertaken for financial reasons, terrorism for political or religious reasons; whereas pirates prefer to avoid publicity and use violence as a last resort, maritime terrorists typically aim for maximum publicity and violence. But the world they mutually inhabit fosters a blurring of the lines. The sources of piracy and terrorism are getting more entangled. Especially within Somalia, links exist between pirates and terrorist groups; in addition to being a bustling pirates' nest, Somalia is one of the three main theaters for al Qaeda's mujahideen, along with Iraq and Afghanistan, according to al Qaeda leader Ayman al-Zawahiri.[7] Modern-day pirate waters—the Gulf of Aden, the Arabian Sea, the Indian Ocean, and the South China Sea—have become lucrative realms for exploitation by terrorist organizations as well. Using pirate tactics, they seek to extend their jihad to sea. Today's pirates are trained fighters, violent and aggressive, taking to the high seas in mother ships and speedboats. Their use of satellite phones, GPS, AK-47s, anti-tank missiles, and rocket-propelled grenades hints at shared training with terrorists. With bank accounts frozen as part of the anti-terror crackdown, major terrorist groups are feeling the financial crunch and learning to rely on alternate funding sources: They're either engaging in acts of piracy themselves or outsourcing hijacking jobs to pirates. In addition to fund-raising, the rogues' alliance extends to gun-running as well. The Somalian Islamist insurgency group al Shabaab is now working with pirates and local warlords to smuggle arms and ammunition. In the face of massive international efforts arrayed against them, pirates and terrorists have joined hands.

With 80 percent of the world's trade cargo and 60 percent of the world's oil and gas traversing the oceanic highways, it is little wonder that terrorists regard the sea as «the next strategic step towards ruling the world . . . a strategic point to expel the enemy from the most important pillars of its battle.» Al Qaeda has undergone maritime-terrorism training with Sri Lanka's Tamil Tigers, and al Qaeda strategist Al-Suri writes about carrying out attacks in the Straits of Hormuz and at Bar el-Mandeb by scuttling ships at choke points. In addition, al Qaeda has been closely monitoring the success of the Somali pirates and showing appreciation of the pirates' achievements on al Qaeda Web sites.

Somali Terror Triangle

Somalia is the unfortunate center of a «terror triangle,» a three-part recipe consisting of a failed state, piracy, and terrorism. As a failed and ungoverned state since 1991, Somalia poses a threat to international security with a host of associated problems. Lawlessness in Somalia has affected the entire region and created problems such as arms flow and other black markets, an environmental threat with toxic waste dumping along the coastline, illegal immigrants, illegal fishing, and, of course, piracy. Piracy off the Horn of Africa accounts for 48 percent of the total number of attacks reported in 2009. Somalia's terrorist element, meanwhile, includes such radical movements as the Union of Islamic Courts, al Ittihad al Islamiyya, and al Shabaab, which share parallel jihadist ideologies, have links with al Qaeda, and are known to provide assistance to transnational Islamic terrorists. Having lost reliable bases elsewhere due to the global war on terror, al Qaeda has used Somalia not only as a transit or entry port fo a safe haven, but also as a base from which to spread terrorism. The implications for international security are serious, particularly in the maritime context. Somalia offers an ideal opportunity for al Qaeda and related terrorist groups to pool resources with pirates. As these existing links become stronger, al Qaeda, using pirates' expertise and training, could increasingly extend terrorism to the sea, generate money, and strengthen into a pirate-warlord confederacy. Somalia-based extremists coordinating their schemes with Somalia-based pirates pose the greatest maritime terror challenge in the near future.

An Emerging, Unified Definition

While the debate about the relative similarities and differences between piracy and terrorism is ongoing, a comprehensive definition is needed for the areas in which they indeed do overlap-in short, a definition of maritime terrorism: Any act of piracy or terrorism undertaken in territorial waters or high seas for personal, financial or political motive against military or civilian targets by non-state actors. It also includes acts of piracy conducted with the motive of passing the monetary benefits to support terrorist organizations. Operating within a maritime-terrorism context would improve both counter-terrorism and counter-piracy actions by preventing any breach of sovereignty, ensuring concerted efforts, and providing more clear-cut legal parameters. The implications of resolving maritime terrorism and piracy off the coast of Somalia and throughout the world involves a multi-directional approach that begins with addressing the problems on land. Such an approach entails monitoring and surveillance of Somalia as part of the global war on terrorism, with emphasis on beaches, ports, and cross-border smuggling points. It may even require landing an international-coalition military force ashore in those regions that foster piracy. Parallel initiatives already being undertaken by international naval forces need to continue along with these land efforts to eradicate piracy. The aim must be to ensure that the piracy-terrorism link is not strengthened, and that it does not become a platform for terrorists in the immediate future. Post-9/11, the international community has been faced with many new challenges, prominent among them being failed states, terrorism, and piracy. Though the efforts are on to curb these problems, they have not been synchronized. It should be understood that piracy and terrorism are no longer two different problems and need to be addressed together by accepting this merger and legally defining it as maritime terrorism. So far, despite increased efforts, the international community has not been successful in controlling or eradicating either menace. Left unchecked, pirates and terrorists increasingly will pool their resources and terror groups will hire local pirates for financial gain and to buttress their jihad's maritime element. Whatever the motivation for this merger-ideology, poverty, criminality, or all of the above-the nexus of piracy and terrorism will be dangerous for both the world economy and security. When addressing the alarming rise in piracy off Somalia, we must not overlook the emerging alliance between piracy and terrorism. To win the battles against piracy and terrorism, they need to be perceived as one battle; they need to be resolved with a unified effort, extending the global war on terrorism to include a war on maritime terrorism, with Somalia as its focal point, to prevent another 9/11-this time at sea.

Lieutenant Commander Chaturvedi recently graduated from the Marine Corps University's Expeditionary Warfare School in Quantico, Virginia. A surface warfare officer specializing in missiles and gunnery, he has held various gunnery-officer posts on Indian Navy guided-missile destroyers and missile corvettes, and has commanded a torpedo-firing and recovery vessel.

CBRN Security in the public sector

Live Agent Training

Build stronger, more competent teams in field exercises using live chemical agents, biological materials, radiological materials and improvised explosive devices. Gain confidence, knowledge and experience not possible with the use of simulants alone.

On Site Training

Create highly skilled employees through on-site theoretical and practical training using specially formulated simulants designed to respond to detectors.

Equipment Testing

Conduct operational testing of CBRN equipment with live chemical agents under field conditions.

hotzone SOLUTIONS

http://www.hotzonesolutions.com

HEADQUARTER
Hotzone Solutions Group
Binckhorstlaan 36, suite C010
2516 BE, The Hague, Netherlands
Ph. +31 70 262 9704
Email: info@hotzonesolutions.com

AUSTRIA
Hotzone Solutions GmbH
P.O. Box 107
7100 Neusiedl, Austria
Ph. +43 699 1966 7890
Email: info@hotzonesolutions.com

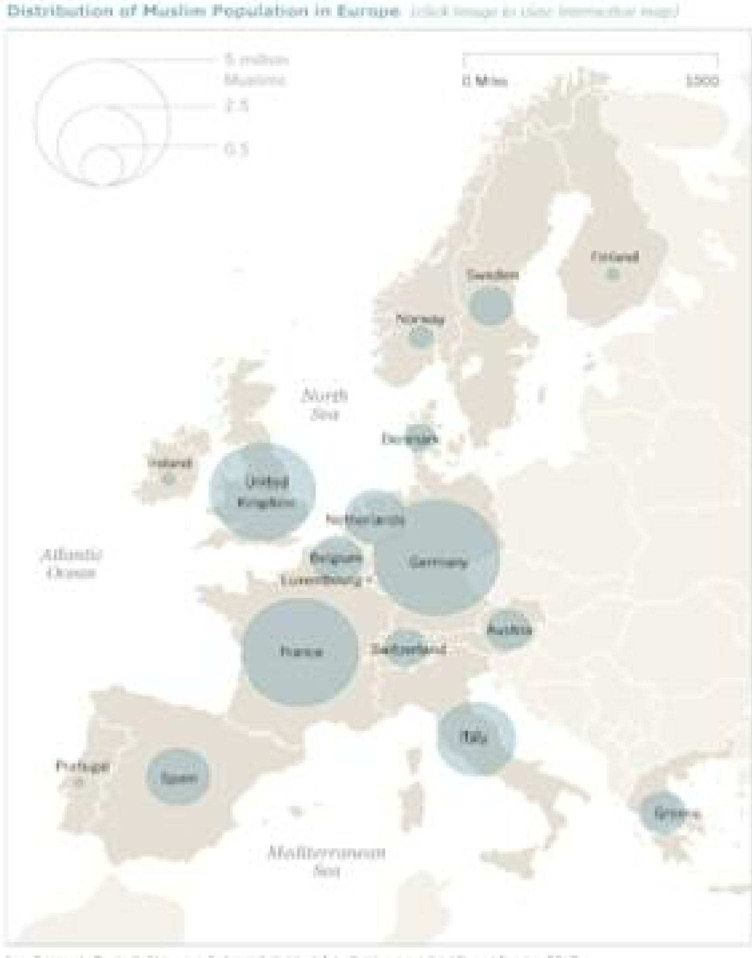
The Muslim population has grown from 1.65 million to 2.87 million since 2001

What does this mean for liberal Britain?

Source:http://blogs.telegraph.co.uk/news/damianthompson/100069830/the-muslim-population-has-grown-from-1-65-million-to-2-87-million-since-2001-say-researchers-what-does-this-mean-for-liberal-britain/

The Pew Forum on Religion and Public Life estimates that there are 2,869,000 Muslims in Britain, an increase of 74 per cent on its previous figure of 1,647,000, which was based on the 2001 census. No demographic statistics are reliable in an era of open borders, but such an expansion is unprecedented. The figure of 2.87 million was first published by Pew in a little-noticed press release last September, announcing a report on Muslim Networks and Movements in Western Europe. The Pew Centre, based in Washington DC, is one of the most respected demographic research bodies in the world; its methodology is scrupulous and its approach non-partisan. The new total for British Muslims means that, so far as this country as concerned, Pew's major 2009 report Mapping the Global Muslim Population is already spectacularly out of date. Here's a map showing the updated distribution of the Muslim population in Europe:

Distribution of Muslim Population in Europe (click image to view interactive map)



Pew Research Center's Forum on Religion & Public Life • Forthcoming Pew Forum Report, 2010

The material about global Islam in the 2010 report is fascinating, but it's the revision of British figures that took me by surprise. Why was it not more widely reported in the autumn? And what are the implications for society? For an analysis that puts the statistics in context, let me recommend this article from the British Religion In Numbers website, which makes the point that the 2001 figure was probably an underestimate.

Pew's UK figure for 2010 is 2,869,000, which is equivalent to 4.6% of the population. In absolute terms, the UK has the third largest Muslim community on the continent, after Germany (4,119,000) and France (3,574,000). In percentage terms, the UK is in ninth position, after Belgium (6.0%), France, Austria and Switzerland (5.7%), The Netherlands (5.5%), Germany (5.0%), Sweden (4.9%) and Greece (4.7%). UK Muslims account for 16.8% of all Muslims in Western Europe. There have been other indications of a dramatic increase in the numbers of British Muslims: the UK Labour Force Survey recorded a rise from 1,870,000 in 2004 to 2,422,000 in 2008. So Pew's findings aren't unsupported by independent data. Common sense suggests explanations for the increase: a high Muslim birth rate and large-scale immigration. But I'm not sure that common sense tells us what this demographic earthquake means in practice for British public life.

Setting aside for the moment the topics of Muslim ghettos and jihadist Islam, let's ask another question. How will the rapid growth of a conservative religion affect British social attitudes towards women's rights, marriage, divorce, homosexuality and abortion? Liberal commentators are busy making fools of themselves in the Guardian and on Twitter accusing the mild-mannered Coalition of behaving like Nazis for trimming state spending. But I suspect that nothing politicians do will, in chattering terminology, "set back" social attitudes as drastically as the growth among young people of a faith that, even in its moderate incarnations, is resolutely non-liberal on many moral issues. What do you think?

Terrorism and the Maritime Transportation System

Anthony M. Davis

Source:http://www.homelandsecuritygroup.info/index.php?option=com_content&view=section&layout=blog&id=7&Itemid=15

Each day there seems to be new reports of piracy near the coast of Somalia. The pirates have learned over time that a hostile takeover of an unwitting crew and cargo is big business. With each successful attack, they get their prize – ransom. In the past, smaller cargo and fishing vessels transiting isolated shipping lanes along the coast were easy targets by pirates concealed by a variety of unprotected inlets. Criminal organizations behind piracy attacks continued filling their coffers with ransom payments. As commercial shippers sought safer passage, they began transiting further from the dangerous waters known for attacks. The pirates looking for their prey now began traveling further out to sea for the hunt. By doing so, they found bigger, more lucrative vessels…and unprotected targets of opportunity. The International Maritime Bureau reports a, "dramatic increase in attacks of piracy for the first nine months of 2008." The heightened number of piracy incidents is attributed to instability in the region, particularly the hazardous waters of the Gulf of Aden and the East coast of Somalia. The region faces continual political disorder with no indicator that anyone in power will challenge organized crime groups attacking vessels in the region. Incidents of piracy off the coast of Somalia are directly proportional to the political environment.

Some History

During the summer of 2006, the Union of Islamic Courts (UIC) came to power in Somalia. Immediately afterward, the UIC announced they would punish those engaged in piracy according to Sharia law. For a time the incidents ceased, until pirates struck the United Arab Emirates cargo ship, MV Veesham I. A small boat with six pirates boarded and took control of the cargo ship shortly after leaving port. Initially the pirates demanded a $1 million ransom; negotiations lowered the amount to $150,000. The UIC in response, set to sea in small boats, recaptured the vessel and rescued the crew after a gun battle with the pirates.

The UIC withstood the challenge to their authority. Unfortunately, the success was short-lived. One month later, Ethiopian forces entered Somalia gaining political control of the country. They pushed the UIC out of power. With the UIC gone, the organized gangs of pirates no longer feared governmental retribution for their offshore attacks. Offshore piracy assaults continued again.

Rules of Engagement

Recently, I was asked a variety of questions related to the "Rules of Engagement" for the protection of cargo vessels transiting piracy-prone areas. Discussions with a variety of law enforcement and security professionals indicated they had the same questions. Given that, here's an attempt to clarify the options available for commercial shippers transiting the area. The answers below apply to U.S. mariners sailing under a Merchant Mariners' Document (MMD) or USCG License.

Question: It seems that pirates have no difficulty these days jumping onto a cargo ship; can the crew shoot back at them?

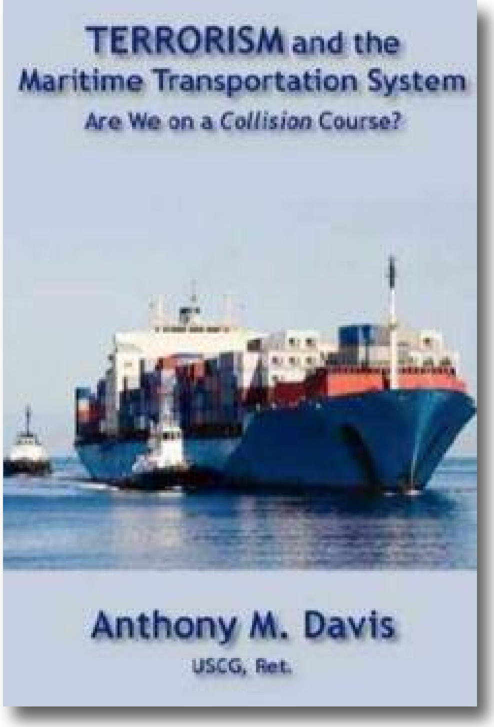
Generally, that's a bad idea. If the crew were to engage in an at-sea firefight, the pirate is more agile and difficult to hit. If a crew starts shooting, it is likely the pirates will make a choice: leave or shoot back.

As I describe in my book, "Terrorism and the Maritime Transportation System" the weapon of choice for pirates are AK-47 assault rifles and Rocket-Propelled Grenades (RPG). If attacked by an RPG, the ship becomes vulnerable to fire and no sailor wants to face such a calamity at sea. If a ship burns, there's nowhere to go. When combating a fire, the ship must stop otherwise the prevailing wind caused by forward motion of the vessel feeds the fire, making matters worse. The Captain generally has two choices: risk catastrophic damage to the vessel, risk crew safety and stop, or, protect the ship and stop. A minimal crew with no security protection stands little chance of successfully fighting a fire and out maneuvering a smaller, faster boat armed with weapons. The ship will always stop and the pirates know that.

Question: Is the crew allowed to carry firearms in a cargo ship?

Title 46 of United States Code applies to U.S. Merchant Mariners. There is no provision within the code allowing crew to carry firearms. In fact, mariners are subject to standing regulations defined by the Master of the vessel. Typically, prohibitions include drugs, alcohol and weapons being brought aboard the vessel. Violations can result in punitive measures, including a charge of misconduct resulting in suspension or revocation of their license or document as noted in 46 U.S. Code § 7703, "Bases for suspension or revocation. " Additionally, the regulation pertaining to Personnel Action against mariners is included in 46 Code of Federal Regulations 5.27:

> *"Misconduct is human behavior which violates some formal, duly established rule. Such rules are found in, among other places, statutes, regulations, the common law, the general maritime law, a ship's regulation or order, or shipping articles and similar sources. It is an act which is forbidden or a failure to do that which is required."*



That's the long answer. The short answer is: No.

Question: I understand that if the pirate attack happens within territorial waters, the ship captain cannot take matters on his own hands but depends on the navy of the country guarding that coast. Is this correct?

One of the reasons that piracy is so rampant near the coast of Somalia, Nigeria and the Gulf of Aden is that there are few security resources available to protect a vessel. The International Maritime Organization (IMO) established a Maritime Security Patrol Area with the intent of discouraging attacks against vessels transiting the area. There are few resources available with a large body of water. I remember many U.S. Coast Guard patrols when we were searching for survivors from a marine casualty, drug smugglers or migrant traffickers. There were times when we knew of a last location or intelligence may have provided an intended track line for smugglers. Many times, we were successful; other times not. A body of water seems very large when searching for a small boat.

In August of this year, the USS Peleliu received a distress from the Singaporean cargo ship, Gem of Kilakarai. The naval ship was outfitted with a contingent of U.S. Marine helicopters from the 15th Marine Expeditionary Unit. The Marines launched two aircraft and chased the pirates away. While the Navy and Marine Corps did an excellent job, it's important to note that the piracy attempt was only 10-miles from the ship. The favorable results came from quick notification and the close location. Another issue deals with territorial waters. The U.S. or other allied vessels will not engage unless fired upon, or given specific permission to conduct law enforcement missions within their waters. Just as the U.S respects our own territorial boundaries, we must respect those of other nations. For those incidents occurring within territorial waters, there are many times no resources to help.

Question: What are the rules of engagement for private cargo ships?

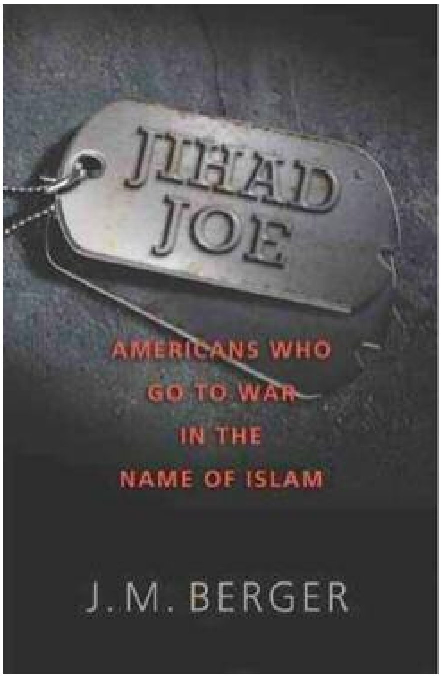
Given that the crews of cargo ships are exempt from carrying weapons according to U.S. law, the remaining options are to use non-lethal force or hire private security. Crews can use a variety of sonic guns, water cannons, etc. These have some value but still, the pirates can often out maneuver a larger vessel and attempt to climb aboard in a place outside the range/bearing of the gun. Personally, I would consider coating a portion of the decks where a pirate would likely climb aboard with a thick, biodegradable coating of lard. Once someone slips and falls in that mess, they can be an easy target to take them down. The other option of course is to hire private security protection. Remembering the points I made earlier about RPG's and fire at sea, private security professionals must consider specific tactical options. When pirates attack, it impacts the global economy. Ships are detained or stolen, crews are injured and sometimes killed and cargoes are lost. With each incident, maritime shipping firms are faced with cargo losses and the payout of high ransoms. Sometimes attacks are not reported attempting to prevent maritime insurers from raising already expensive premiums. In the end, confidence of safe global shipping is in jeopardy. Pirates making millions each year continue to buy weapons and new communications technologies to build upon their organized crime network. As these networks grow, their logistical and internal intelligence capability increases. Over time, there are more loyal to the network than those seeking to prevent attacks. The same methodology continues much like organized drug and alien smuggling operations have for years. Terrorist organizations operate the same way. According to a Washington DC-based think tank, they say there is no link between piracy and terrorism. I disagree; but that's ok. We need to look at each problem from every direction and sometimes collaboratively seek viable options. Piracy is seriously impacting the global economy in a negative way. Perhaps the rules of engagement should be revisited.

Jihad Joe: Americans Who Go to War in the Name of Islam

J. M. Berger (Author)

They are Americans, and they are mujahideen. Hundreds of men from every imaginable background have walked away from the traditional American dream to volunteer for battle in the name of Islam. Some have taken part in foreign wars that aligned with U.S. interests while others have carried out violence against Western interests abroad, fought against the U.S. military, and even plotted terrorist attacks on American soil. This story plays out over decades and continents: from the Americans who took part in the siege of Mecca in 1979 through conflicts in Lebanon, Afghanistan, and Bosnia, and continuing today in Afghanistan and Somalia.

Investigative journalist J. M. Berger profiles numerous fighters, including some who joined al Qaeda and others who chose a different path. In these pages he portrays, among others, Abdullah Rashid, who fought the Soviets in Afghanistan; Mohammed Loay Bayazid, who was present at the founding of al Qaeda; Ismail Royer, who fought in Bosnia and Kashmir, then returned to run training camps in the United States; Adam Gadahn, a California Jew who is now al Qaeda's chief



spokesman; and Anwar Awlaki, the Yemeni-American imam with links to 9/11 who is now considered one of the biggest threats to America's security.

J. M. Berger is an investigative journalist working on television documentaries about al Qaeda and the global foreign fighter (mujahideen) phenomenon. Berger recently completed work on a documentary about America's role in the Bosnian civil war, which premiered on European television in 2010. His previous work includes the 2006 National Geographic documentary Triple Cross, about an American al Qaeda operative who infiltrated the Army and FBI. He runs the investigative journalism website Intelwire.com from his office in the greater Boston area.

Homegrown terrorists share characteristics, backgrounds

Source: http://homelandsecuritynewswire.com/homegrown-terrorists-share-characteristics-backgrounds

Since the 9/11 attacks, 90 people were arrested in the United States on terrorism charges for plots or attacks against the United States; a new study of the group finds that 44 percent had prior criminal records; 61 percent of the terrorism defendants attended some college, including three who earned doctoral degrees; 64 percent of those college-educated terrorism suspects were engineering majors

Almost half of those arrested for plotting or carrying out attacks against the United States had prior criminal records, mostly for small-time offenses, a study by New York state investigators found. Such interactions with local law enforcement represented possible opportunities to "detect and deter an attack," the study said.

Abdulmutallab - underwear bomber, mechanical engineer // Source: mirror.co.uk

The Wall Street Journal reviewed a draft of the study by officials at the New York State Intelligence Center titled "The Vigilance Project: An Analysis of 32 Terrorism Cases Against the Homeland." Using twenty-five variables, such as place of birth, age, religion, and affiliations, the report attempted to identify "trends in basic pedigree information" of ninety people arrested in connection with the thirty-two cases, which all took place after the attacks of 9/11. One of the variables looked at by officials at the center, which is run by the New York State Police and brings together federal, other state, and local agencies to analyze and share information about terrorism, was the terror suspects' criminal backgrounds. Center officials obtained the criminal histories of 77 of the 90 people arrested on terrorism charges for plots or attacks against the United States after 9/11. Thirty-four of those suspects, or 44 percent, had prior criminal records, according to the report. A third of the charges were for possession or sale of drugs. All but one of those cases involved marijuana, according to the report. The next leading charge was for assault and battery, followed by weapons possession, the report said. "Assuming that criminal history information about these individuals is placed in appropriate law enforcement databases, each instance of contact with local law enforcement officers represents a possible opportunity for them to detect and deter an attack," the report said. "It can also provide an opportunity to identify associates and links to foreign entities through subsequent investigation. As such, law enforcement can play a critical role in the counter-terrorism arena while performing routine duties."

The Wall Street Journal reports that the cases analyzed by the New York state officials began with the so-called shoe bomber, Richard Reid, who tried to set off explosives hidden in his boot during a Paris to Miami flight in December 2001. The most recent of the terrorism cases was the Times Square car bombing attempted by Faisal Shahzad in May. Thirteen of the cases were plots against targets in New York or New Jersey. The pedigree information provided a general description of the terrorists arrested in the thirty-two cases; young men, mostly educated, and mostly U.S. citizens. Eighty-two percent were between the ages of 18 and 33, suggesting "that younger persons are less established, more impressionable, and therefore more susceptible to radicalization," according to the report. The report said 61 percent of the terrorism defendants attended some college, including three who earned doctoral degrees. The report states that 64 percent of those college-educated terrorism suspects were engineering majors. Fifty of the 88 suspects in the study whose citizenship could be identified were born in the U.S., the report said. Eleven of those were born in New York and eight in California. Also, 11 of the 32 cases happened during the past two years. In those cases, 17 of the 19 defendants were in this country legally. "Based on that information," the report said, "it is likely that the 'homegrown' threat will remain a considerable challenge to our law enforcement partners in the future." Thomas Fresenius, the state police lieutenant colonel who heads the New York State Intelligence Center, declined to discuss the specifics of the report with the Wall Street Journal because he said it is "law enforcement sensitive." He said, though, that the intent of the project was to try to pull together all the available information on terrorism attacks on the United States and create a "living document" — one that is updated with all new case information. The information is intended to provide law-enforcement officers with some personal and tactical characteristics of typical terrorism suspects to keep them engaged in the fight against terrorism. Fresenius said the study shows that for officers from the largest to the smallest police agency, "there are opportunities at all times to possibly come across and encounter the movements and behavior of these people."

Al Qaeda aiming at soft targets in U.S.

Source: http://homelandsecuritynewswire.com/al-qaeda-aiming-soft-targets-us

DHS has ramped up its efforts to protect soft targets in the United States from terrorist attack this year; the department has issued bulletins to state and local law enforcement warning of the possibility terrorists could target religious gatherings, sports matches, and parades; the al Qaeda affiliate in Yemen puts out an online magazine in English that encourages U.S. residents to plan attacks. Suggestions include driving a truck into a crowded place or shooting into a restaurant

The U.S. Department of Homeland Security ramped up its efforts to protect soft targets from terrorist attack this year, intelligence analysts said. During the holidays, the effort has included more visible security at places like train stations, the Los Angeles Times reports.

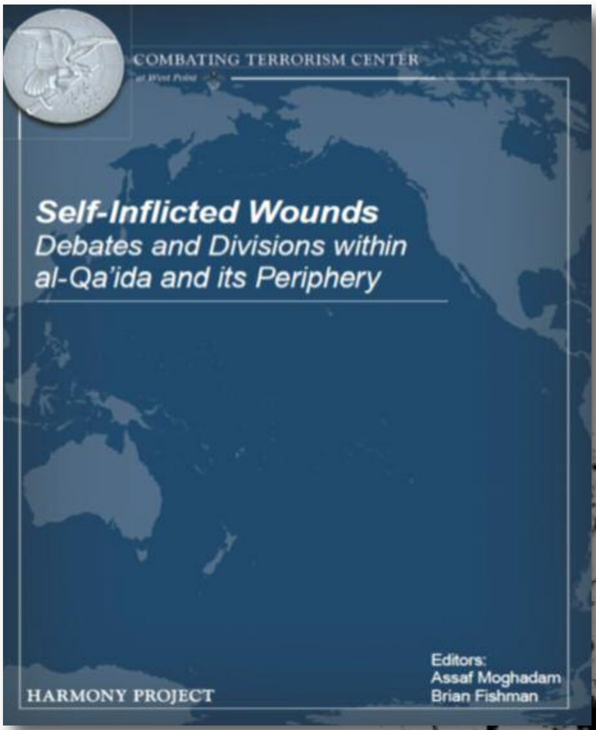
DC Metro station at rush hour // Source: thedc-traveler.com

Just before Christmas, riders on the Washington Metro were subjected to random checks. UPI reports that the department has issued bulletins to state and local law enforcement warning of the possibility terrorists could target religious gatherings, sports matches, and parades. Rick Nelson of the Center for Strategic and International Studies suggested al Qaeda affiliates are trying "to expand their repertoire" because their leadership in Pakistan is under pressure. As a result, he said, they are turning to attacks that are easy to carry out even if they are less dramatic than the destruction of the World Trade Center or the London Transport bombings. The al Qaeda affiliate in Yemen puts out an online magazine in English that encourages U.S. residents to plan attacks. Suggestions include driving a truck into a crowded place or shooting into a restaurant.

Self-inflicted wounds: Debates and division within al Qaeda and its periphery

Edited by Assaf Moghadam and Brian Fishman
Harmony Project – Combating Terrorism Center at West Point
Source: www.ctc.usma.edu

As we approach the tenth anniversary of the 9/11 attacks next September, the United States, its Western allies, and nearly all states in the Islamic world are facing a weakened jihadi enemy, but one still capable of inflicting, or threatening to inflict, spectacular acts of terrorist violence. The recent attempts to send package bombs on cargo planes is only the latest in a series of plots suggesting that although al Qaeda and its cohorts have suffered a number of setbacks, the group and its affiliates and associates continue to pose a serious challenge to the security of the United States and its allies. Self-Inflicted Wounds: Debates and Divisions within al Qaeda and its Periphery examines the internal, or endogenous, reasons that have hastened the decline of the jihadi movement. In doing so, it exposes the jihadi movement, with al Qaeda at its helm, as one that lacks coherence and unity, despite its claims to the contrary. The report divides the jihadis' endogenous problems into two categories: internal divisions plaguing al Qaeda and the jihadi movement proper; and fault lines dividing the jihadi movement from other Muslim and Islamist actors. The internal jihadi divisions examined in this report include tactical disagreements over takfir (excommunication of Muslims) and the killing of Muslims; Strategic disagreements over whether the jihadi struggle should focus on the near enemy (i.e., nominally Muslim regimes) or the far enemy (the United States and its Western allies); friction between jihadi pragmatists and jihadi doctrinarians; rifts between al Qaeda Central and local affiliates; as well as the sometimes tense relations between Arab and non]Arab members of the jihadi movement. The competition between the jihadis and their Muslim counterparts scrutinizes the jihadis' relationship with the Muslim Brotherhood, Hamas, and the Shi'a community. Three main counterintuitive findings can be gleaned from the discussion. First, while the net impact of divisions within and around



COMBATING TERRORISM CENTER
at West Point

Self-Inflicted Wounds
Debates and Divisions within al-Qa'ida and its Periphery

HARMONY PROJECT

Editors:
Assaf Moghadam
Brian Fishman

the jihadis on their movement is negative, the jihadi movement is resilient to some of these divisions due to its unique structure and situational context. Even worse, and contrary to the received wisdom, intra-jihadi rifts and fault lines between jihadis and other Islamic actors may even enhance some of the jihadi movement□fs resilient traits. Second, we find that although the jihadi movements' competition with its non-jihadi Islamic counterparts is mostly harmful to al Qaeda, such competition bestows certain advantages on the group. On the one hand, al Qaeda cannot possibly compete with groups such as the Muslim Brotherhood, Hamas, or Hizballah, who have far deeper social bases and provide social services to their constituents. At the same time, al Qaeda's status as a recalcitrant underdog affords it a higher degree of credibility among more extremist members of the umma. A third broad finding is that jihadi divisions matter in different ways. Quarrels over tactics and strategy tend to be more damaging to jihadis than dissent over goals and views of the enemy. Disagreements over tactics.and especially ongoing protests at al Qaeda's killing of Muslims.have greater potential to shove al Qaeda further toward the margins of the Islamic community than to split jihadi organizations. Ongoing leadership debates over strategic questions, on the other hand, can pose direct threats to the group itself, but do not necessarily marginalize al Qaeda further from the mainstream. In practical terms, certain tactics tend to be more controversial for jihadis than lack of consensus on broader questions as goals and objectives because tactical adaptations have direct practical consequences visible on the ground. The report highlights a number of additional findings. First, it argues that the jihadi movement can be usefully divided into three categories – global, classical, and hybrid – with important implications for counterterrorism policy. Counter-radicalization and deradicalization techniques that might be effective with global jihadis, for example, may not be as effective with classical or hybrid jihadis. Second, the practice of takfir and attacks on Muslims are the jihadis' most consequential weakness and should be actively exploited. And third, the jihadi community is increasingly divided about its leadership, especially as a younger generation of virtually-connected fighters usurps traditional sources of strategic and ideological authority. In the final section of the report, the editors conclude with a number of recommendations for policymakers. They are designed to advance our thinking on how jihadi and Islamist fault lines can be exploited in a way that does not exacerbate the problem of jihadi violence.

Kosovo «Freedom Fighters» Financed by Organised Crime

By Michel Chossudovsky

Source: www.globalresearch.ca/index.php?context=va&aid=22619

Author's note: This article was published almost 12 years ago, at the height of the NATO bombings of Yugoslavia.

Heralded by the global media as a humanitarian peace-keeping mission, NATO's ruthless bombing of Belgrade and Pristina goes far beyond the breach of international law. While Slobodan Milosevic is demonised, portrayed as a remorseless dictator, the Kosovo Liberation Army (KLA) is upheld as a self-respecting nationalist movement struggling for the rights of ethnic Albanians. The truth of the matter is that the KLA is sustained by organised crime with the tacit approval of the United States and its allies.

Following a pattern set during the War in Bosnia, public opinion has been carefully misled. The multibillion dollar Balkans narcotics trade has played a crucial role in «financing the conflict» in Kosovo in accordance with Western economic, strategic and military objectives. Amply documented by European police files, acknowledged by numerous studies, the links of the Kosovo Liberation Army (KLA) to criminal syndicates in Albania, Turkey and the European Union have been known to Western governments and intelligence agencies since the mid-1990s.

« ... The financing of the Kosovo guerrilla war poses critical questions and it sorely tests claims of an «ethical» foreign policy. Should the West back a guerrilla army that appears to partly financed by organised crime.»[1]

While KLA leaders were shaking hands with US Secretary of State Madeleine Albright at Rambouillet, Europol (the European Police Organization based in The Hague) was «preparing a report for European interior and justice ministers on a connection between the KLA and Albanian drug gangs.»[2] In the meantime, the rebel army has been skilfully heralded by the global media (in the months preceding the NATO bombings) as broadly representative of the interests of ethnic Albanians in Kosovo.

With KLA leader Hashim Thaci (a 29 year «freedom fighter») appointed as chief negotiator at Rambouillet, the KLA has become the de facto helmsman of the peace process on behalf of the ethnic Albanian majority and this despite its links to the drug trade. The West was relying on its KLA puppets to rubber-stamp an agreement which would have transformed Kosovo into an occupied territory under Western Administration.

Ironically Robert Gelbard, America's special envoy to Bosnia, had described the KLA last year as «terrorists». Christopher Hill, America's chief negotiator and architect of the Rambouillet agreement, «has also been a strong critic of the KLA for its alleged dealings in drugs.»[3] Moreover, barely a few two months before Rambouillet, the US State Department had acknowledged (based on reports from the US Observer Mission) the role of the KLA in terrorising and uprooting ethnic Albanians:

« ... the KLA harass or kidnap anyone who comes to the police, ... KLA representatives had threatened to kill villagers and burn their homes if they did not join the KLA [a process which has continued since the NATO bombings]... [T]he KLA harassment has reached such intensity that residents of six villages in the Stimlje region are «ready to flee.»[4]

While backing a «freedom movement» with links to the drug trade, the West seems also intent in bypassing the civilian Kosovo Democratic League and its leader Ibrahim Rugova who has called for an end to the bombings and expressed his desire to negotiate a peaceful settlement with the Yugoslav authorities.[5] It is worth recalling that a few days before his March 31 Press Conference, Rugova had been reported by the KLA (alongside three other leaders including Fehmi Agani) to have been killed by the Serbs.

Covert financing of «freedom fighters»

Remember Oliver North and the Contras? The pattern in Kosovo is similar to other CIA covert operations in Central America, Haiti and Afghanistan where «freedom fighters» were financed through the laundering of drug money. Since the onslaught of the Cold War, Western intelligence agencies have developed a complex relationship to the illegal narcotics trade. In case after case, drug money laundered in the international banking system has financed covert operations.

According to author Alfred McCoy, the pattern of covert financing was established in the Indochina war. In the 1960s, the Meo army in Laos was funded by the narcotics trade as part of Washington's military strategy against the combined forces of the neutralist government of Prince Souvanna Phouma and the Pathet Lao.[6]

The pattern of drug politics set in Indochina has since been replicated in Central America and the Caribbean. «The rising curve of cocaine imports to the US», wrote journalist John Dinges «followed almost exactly the flow of US arms and military advisers to Central America».[7]

The military in Guatemala and Haiti, to which the CIA provided covert support, were known to be involved in the trade of narcotics into Southern Florida. And as revealed in the Iran-Contra and Bank of Commerce and Credit International (BCCI) scandals, there was strong evidence that covert operations were funded through the laundering of drug money. «Dirty money» recycled through the banking system—often through an anonymous shell company— became «covert money,» used to finance various rebel groups and guerrilla movements including the Nicaraguan Contras and the Afghan Mujahadeen. According to a 1991 Time magazine report:

«Because the US wanted to supply the mujehadeen rebels in Afghanistan with stinger missiles and other military hardware it needed the full cooperation of Pakistan. By the mid-1980s, the CIA operation in Islamabad was one of the largest US intelligence stations in the World. 'If BCCI is such an embarrassment to the US that forthright investigations are not being pursued it has a lot to do with the blind eye the US turned to the heroin trafficking in Pakistan', said a US intelligence officer.[8]

America and Germany join hands

Since the early 1990s, Bonn and Washington have joined hands in establishing their respective spheres of influence in the Balkans. Their intelligence agencies have also collaborated. According to intelligence analyst John Whitley, covert support to the Kosovo rebel army was established as a joint endeavour between the CIA and Germany's Bundes Nachrichten Dienst (BND) (which previously played a key role in installing a right-wing nationalist government under Franjo Tudjman in Croatia).[9] The task to create and finance the KLA was initially given to Germany: «They used German uniforms, East German weapons and were financed, in part, with drug money».[10] According to Whitley, the CIA was subsequently instrumental in training and equipping the KLA in Albania.[11]

The covert activities of Germany's BND were consistent with Bonn's intent to expand its «Lebensraum» into the Balkans. Prior to the onset of the civil war in Bosnia, Germany and its Foreign Minister Hans Dietrich Genscher had actively supported secession; it had «forced the pace of international diplomacy» and pressured its Western allies to recognize Slovenia and Croatia. According to the Geopolitical Drug Watch, both Germany and the US favoured (although not officially) the formation of a «Greater Albania« encompassing Albania, Kosovo and parts of Macedonia.[12] According to Sean Gervasi, Germany was seeking a free hand among its allies «to pursue economic dominance in the whole of Mitteleuropa.»[13]

Islamic fundamentalism in support of the KLA

Bonn and Washington's «hidden agenda» consisted in triggering nationalist liberation movements in Bosnia and Kosovo with the ultimate purpose of destabilising Yugoslavia. The latter objective was also carried out «by turning a blind eye» to the influx of mercenaries and financial support from Islamic fundamentalist organisations.[14]

Mercenaries financed by Saudi Arabia and Kuwait had been fighting in Bosnia.[15] And the Bosnian pattern was replicated in Kosovo: Mujahadeen mercenaries from various Islamic countries are reported to be fighting alongside the KLA in Kosovo. German, Turkish and Afghan instructors were reported to be training the KLA in guerrilla and diversion tactics.[16]

According to a Deutsche Press-Agentur report, financial support from Islamic countries to the KLA had been channelled through the former Albanian chief of the National Information Service (NIS), Bashkim Gazidede.[17] «Gazidede, reportedly a devout Moslem who fled Albania in March of last year [1997], is presently [1998] being investigated for his contacts with Islamic terrorist organizations.»[18]

The supply route for arming KLA «freedom fighters» are the rugged mountainous borders of Albania with Kosovo and Macedonia. Albania is also a key point of transit of the Balkans drug route which supplies Western Europe with grade four heroin. Seventy-five percent of the heroin entering Western Europe is from Turkey. And a large part of drug shipments originating in Turkey transits through the Balkans. According to the US Drug Enforcement Administration (DEA), «it is estimated that 4-6 metric tons of heroin leave each month from Turkey having [through the Balkans] as destination Western Europe.»[19] A recent intelligence report by Germany's Federal Criminal Agency suggests that: «Eth nic Albanians are now the most prominent group in the distribution of heroin in Western consumer countries.»[20]

The laundering of dirty money

In order to thrive, the criminal syndicates involved in the Balkans narcotics trade need friends in high places. Smuggling rings with alleged links to the Turkish State are said to control the trafficking of heroin through the Balkans «cooperating closely with other groups with which they have political or religious ties» including criminal groups in Albanian and Kosovo.[21] In this new global financial environment, powerful undercover political lobbies connected to organized crime cultivate links to prominent political figures and officials of the military and intelligence establishment.

The narcotics trade nonetheless uses respectable banks to launder large amounts of dirty money. While comfortably removed from the smuggling operations per se, powerful banking interests in Turkey but mainly those in financial centres in Western Europe discretely collect fat commissions in a multibillion dollar money laundering operation. These interests have high stakes in ensuring a safe passage of drug shipments into Western European markets.

The Albanian connection

Arms smuggling from Albania into Kosovo and Macedonia started at the beginning of 1992, when the Democratic Party came to power, headed by President Sali Berisha. An expansive underground economy and cross border trade had unfolded. A triangular trade in oil, arms and narcotics had developed largely as a result of the embargo imposed by the international community on Serbia and Montenegro and the blockade enforced by Greece against Macedonia.

Industry and agriculture in Kosovo were spearheaded into bankruptcy following the IMF's lethal «economic medicine» imposed on Belgrade in 1990. The embargo was imposed on Yugoslavia. Ethnic Albanians and Serbs were driven into abysmal poverty. Economic collapse created an environment which fostered the progress of illicit trade. In Kosovo, the rate of unemployment increased to a staggering 70 percent (according to Western sources).

Poverty and economic collapse served to exacerbate simmering ethnic tensions. Thousands of unemployed youths «barely out of their teens» from an impoverished population, were drafted into the ranks of the KLA ...[22]

In neighbouring Albania, the free market reforms adopted since 1992 had created conditions which favoured the criminalisation of state institutions. Drug money was also laundered in the Albanian pyramids (ponzi schemes) which mushroomed during the government of former President Sali Berisha (1992-1997).[23] These shady investment funds were an integral part of the economic reforms inflicted by Western creditors on Albania.

Drug barons in Kosovo, Albania and Macedonia (with links to the Italian Mafia) had become the new economic elites, often associated with Western business interests. In turn the financial proceeds of the trade in drugs and arms were recycled towards other illicit activities (and vice versa) including a vast prostitution racket between Albania and Italy. Albanian criminal groups operating in Milan, «have become so powerful running prostitution rackets that they have even taken over the Calabrians in strength and influence.»[24]

The application of «strong economic medicine» under the guidance of the Washington based Bretton Woods institutions had contributed to wrecking Albania's banking system and precipitating the collapse of the Albanian economy. The resulting chaos enabled American and European transnationals to carefully position themselves. Several Western oil companies including Occidental, Shell and British Petroleum had their eyes riveted on Albania's abundant and unexplored oil-deposits. Western investors were also gawking Albania's extensive reserves of chrome, copper, gold, nickel and platinum.... The Adenauer Foundation had been lobbying in the background on behalf of German mining interests.[25]

Berisha's Minister of Defence Safet Zoulali (alleged to have been involved in the illegal oil and narcotics trade) was the architect of the agreement with Germany's Preussag (handing over control over Albania's chrome mines against the competing bid of the US led consortium of Macalloy Inc. in association with Rio Tinto Zimbabwe (RTZ).[26]

Large amounts of narco-dollars had also been recycled into the privatisation programmes leading to the acquisition of state assets by the mafias. In Albania, the privatisation programme had led virtually overnight to the development of a property owning class firmly committed to the «free market». In Northern Albania, this class was associated with the Guegue «families» linked to the Democratic Party.

Controlled by the Democratic Party under the presidency of Sali Berisha (1992-97), Albania's largest financial «pyramid» VEFA Holdings had been set up by the Guegue «families» of Northern Albania with the support of Western banking interests. VEFA was under investigation in Italy in 1997 for its ties to the Mafia which allegedly used VEFA to launder large amounts of dirty money.[27]

According to one press report (based on intelligence sources), senior members of the Albanian government during the presidency of Sali Berisha including cabinet members and members of the secret police SHIK were alleged to be involved in drugs trafficking and illegal arms trading into Kosovo:

(...) The allegations are very serious. Drugs, arms, contraband cigarettes all are believed to have been handled by a company run openly by Albania's ruling Democratic Party, Shqiponja (...). In the course of 1996 Defence Minister, Safet Zhulali [was alleged] to had used his office to facilitate the transport of arms, oil and contraband cigarettes. (...) Drugs barons from Kosovo (...) operate in Albania with impunity, and much of the transportation of heroin and other drugs across Albania, from Macedonia and Greece en route to Italy, is believed to be organised by Shik, the state security police (...). Intelligence agents are convinced the chain of command in the rackets goes all the way to the top and have had no hesitation in naming ministers in their reports.[28]

The trade in narcotics and weapons was allowed to prosper despite the presence since 1993 of a large contingent of American troops at the Albanian-Macedonian border with a mandate to enforce the embargo. The West had turned a blind eye. The revenues from oil and narcotics were used to finance the purchase of arms (often in terms of direct barter): «Deliveries of oil to Macedonia (skirting the Greek embargo [in 1993-4] can be used to cover heroin, as do deliveries of kalachnikov rifles to Albanian 'brothers' in Kosovo».[29]

The Northern tribal clans or «fares» had also developed links with Italy's crime syndicates.[30] In turn, the latter played a key role in smuggling arms across the Adriatic into the Albanian ports of Dures and Valona. At the outset in 1992, the weapons channelled into Kosovo were largely small arms including Kalashnikov AK-47 rifles, RPK and PPK machine-guns, 12.7 calibre heavy machine-guns, etc.

The proceeds of the narcotics trade has enabled the KLA to rapidly develop a force of some 30,000 men. More recently, the KLA has acquired more sophisticated weaponry including anti-aircraft and anti-armor rockets. According to Belgrade, some of the funds have come directly from the CIA «funnelled through a so-called 'Government of Kosovo' based in Geneva, Switzerland. Its Washington office employs the public-relations firm of Ruder Finn—notorious for its slanders of the Belgrade government».[31]

The KLA has also acquired electronic surveillance equipment which enables it to receive NATO satellite information concerning the movement of the Yugoslav Army. The KLA training camp in Albania is said to «concentrate on heavy weapons training—rocket propelled grenades, medium caliber cannons, tanks and transporter use, as well as on communications, and command and control». (According to Yugoslav government sources).[32]

These extensive deliveries of weapons to the Kosovo rebel army were consistent with Western geopolitical objectives. Not surprisingly, there has been a «deafening silence» of the international media regarding the Kosovo arms-drugs trade. In the words of a 1994 Report of the Geopolitical Drug Watch: «the trafficking [of drugs and arms] is basically being judged on its geostrategic implications (...) In Kosovo, drugs and weapons trafficking is fuelling geopolitical hopes and fears»...[33]

The fate of Kosovo had already been carefully laid out prior to the signing of the 1995

Dayton agreement. NATO had entered an unwholesome «marriage of convenience» with the mafia. «Freedom fighters» were put in place, the narcotics trade enabled Washington and Bonn to «finance the Kosovo conflict» with the ultimate objective of destabilising the Belgrade government and fully recolonising the Balkans. The destruction of an entire country is the outcome. Western governments which participated in the NATO operation bear a heavy burden of responsibility in the deaths of civilians, the impoverishment of both the ethnic Albanian and Serbian populations and the plight of those who were brutally uprooted from towns and villages in Kosovo as a result of the bombings.

Notes:

1. Roger Boyes and Eske Wright, Drugs Money Linked to the Kosovo Rebels, The Times, London, Monday, March 24, 1999.
2. Ibid.
3. Philip Smucker and Tim Butcher, «Shifting stance over KLA has betrayed' Albanians», Daily Telegraph, London, 6 April 1999
4. KDOM Daily Report, released by the Bureau of European and Canadian Affairs, Office of South Central European Affairs, U.S. Department of State, Washington, DC, December 21, 1998; Compiled by EUR/SCE (202-647-4850) from daily reports of the US element of the Kosovo Diplomatic Observer Mission, December 21, 1998.
5. «Rugova, sous protection serbe appelle a l'arret des raides», Le Devoir, Montreal, 1 April 1999.
6. See Alfred W. McCoy, The Politics of Heroin in Southeast Asia, Harper and Row, New York, 1972.
7. See John Dinges, Our Man in Panama, The Shrewd Rise and Brutal Fall of Manuel Noriega, Times Books, New York, 1991.
8. «The Dirtiest Bank of All,» Time, July 29, 1991, p. 22.
9. Truth in Media, Phoenix, 2 April, 1999; see also Michel Collon, Poker Menteur, editions EPO, Brussels, 1997.
10. Quoted in Truth in Media, Phoenix, 2 April, 1999).
11. Ibid.
12. Geopolitical Drug Watch, No 32, June 1994, p. 4
13. Sean Gervasi, «Germany, US and the Yugoslav Crisis», Covert Action Quarterly, No. 43, Winter 1992-93).
14. See Daily Telegraph, 29 December 1993.
15. For further details see Michel Collon, Poker Menteur, editions EPO, Brussels, 1997, p. 288.
16. Truth in Media, Kosovo in Crisis, Phoenix, 2 April 1999.
17. Deutsche Presse-Agentur, March 13, 1998.
18. Ibid.
19. Daily News, Ankara, 5 March 1997.
20. Quoted in Boyes and Wright, op cit.
21. ANA, Athens, 28 January 1997, see also Turkish Daily News, 29 January 1997.
22. Brian Murphy, KLA Volunteers Lack Experience, The Associated Press, 5 April 1999.
23. See Geopolitical Drug Watch, No. 35, 1994, p. 3, see also Barry James, in Balkans, Arms for Drugs, The International Herald Tribune, Paris, June 6, 1994.
24. The Guardian, 25 March 1997.
25. For further details see Michel Chossudovsky, La crisi albanese, Edizioni Gruppo Abele, Torino, 1998.
26. Ibid.
27. Andrew Gumbel, The Gangster Regime We Fund, The Independent, February 14, 1997, p. 15.
28. Ibid.
29. Geopolitical Drug Watch, No. 35, 1994, p. 3.
30. Geopolitical Drug Watch, No 66, p. 4.
31. Quoted in Workers' World, May 7, 1998.
32. See Government of Yugoslavia at http://www.gov.yu/terrorism/terrorist-camps.html.
33. Geopolitical Drug Watch, No 32, June 1994, p. 4.

P.A.S.S. DEFENCE

COMPANY PROFILE

P.A.S.S. DEFENCE is a 100% Hellenic company, certified according to the standards of ISO 9001:2000, exclusive representative in Greece of more than thirty (30) Defence Manufacturing companies of security and NBC materials. The staff of **P.A.S.S DEFENCE** is fully trained to provide accurate training about the operation, application and support of their products.

Having long term experience on the qualitative design and support of products and services, P.A.S.S. DEFENCE offers to the Hellenic Armed Forces, Police, Security services, Athens 2004 Olympic Committee, Embassies and Private organizations the following:

- Defence systems
- Demining - Ammunition collection and disposal
- Consulting services concerning defence and security
- Security systems for persons and facilities
- Space control assuring secure communication
- NBC protection material
- Certified to provide training in protection of humans and facilities from asymmetric threats, in NBC protection and codification of materials according to NATO standards.
- Full after sales support
- Secure inner and international transportation of household effects and cargos

P.A.S.S. DEFENCE covers a wide range of provided technology and services by developing the human potential, the experience and the know how, we have received after the successful completion of more than 200 contracts. We offer integrated solutions, high technology services, research elaborations, material and system sales, certified training and full after sales support.

P.A.S.S. DEFENCE is now one of the most reliable companies in its field expanding in high speed. We own facilities, modern warehouses and two trucks.

MILITARY PROTECTION | CIVILIAN PROTECTION

http://www.defence.gr

Surviving terrorism

Source:http://www.latimes.com/news/opinion/commentary/la-oe-mcmanus-terrorism-20101226,0,29986 59.column

A year ago, on Christmas Day, a young Nigerian named Umar Farouk Abdulmutallab allegedly tried to blow up a passenger jet in midair as it was landing in Detroit, using a bomb hidden in his pants. As he fumbled with the detonator, other passengers realized something was amiss and wrestled him to a halt.

In the 12 months since, the U.S. government has fixed the most obvious problems the «underwear bomber» exposed. The State Department says it now checks routinely to see whether potential terrorists have U.S. visas. The Department of Homeland Security says it can now block suspects from boarding U.S.-bound planes more reliably. The National Counterterrorism Center, which was supposed to «connect the dots» of intelligence from various sources, says it has improved its ability to search government databases for information on potential threats.

And, of course, airline passengers are now subjected to full-body scans — or, if they choose, to old-fashioned pat-downs.

But some of the most vexing problems have not been fixed. At the National Counterterrorism Center, for example, there's still no single database that automatically merges information from the entire spectrum. Officials say the information systems of the CIA and FBI are still mostly incompatible, both technically (different computer languages) and legally (different rules on how information can be shared). As a result, analysts still sit in front of multiple computer screens, run their searches in different systems and, in effect, connect dots by hand.

Meanwhile, terrorists are still out there, still trying to find a gap in all those defenses. When a shoe bomb didn't work, they tried liquid explosives. When those were detected, they tried the underpants bomb. When air travel became difficult, they encouraged a disgruntled Pakistani American to load a station wagon with explosives and drive to Times Square. When passenger scrutiny increased, they shifted to sending packages. And when large-scale attacks became impractical, plans for small-scale attacks began to crop up.

One of these days, one of these plots is going to succeed. It's not unpatriotic or defeatist to say that; it's realistic.

And that's why one of the most intriguing concepts in counterterrorism today is called «resilience» — preparing for terrorist attacks and minimizing their impact when they happen.

Terrorists aim to damage their opponents partly by provoking reactions bigger than the original attack. Osama bin Laden spent less than half a million dollars on the Sept. 11, 2001, attacks in New York and Washington, but he caused billions in damage by prompting a shutdown of financial markets, air travel and other chunks of the U.S. economy — not to mention the war in Afghanistan and the other counterterrorist campaigns that ensued.

But if a society is prepared for terrorist attacks, makes sure its citizens know how to react when they happen, and protects its transportation, communications and utilities networks from being paralyzed by local disruptions, the impact of terrorism is reduced. It's still a problem, but it's no longer an existential threat.

«As a practical matter we should be far better prepared for these events and make them far less disastrous,» says Stephen E. Flynn, a former Coast Guard counterterrorism expert who now runs a think tank called the Center for National Policy.

We can't control everything, Flynn notes, but «we are in control of how we react.»

The federal government has spent a lot of time and money working on ways to protect infrastructure. And it has encouraged local governments to improve their emergency planning.

But there hasn't been much focus on public education since the days when Tom Ridge, the first secretary of Homeland Security, encouraged people to seal rooms with duct tape as protection against chemical weapons.

The Federal Emergency Management Agency has a website called Ready.gov that explains what to do in case of various emergencies, agency's publicity budget is small; it relies mostly on donated advertising time to get the word out. Homeland Security sponsored National Preparedness Month in September, but I'll bet most of us didn't notice.

Here's an example of how public education can work:

In case of most terrorist bombs, experts say, the best thing to do is to seek shelter inside a building — whether the bomb is conventional, chemical, radiological or (in the least likely scenario) nuclear. If the bomb is inside your building, get out; but if it's somewhere else, take shelter.

The greatest danger from most of those bombs may be from secondary explosions, airborne contaminants or radiation. Jumping into your car to flee merely exposes you to more risks, and when thousands of people try to evacuate, they choke the roads, cause traffic accidents and impede emergency responders.

But not everybody knows that. A 2007 survey found that in the event of a «dirty bomb,» a conventional explosion that spreads radioactive material, 65% of people said their first impulse would be to flee. Flynn talked last year with New York City firefighters and said some of them didnt know whether they should tell people to evacuate or seek shelter in the event of an explosion. («The policy of the department is clear, and that's shelter in place,» responded Joseph W. Pfeifer, New York's assistant fire chief for counterterrorism. «We've trained everyone on that.... The real challenge is educating the public.»)

«Nobody ever told the emergency responders what to do,» he said.

In the case of a nuclear explosion, a study by Stanford professor Lawrence Wein estimated that a small nuclear device in Washington, D.C., could kill 120,000 people if most people sought shelter in buildings — but 180,000 if most people tried to evacuate.

Brooke Buddemeier of Lawrence Livermore recently estimated that an explosion in Los Angeles could cause 285,000 deaths or injuries from fallout among people a mile or more away from the blast if they took no shelter, but only a small fraction of that number if they found shelter in brick or concrete buildings. Even a wood-frame house would provide some protection.

Flynn offers three ideas for reducing deaths and injuries in an attack: First, make sure everyone knows that if a bomb goes off, the first thing to do is seek shelter — preferably underground. Next, teach airline passengers to recognize bombs and detonators, so the next Umar Farouk Abdulmutallab doesn't have a better chance of success. And third, develop national standards for emergency planning that communities would have to meet — or see their insurance rates go up.

The Obama administration, to its credit, has focused on resilience as a major goal of its homeland security policy. And some officials have been blunt in warning that an attack is likely to succeed some day. «We must be honest with ourselves,» Obama's top advisor on terrorism, John O. Brennan, said this year.

Still, in practice, the administration hasn't talked about much about preparedness. «There's a concern about sounding as if you're no longer focused on preventing attacks from happening,» one official acknowledged.

But Californians know what to do in an earthquake. Kansans know what to do in a tornado. Floridians know what to do in a hurricane.

Everybody ought to know what to do in the event of an attack — of any kind.

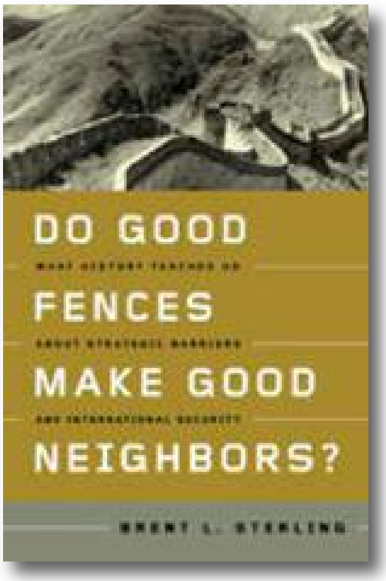
We're tougher than we look. We can take it.

Do Good Fences Make Good Neighbours?

What History Teaches Us About Strategic Barriers and International Security

By Brent L. Sterling
Washington, DC: Georgetown University Press, 2009
Reviewed by Scott Savitz, senior analyst, HOMELAND SECURITY STUDIES AND ANALYSIS INSTITUTE
Source: http://www.homelandsecurity.org/journal/Default.aspx?t=348

The challenge of border security—a central element of homeland security—is among the most ancient concerns of humanity. Throughout recorded history, human beings have sought to regulate access to the territories under their authority, controlling (or preventing) movement across a demarcated boundary. In Do Good Fences Make Good Neighbors? Brent Sterling explores historical lessons regarding the use of strategic defenses for this purpose. He examines case studies of instances in which a nation, facing a menu of prospective choices for securing a frontier, chose to build a strategic barrier. He then examines the subsequent implementation of this decision and its impact. The subjects of Sterling's six case studies range widely over time and space: the Long Walls of ancient Athens, Hadrian's Wall in Britain, the Ming Dynasty's Great Wall of China, Louis XIV's defensive lines in northeastern France, the pre–World War II Maginot Line, and the Israelis' Bar-Lev line along the Suez Canal. The author recognizes from the outset that these six cases involved very distinct structures, including both continuous barriers and discrete, mutually supporting fortifications. He also notes that they were built in response to diverse, situationally specific threats. While Sterling demonstrates similarities among the case studies, he does not attempt to force them.



Sterling explicitly resists answering what he considers to be an overly simplistic question: whether particular strategic defenses worked. Each barrier described gave its builders a greater ability to resist incursions, though none was inviolable (nor should we expect it to have been). Even intermittent barriers, or those that covered only part of a frontier, aided considerably in defense; the oft-derided Maginot Line forced the Germans to bypass it via the challenging terrain of the Ardennes forest. However, most of these barriers also had more complex, indirect consequences for security. In each case, the existence of barriers contributed to complacency on the part of those who had built them, fostering underinvestment in personnel and maintenance (subtly degrading the barriers' effectiveness over time), while reducing emphasis on the mobile defenses that were intended to complement the barriers. It also diminished the defenders' interest in addressing the tensions that had led to the barriers' construction. Citizens or allies who lived beyond the barriers were usually piqued by a sense of abandonment, which had political consequences (particularly in democracies) and led to diplomatic isolation. Moreover, when barriers were tested by an adversary and found to be wanting, the psychological and political consequences for the builders were often severe. One of the book's striking findings is that in nearly every case, the builders misjudged their adversaries' reactions to the barrier. Adversaries often viewed the construction of a strategic barrier as an act of aggression, enabling the builder to aggrandize itself with a diminished fear of retribution. In instances where adversaries had economic or traditional ties that spanned the boundary, they were particularly aggrieved by the barrier's symbolic permanence. Having been co doned off but still retaining the initiative, these adversaries sought to bypass or otherwise defeat the barriers, sometimes successfully. As Sterling points out, the success of barriers depends on the numerical strength, courage, and incorruptibility of those who guard them. Sterling's analysis is consistently thorough and thought provoking. He devotes ample time to each case study, providing a balanced review of the political, economic, diplomatic, military, cultural, and other factors that influenced the decision to build strategic defenses. There is considerable discussion of states' decisions on where to locate these barriers, as well as the extent to which states subsequently invested in ensuring adequate maintenance and personnel. The political effects of barriers on both the builders and their adversaries are neatly captured, as are the barriers' performance when challenged and subsequent reactions. This book is written for a general audience, though individuals pursuing further research will find sources in its ample endnotes. The text is also peppered with apposite, insightful quotes by authors ranging from Plato to Edward Luttwak. In his introduction and conclusion, Sterling explicitly connects the results of his findings to the debates about U.S. and Israeli efforts to secure borders using a combination of barriers, personnel, and detection technologies. While it may be argued that the barriers described in the case studies were not aimed at countering threats like those facing the United States and Israel today (notably terrorism, smuggling, and illegal migration), several of the barriers were aimed at preventing small-scale incursions in which adversaries sought to inflict harm, acquire goods, or reside on the other side for some time. Sterling also briefly suggests that his analysis could be applied to missile and air defense, but the qualitative differences between barrier defenses and interceptor weapons would seem to preclude its straightforward application. However, this analysis might apply to numerous other conflicts in which insurgents freely cross international frontiers and in which barriers to impede movement could conceivably play a role. Sterling wisely refrains from making explicit policy recommendations for U.S., Israeli, or other nations' border defense. However, his work provides considerable food for thought as policymakers attempt to grapple anew with the ancient challenge of border security

Jihad and Terrorism

Author: Anita Rai

Source: http://www.anitarai.com/jihad-and-terrorism.htm

Anita Rai's 6th book, **JIHAD AND TERRORISM** is soon coming out. As with every of her other book, this one too stands out in a sea of run of the mill publications on the same subjects. Rai says: "The spirit of Islam is promotion of peace, love and enlightenment and justice for all. *Justice* is the guiding force of Islam. And its very spirit requires Islam to defend the oppressed and establish the rule of justice in order to facilitate the superior functioning of the law of God for the optimum welfare of His creatures, basically and spiritually – this calls for ***Jihad***, which means striving hard and honest, in the Way of God. **Jihad**, as preached and practiced by Muhammad, the Messenger of Peace (pbuh) is not necessarily same and similar to its understanding by the Muslims and the non-Muslims down the centuries. Hence, the **history of Jihad** – its phases, periods, politics and ploys – is very complex, which is not easy to grasp if one does not have the sophistication and

depth of knowledge of the very complex and turbulent history of Islam. The why - when - how of **jihad** transgressing into **terrorism** is essential because almost always it is mentioned in the same breath as **terrorism** and even described as an equivalent. **JIHAD AND TERRORISM** is about portraying the **Essential Jihad** – illustrated by the **Custodians of Islam** (p b u them) and the Holy Book – which is averse to terrorism and wages a constant **War on terror**. So, although we find the **history of jihad** and the **history of terrorism** entangled, **jihad** and **terrorism** stand for distinctly separate and profoundly different values."

Anita Rai was born in 1975 in a metropolis of India. Although she now resides in UK, she is still very attached to her roots, culture, aesthetics, and literature. She has done her BA from India, with Honours in English Literature and Language. After coming to the UK, Anita has done her MBA with specialisation in Marketing.

Napolitano says Israeli-style security is not suitable for U.S.

Source: http://homelandsecuritynewswire.com/napolitano-says-israeli-style-security-not-suitable-us

DHS secretary Janet Napolitano is in Israel on a visit; during her private briefing with Israeli officials at Ben-Gurion Airport, they discussed cargo screening and how to stop non-metallic explosives, such as those used in the recent plots, from getting onto a plane; Napolitano was also briefed on other airport security measures used in Israel; Napolitano said, however, that what is effective in Israel, a nation of 7.3 million, would not necessarily work for 310 million Americans; Ben-Gurion is Israel's only major international airport; the United States has 450 such facilities; about eleven million people pass through Israeli airports each year, while seventy times that many passengers go through American airports each year. DHS secretary Janet Napolitano on Tuesday rebuffed suggestions that U.S. airports should adopt the practices of airports in Israel, calling the Israeli air travel system "a very different model." "We share a common goal, which is to protect the people of our countries from terror or other attacks," Napolitano told Fox News ahead of a tour of security facilities at Tel Aviv's Ben-Gurion International Airport. "But there are many differences in the United States system versus Israel. Part of that is driven by sheer size." Fox News reports that critics of U.S. security methods, particularly full body scans and the so-called "invasive pat down" used by the Transportation Security Administration (TSA), have called for American airports to adopt Israeli-style security measures, which rely heavily on behavioral profiling of travelers. Napolitano said, however, that what is effective in Israel, a nation of 7.3 million, would not necessarily work for 310 million Americans. Ben-Gurion is Israel's only major international airport. The United States, however, has 450 such facilities. Plus, about eleven million people pass through Israeli airports each year, while seventy times that many passengers go through American airports each year. "So there's a very big difference in terms of size and scale," said Napolitano, who granted Fox News exclusive access to join her on a week-long, security-focused trip to Europe and the Middle East. Early Tuesday, the head of security at Ben-Gurion gave Napolitano a tour of his airport's system and a "comprehensive briefing" on Israeli airport security that "covered the spectrum from intelligence to the perimeter security of the airport to checkpoint screening and everything in between," according to a

Homeland Security official. Ben-Gurion has formidable security measures apparent even to an outsider. Snipers stand watch from a glass-encased booth suspended above the airport's main entrance, visible from a traveler's first steps into the airport. In the run-up to the Thanksgiving holiday, the Transportation Security Administration began to come under fire for its enhanced security measures at. In the midst of the firestorm, Representative John Mica (R-Florida), and others called for TSA to adopt Israel's style of screening. Napolitano and TSA chief John Pistole have said repeatedly that the new procedures at U.S. airports are so far the best way to keep ahead of the "evolving threat." A department statement issued late Tuesday noted that the TSA uses a "layered security approach," including the deployment of behavior detection officers, air marshals and explosives detection canine teams. Overseas terrorists have repeatedly targeted U.S.-bound flights. On Christmas Day 2009, Umar Abdulmutallab of Nigeria tried to detonate his explosives-laden underwear over Detroit. In October, two packages containing explosives were sent from Yemen to the United States, but they were intercepted overseas after Saudi intelligence officials shared information about the plot. Both attempts have been tied to Yemen-based al Qaeda in the Arabian Peninsula. "We know that there've been terrorist attacks that have emanated from this area of the world for years," Napolitano said, speaking of the Mideast and Persian Gulf regions. So, she said, her discussions with Israeli officials would focus on "what partnerships we have, what information we're sharing, what kind of best practices we can share in terms of protecting security and safety." During Napolitano's private briefing with Israeli officials at Ben-Gurion, they discussed cargo screening and how to stop non-metallic explosives, such as those used in the recent plots, from getting onto a plane, a Homeland Security official said. Despite repeated attempts to speak with an Israeli official about using their security model in the United States, the Israeli government declined to talk with Fox News, citing an aversion to discussing their security measures publicly.

EDITOR'S NOTE: Being recently in Israel I had the chance to participate in an "inside security tour" at Ben Gurion International Airport and watch a security exercise where unmanned patrol vehicles were deployed (see Winter 2010 issue). Although it is true that "numbers" and "quantities" are different between these two countries and having travelled through almost all major international airports worldwide, I will totally disagree with Mrs Napolitano. The Israeli airport security system should be the "model" for airports around the world. An attack against an airport should take place in the area before check-in not in the waiting lounges, not in the airfield or the inner infrastructure facilities. Although such a change might cost al lot of money it should be seriously considered for all new airports. For example it could be done at new Terminal 5 at Heathrow Airport in London.

How the Israelis do airport security

Source: http://www.cnn.com/2010/OPINION/01/11/yeffet.air.security.israel/

In the wake of the failed Christmas Day bombing of Northwest Flight 253, authorities are ramping up air passenger screening, particularly for those flying from 14 nations that the U.S. describes as «state sponsors of terrorism or other countries of interest.» Hundreds more full body scanning machines are on order for U.S. airports. But some airline security experts say the real answer to greater security is to follow the approach used by Israel's airline, El Al. Isaac Yeffet, the former head of security for El Al and now an aviation security consultant in New York, said El Al has prevented terrorism in the air by making sure every passenger is interviewed by a well-trained agent before check-in. «Stop relying only on technology,» Yeffet told CNN. «Technology can help the qualified, well-trained human being but cannot replace him.»

Yeffet spoke to CNN:

CNN: What do you think we've learned about airport security from the failed bombing in Detroit?

Isaac Yeffet: We learned one thing. We do not have a good security system to be able to prevent tragedies in this country. After Lockerbie, everyone thought, now we've learned the lesson of how to be proactive instead of being reactive. Unfortunately, September 11 came and we know the result. Thousands of people lost their lives. Security totally failed, not at one airport, at three different airports around the country. In 2002, we had Richard Reid, the shoe bomber. This man gave the security people all the suspicious signs that any passenger could show. The man got a British passport in Belgium, not in England. Number Two: he flew to Paris, he bought a one-way ticket from Paris to Florida. He paid cash. He came to the airport with no luggage. What else do I need to know that this passenger is suspicious? What did we learn from this? Just to tell the passenger from now on, you take off your shoes when you come to the airport? This I call a patch on top of a patch. Now we face the story with [Umar Farouk] AbdulMutallab. We had all the information that we could dream the security people could get. He was on the list of people connected to al Qaeda. I don't need more to understand that when he comes, I am not looking for more evidence. He is suspicious; I have to take care of him. His father called the U.S. Embassy a month before he took the flight and told the U.S. Embassy that his son had called and said this was the last time you were going to hear from me. And the father warned the U.S. Embassy that his son was going to do something bad, watch him. What happened to this information? The guy bought a ticket and paid $3,000 cash. ... No one knew the information that we had about him, no one could interview him and to ask him why is he flying to America.

STORY HIGHLIGHTS

- U.S. authorities have stepped up airport screening after failed Christmas Day attack
- Consultant Isaac Yeffet says Israel safeguards planes by interviewing all passengers
- He says well-trained agents can detect attackers and prevent incidents
- Yeffet: Security people need to be constantly tested — and fired if they fail

CNN: What needs to be done to improve the system?

Yeffet: It's mandatory that every passenger — I don't care his religion or whatever he is — every passenger has to be interviewed by security people who are qualified and well-trained, and are being tested all year long. I trained my guys and educated them, that every flight, for them, is the first flight. That every passenger is the first passenger. The fact that you had [safe flights] yesterday and last month means nothing. We are looking for the one who is coming to blow up our aircraft. If you do not look at each passenger, something is wrong with your system. Every passenger has to be interviewed by security people who are qualified and well-trained.

CNN: What is El Al's approach to airline security? How does it differ from what's being done in this country?

Yeffett: We must look at the qualifications of the candidate for security jobs. He must be educated. He must speak two languages. He must be trained for a long time, in classrooms. He must receive on-the-job training with a supervisor for weeks to make sure that the guy understands how to approach a passenger, how to convince him to cooperate with him, because the passenger is taking the flight and we are on the ground. The passengers have to understand that the security is doing it for their benefit. We are constantly in touch with the Israeli intelligence to find out if there are any suspicious passengers among hundreds of passengers coming to take the flight — by getting the list of passengers for each flight and comparing it with the suspicious list that we have. If one of the passengers is on the list, then we are waiting for him, he will not surprise us. During the year, we did thousands of tests of our security guys around the world. It cost money, but once you save lives, it's worth all the money that the government gave us to have the right security system. I used to send a male or female that we trusted. We used to give them tickets and send them to an airport to take a flight to Tel Aviv. We concealed whatever we could in their luggage. Everything was fake, and we wanted to find out if the security people would stop this passenger or not. If there was any failure, the security people immediately were fired, and we called in all the security people to tell people why they failed, what happened step by step. I wanted everyone to learn from any failure. And if they were very successful, I wanted everyone to know why.

CNN: Let's say all the airlines instituted the system that you're talking about. So let's say I go to an airport for a flight to London. What should happen?
Yeffet: When you come to the check-in, normally you wait on line. While you wait on line, I want you to be with your luggage. You have to meet with me, the security guy. We tell you who we are. We ask for your passport, we ask for your ticket. We check your passport. We want to find which countries you visited. We start to ask questions, and based on your answers and the way you behave, we come to a conclusion about whether you are bona fide or not. That's what should happen.

CNN: Every passenger should be interviewed, on all flights?
Yeffet: Yes, 100 percent... I want to interview you. It won't take too long if you're bona fide. We never had a delay. Number two, I have heard so many times El Al is a small airline. We in America are big air carriers. Number one, we have over 400 airports around the country, why hasn't anyone from this government asked himself, let's take one airport out of 400 airports and try to implement El Al's system because their system proved they're the best of the best. For the last 40 years, El Al did not have a single tragedy. And they came to attack us and to blow up our aircraft, but we knew how to stop them on the ground. So let's try to implement the system at one airport in the country and then come to a conclusion...

CNN: What do you think of using full body scanners?
Yeffet: I am against it, this is once again patch on top of patch. Look what happened, Richard Reid, the shoebomber, hid the explosives in his shoes. The result — all of us have to take off our shoes when we come to the airport. The Nigerian guy hid his explosives in his underwear. The result — everyone now will be seen naked. Is this the security system that we want? We have millions of Muslims in this country. I am not Muslim, but I am very familiar with the tradition, I respect the tradition. Women who walk on the street cover their body from head to toe. Can you imagine the reaction of the husband? Excuse me, wait on the side, we want to see your wife's body naked?... This is not an answer. I appreciate what the president said, but we need to see the results on the ground at the airports. ... I strongly recommend that TSA call experts ... and not let them leave before they come to conclusions about what must be done at each airport to make sure that we are really pro-active. Let us be alert, let us work together, and show no mercy for any failure, no mercy. If we do this system, believe me we will show the world that we are the best proactive security system and the terrorists will understand that it's not worth it to come to attack us.

CNN: Would it be more expensive to provide the kind of security system you recommend?
Yeffet: For sure El Al spends more money on security than the American air carriers. But the passengers are willing to pay for it if we can prove to them that they are secure when they come to take a flight.

Airport screening: The new—and you

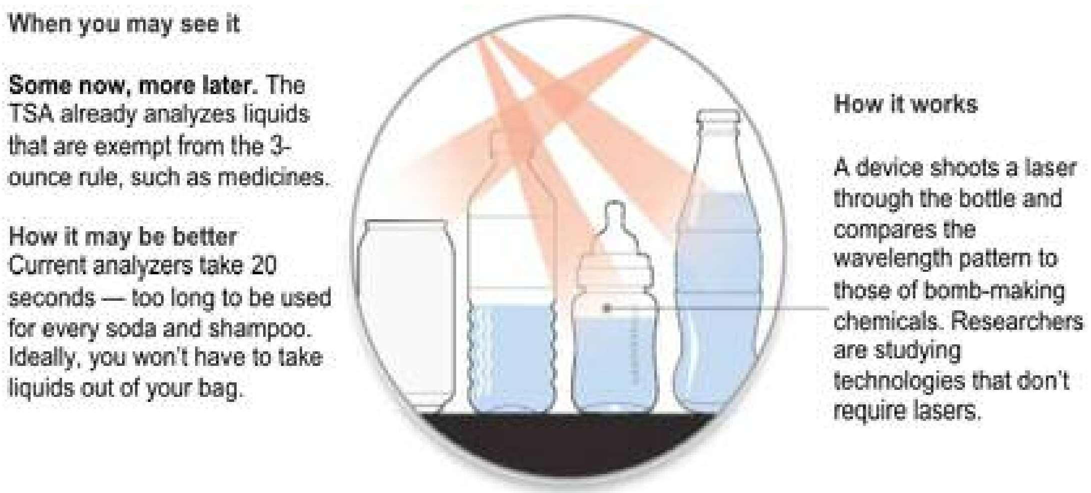
Source: http://www.washingtonpost.com/wp-srv/special/nation/future-airport-security/

Companies around the world are pouring research money and brainpower into making the slog through airport security into more of a stroll. Ideally, these innovations improve safety and convenience. But some technologies would require passengers to reveal more personal information than U.S. travelers are used to providing.

LIQUID ANALYZER

What it does

A scanner checks bottles without opening them, determining, for example, whether that pale liquid is a bomb ingredient or ginger ale.



When you may see it

Some now, more later. The TSA already analyzes liquids that are exempt from the 3-ounce rule, such as medicines.

How it may be better

Current analyzers take 20 seconds — too long to be used for every soda and shampoo. Ideally, you won't have to take liquids out of your bag.

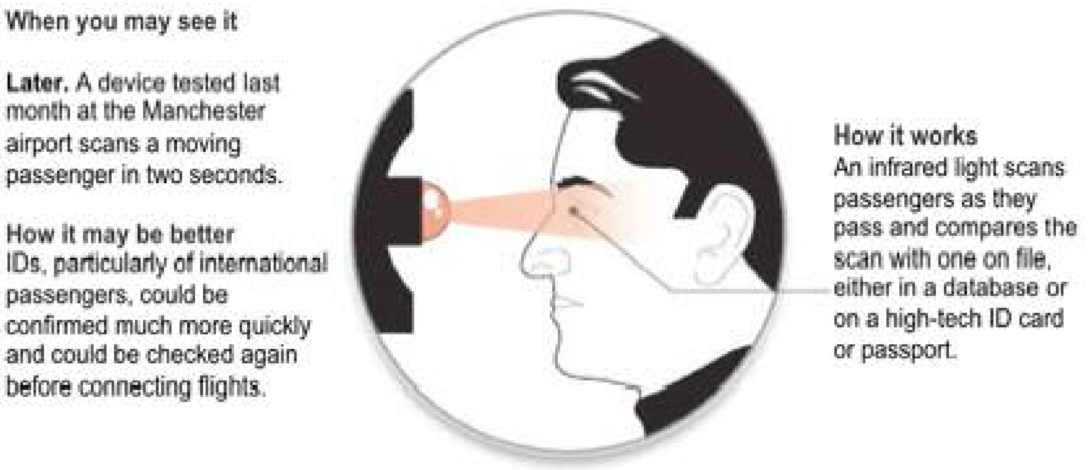
How it works

A device shoots a laser through the bottle and compares the wavelength pattern to those of bomb-making chemicals. Researchers are studying technologies that don't require lasers.

IRIS RECOGNITION

What it does

As a passenger walks past, a device scans the colored portion of the eye to confirm his or her identity.



When you may see it

Later. A device tested last month at the Manchester airport scans a moving passenger in two seconds.

How it may be better

IDs, particularly of international passengers, could be confirmed much more quickly and could be checked again before connecting flights.

How it works

An infrared light scans passengers as they pass and compares the scan with one on file, either in a database or on a high-tech ID card or passport.

‘BOMB SNIFFER’

What it does

This device detects traces of explosives like a bomb-sniffing dog would, only faster. It works in one second while the passenger is moving.

When you may see it

Later. No device has been deemed airport-ready yet, although one version tested well this fall in Glasgow.

How it may be better
You wouldn't have to take off your coat or shoes, as long as the device is used in conjunction with a metal detector.

How it works
The machine creates a slight breeze, and lasers analyze the airflow. The device then reads the chemical fingerprints of gases that are emitted by various substances. The laser beam doesn't actually touch the skin.

NOT-SO-NAKED PICTURES

What it does

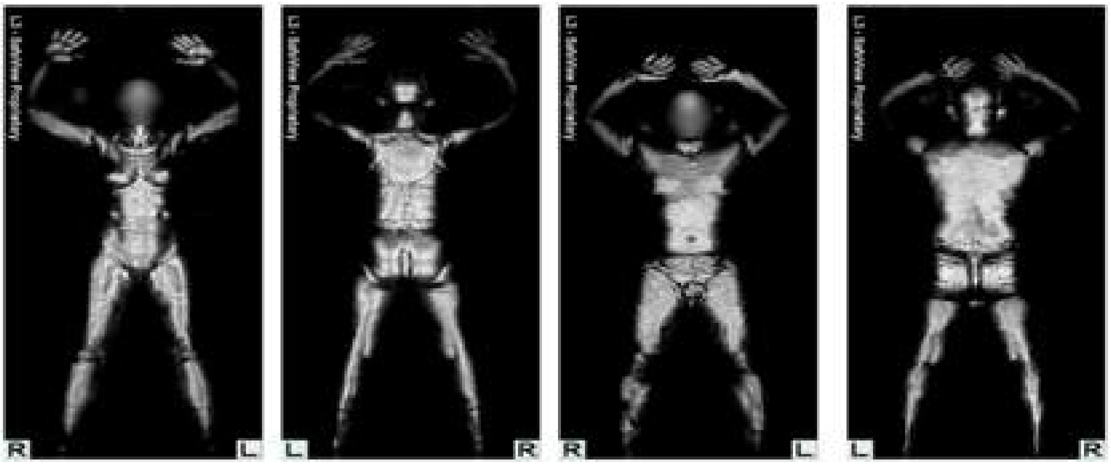
Full-body scanners display a generic image with any suspicious areas highlighted.

When you may see it

Now, but not here. Both makers of U.S. scanners have upgrades awaiting approval; L-3's version is in use in Amsterdam.

How it may be better
No "naked picture" or otherwise identifying image is ever created.

How it works
The scanning technology is the same, but the software interprets the data on a generic figure, so there's no need for a second screener in another room to view and assess the images.


L3 - SafeView Proprietary
R
L
L3 - SafeView Proprietary
L
R
L3 - SafeView Proprietary
R
L
L3 - SafeView Proprietary
L
R

FINGERPRINT READER

What it does

This high-tech version eliminates the ink and paper and matches prints to a database or to a biometric ID card in less than a second.

When you may see it

Now, but not here. South Korea began using a system in September in its ports and airports to ferret out forged papers.

How it may be better

Matching can take less than a second. It is usually used in conjunction with the iris scan to identify travelers reentering the country.

How it works

The version used in South Korea scans one finger at a time using a high-resolution optical scanner. The analysis algorithm runs on a regular computer.

SHOE SCANNER

What it does

The ideal scanner lets passengers keep their shoes on while it detects explosive traces and knives (without flagging metal shoe parts).

When you may see it

Later. Twelve companies are vying to provide shoe screeners to U.S. airports, but the TSA has not chosen yet.

How it may be better

You get to keep your shoes on, and so does the person wearing lace-up boots in front of you.

How it works

The device creates no image but displays a green light (good to go) or red light (check this person further). One tested this summer in Indianapolis took about 8-9 seconds per person.

BEHAVIORAL ASSESSMENT
What it does
Obscure code words or images linked to terrorist groups are projected around the airport while hidden sensors and cameras see who reacts.

When you may see it

Later. It has not been tested in airports yet. Other polygraph-like technologies are being studied as well.

How it may be better
The process would add no time to screening for most passengers. People who don't recognize the images likely wouldn't notice anything unusual.

How it works
The system, by WeCU (pronounced "We See You") Technologies, pairs human observers who watch for darting eyes and other overt behavior with sensors that detect physiological changes (faster breathing, etc.).

BIOMETRIC ID CARD
What it does
Passengers' ID cards contain fingerprints, iris scans, passport info, photos and other personal data—perhaps even a voice sample.

When you may see it

Now, but not here. A few countries use biometric IDs for other purposes; an Israeli airline is phasing in a passenger program.

How it may be better
Passengers could potentially clear many airport hurdles at once, including customs, immigration, check-in and security screening.

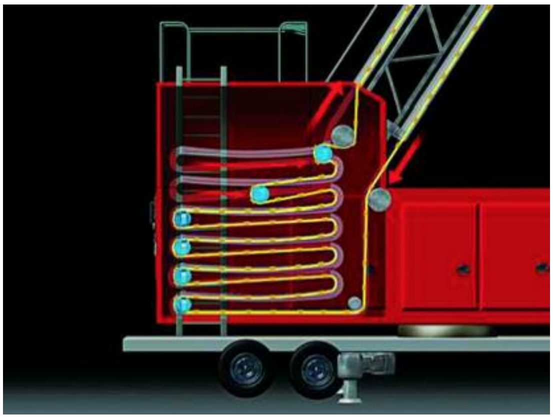
How it works
Screeners match live scans to the data on the card. Currently, cards from various countries may contain different types of data, and voice recognition is in the experimental stages.

SOURCES: Cascade Technologies, Human Recognition Systems, Smiths Detection, L-3 Communications, Rapiscan, Morpho Detection, TSA, Times of India, Globes Online, The Economist.

Escalator to replace fireman ladder

Source1: http://homelandsecuritynewswire.com/escalator-replace-fireman-ladder
Source2: http://www.popsci.com/technology/article/2010-12/invention-month-easy-way

Since the 1880s, firefighters have been climbing ladders to rescue victims trapped by fire inside burning building; a new hydraulic ladder would carry firefighters — the way a conveyer belt does — as high as 113 feet at twice the speed of a climbing man; fire victims would be loaded into bags attached to the ladder; it now take up to fifteen minutes, and sometimes several men, to carry one victim down a ladder from ten stories; the new ladder will allow one firefighter to carry two victims at half the time. Orville Douglas Denison spent much of his youth sketching out futuristic aircraft, but in retirement he has turned pragmatic. His "aerial fire truck," a cross between a conveyer belt and a ladder, could help firefighters quickly shuttle victims out of burning buildings. Popular Science reports that Denison began studying fire-rescue technology after watching TV coverage of the World Trade Center evacuations on 9/11. Eventually he turned his focus to the ladders often used for smaller buildings. Firemen began deploying telescoping ladders in the 1880s, and they have not changed significantly since. "It's ridiculous to climb up, put someone on your shoulders, and climb down," Denison says. There had to be a faster way, he thought. So he designed a moving ladder that could be retrofitted to trucks to reduce a firefighter's climbing time by more than half. In a rescue, firemen could extend Denison's hydraulic ladder to windows as high as 113 feet — but rather than clamber up the ladder, the firefighter would hop on, and the rungs would roll up at 200 feet per minute — more than twice the average climbing speed of a firefighter weighed down by 130 pounds of gear. The firefighter would ride to a window, load unconscious victims into a rescue bag, hook the bag to the ladder, and shift it into reverse to bring the person to safety. Denison says it can now take up to fifteen minutes, and sometimes several men, to carry one victim down a ladder from ten stories. He estimates that his ladder could lower four people to the ground in less than four minutes. Several firefighting experts praise Denison's innovative approach, while also nitpicking the design, suggesting that simpler is better for rescue technology. Denison, who has interest from some manufacturers, welcomes the critiques — he is intent on making his ladder a reality.



"To me," he says, "this is an obvious necessity and a solution to an age-old problem." As Denison's new hydraulic ladder extends, it draws additional rungs from inside the base unit. The rungs are on rollers that slide on tracks to feed the ladder. Each roller moves independently and is attached to a spring-loaded cable that keeps the line taut as the rungs run up and down the ladder at 200 feet per minute.

HHS Announces Resources for Hospital Preparedness Exercises

Source:http://www.hstoday.us/industry-news/general/single-article/hhs-announces-resources-for-hospital-preparedness-exercises/63d35215bee9fbbb469ac626c69bc5cd.html

The Department of Health and Human Services' (HHS) Agency for Healthcare Research and Quality (AHRQ) has released the Hospital Preparedness Exercises Atlas of Resources and Tools planner to give hospital emergency planners a structured compendium of available resources and tools that can help them plan for, design and develop, conduct, evaluate and improve hospital preparedness exercises. AHRQ is the lead federal agency charged with supporting research designed to improve the quality of health care, reduce its cost, address

Hospital Preparedness Pocket Guide
http://www.ahrq.gov/prep/hosppcktgd/hosppcktgd.pdf

Hospital Preparedness Exercises Guidebook
http://www.ahrq.gov/prep/hospexguide/hospexguide.pdf

Hospital Preparedness Exercises Atlas of Resources and Tools
http://www.ahrq.gov/prep/hospatlas/hospatlas.pdf

patient safety and medical errors, and broaden access to essential services. AHRQ sponsors and conducts research that provides evidence-based information on health care outcomes; quality; and cost, use, and access. The information helps health care decisionmakers - patients and clinicians, health system leaders and policymakers - make more informed decisions and improve the quality of health care services. Prepared for AHRQ and the Assistant Secretary for Preparedness and Response by New York-based Weill Cornell Medical College, HHS said "these resources and tools can be used throughout the exercise cycle to help hospital preparedness planners meet federal funding requirements and accreditation standards, as well as strengthen an organization's preparedness systems. The Atlas "describes nearly 200 resources and tools that are available to help exercise coordinators meet federal funding requirements and accreditation standards throughout the exercise cycle. Each entry provides descriptive and citation information for the resource or tool," HHS said. Accompanying the Atlas is the Hospital Preparedness Exercises Guidebook, which complements the Atlas serving as a reference for planning, conducting, and evaluating exercises and for how to comply with accreditation standards and federal guidelines, and the Hospital Preparedness Exercises Pocket Guide, which serves as a quick reference summarizing the Guidebook. According to HHS, the Hospital Preparedness Exercises Atlas of Resources and Tools "is to be used in conjunction with the Hospital Preparedness Exercises Guidebook that "takes the user through the process of exercise planning, design and development, conduct, evaluation and improvement planning, along with requirements and standards (e.g., for federal funding and/or accreditation)." "Atlas users may wish to browse either the Table or the Indexes first, then refer to the detailed description of the resources or tools of interest in the Listings to learn more," HHS said, noting that "each section contains detailed instructions for use." The Hospital Preparedness Exercises Atlas of Resources and Tools was developed with the assistance of students from Weill Cornell Medical College who "worked in three- or four-person teams, with each team member scoring, labeling and writing descriptions of a subset of assigned resources and tools. These descriptions were reviewed and edited by other team members, with consensus on the final scorings within each group; disagreements were adjudicated by the project director," the Atlas stated. The Guidebook addresses preparedness exercise-related requirements for federal funding and hospital accreditation and "is intended for use in planning, conducting and evaluating such exercises, with the goal of improving hospital emergency preparedness programs. It also can serve as a resource for senior leadership to help increase institutional commitment to provide the necessary resources for successful preparedness exercises." The Guidebook provides cross-references to resources and tools that may be useful in these activities; "however, it should not be used as a sole reference for preparedness exercises," HHS emphasized, adding that "the focus of the guidebook is hospital preparedness exercises, an important component of a hospital emergency preparedness program. The contents reflect exercise guidance for US hospitals as of 2009." The Guidebook addresses the needs of a range of hospitals, including acute care and critical access hospitals, as well as those that are accredited, and those that are not. The Pocket Guide "is designed to provide hospital evacuation decision teams with organized and systematic guidance on how to consider the many factors that bear on the decision to order an evacuation, and assist decision teams in identifying some of the special situations, often overlooked, that may exist in their facility or geographic area that could affect the decision to evacuation,” HHS said. HHS explained that “a hospital preparedness exercise is a means for a hospital to test and evaluate its capabilities of preventing, preparing for, protecting from, responding to and/or recovering from an event that puts a significant strain on a hospital’s patient care or operating systems. Exercises are a component of a hospital’s emergency management program, which also may include emergency operations plans and an incident command system.”

Pirates winning war off Somali coast

Source: http://homelandsecuritynewswire.com/pirates-winning-war-somali-coast?page=0,1

The hugely expensive effort against the Somali pirates — a fleet of 40 warships from 30 countries is patrolling the waters near Somalia — has failed to slow down the rate of piracy; Somali attacks had soared dramatically in the past three years — from 40 attacks in 2007 to a reported 218 attacks last year; the Somali buccaneers are roaming over a much bigger territory and causing greater damage; the average ransom payment to the Somalis has doubled to $5 million; they are holding their hostages for up to 120 days — twice as long as in the past; they even used a hijacked freighter to attack a naval warship that was escorting supplies for African peacekeepers; the increasingly brazen pirates are currently holding 26 vessels and 609 hostages off the coast of Somalia; there is growing evidence that Somalia’s Islamic militants, including the feared al-Shabab radical group, are beginning to use piracy to raise money for their relentless rebellion against Somalia’s government. It has been another lucrative week for the barefoot buccaneers of Somalia. First they collected a $5.5-million ransom payment for a German-owned chemical tanker. Then, a day later, they hijacked another European cargo vessel, adding its eight crew members to their growing hoard of hostages. This latest haul of ocean booty is fresh evidence that the world’s navies are facing failure in their massive campaign to defeat the Somali pirates. Despite years of efforts by the naval forces of Canada and dozens of other countries, the pirates are more dangerous than ever. The Globe and Mail reports that a growing number of security experts are concluding that the naval campaign just is not working. At last count, the increasingly brazen pirates were holding 26 vessels and 609 hostages off the coast of Somalia, according to a European Union anti-piracy force. The hugely expensive effort against the pirates, including six naval ships from Canada alone in the past few years, has failed to slow down the rate of piracy. The number of hijackings by Somali pirates has steadily increased in recent years, with the Somalis accounting for 35 of the world’s 39 ships hijacked in the first nine months of this year. Moreover, the Somali buccaneers are roaming over a much bigger territory and causing greater damage. The average ransom payment to the Somalis has doubled to $5 million. They are holding their hostages for up to 120 days — twice as long as in the past. They even used a hijacked freighter to attack a naval warship that was escorting supplies for African peacekeepers. In an effort to crush the pirates, a fleet of 40 warships from 30 countries is patrolling the waters near Somalia. The anti-piracy flotilla is “the largest naval armada the world has seen in recent times,” says Deborah Akoth Osiro, a researcher at the Nairobi office of the Institute for Security Studies. “Yet, rather than contain the prob-

lem, the warships have driven Somali pirates further into the Indian Ocean," she said in the latest issue of the institute's journal. "There have been numerous attempts to combat piracy off the coast of Somalia, yet it is escalating." Osiro estimates that there are 1,000 to 1,500 Somali pirates operating in the seas today, roaming as far as 2,000 kilometers from their base in Somalia. They have launched attacks as far south as the Mozambican channel, as far north as the Red Sea, and as far east as the Maldives and the southern coast of India. "This is a vast area, and the navies cannot realistically cover it," Captain Pottengal Mukundan, director of the International Maritime Bureau, said in a recent report. The bureau is urging vessels to stay at least 600 nautical miles away from Somalia's coastline — although even that distance might be insufficient to protect themselves. A senior United Nations official, Lynn Pascoe, described the piracy situation as "appalling." In a report last month, he warned that the Somali piracy crisis is "outpacing" the international efforts to solve it. A study by the U.S. government in September found that Somali attacks had soared dramatically in the past three years — from 40 attacks in 2007 to a reported 218 attacks last year. The number of hostages seized by the pirates rose fivefold in the same period, reaching 867 hostages last year, and the total amount of ransoms increased from $3 million in 2007 to about $74 million last year. There are "not enough naval vessels among all of the combined navies in the world" to patrol the entire area of operations of the Somali pirates, the study concluded. The Globe and Mail notes that the pirates are often surprisingly low-tech. They bump across the waves in small skiffs, clambering barefoot as they scale the walls of ships, and their weapons are often so old that they are rusty. They are increasingly violent and ruthless, however, not hesitating to fire their automatic weapons and rocket-propelled grenades. They also have successfully dodged the anti-piracy fleet, putting their speedboats onto larger "mother ships" — or hijacked vessels — so that they can travel far away from the naval armada before launching their attacks. The pirates are supported by shadowy financiers who are rarely caught. There is growing evidence that Somalia's Islamic militants, including the feared al-Shabab radical group, are beginning to use piracy to raise money for their relentless rebellion against Somalia's government. Ship owners are responding with a dizzying array of defensive tactics: sonic beams; laser pointers; water cannons; rolls of razor wire; barred windows; lubricant foam to make stairways dangerous; teams of guards with sniper rifles, and "safe rooms" with reinforced steel walls to protect the crew if the pirates climb aboard. But none of this is working, and desperate governments are looking at new options. They have searched for countries willing to put the pirates on trial and imprison them, but almost every country in Africa (and in the West) is unwilling. Kenya has conducted most of the piracy trials, but it complains of being the "dumping ground" for arrested pirates. The Kenyan government is threatening to halt the trials unless it gets more money for its overloaded legal system. Nobody knows what to do with the pirates. Hundreds of them are simply disarmed and released after they are captured. Shipping companies continue to pay ransoms, even to suspected terrorists, because they know that a refusal to pay ransoms could damage their commercial interests. In desperation, many governments and ship owners are turning to mercenaries and private security armies. London-based insurance and shipping companies, for example, are planning to support a private navy of twenty armed patrol boats, with mercenaries on board. But the legal status of these mercenaries is unclear, and their existence could lead to controversial actions such as gun-running and executions at sea. In South Africa this month, police arrested four people who were allegedly smuggling weapons for an anti-piracy force in Somalia. "A return to privateering indicates that the Somali buccaneers have overwhelmed the naval armada," Osiro says. "The common thread of these anti-piracy responses is that they follow the path of least resistance. They seem to have been chosen to provide cosmetic solutions and circumnavigate the only obvious resolution: stabilizing Somalia."

ZAŠTITA
Zaštitari i oružje

Clinical psychology on how American Muslims cope with 9/11 aftermath

Source:http://homelandsecuritynewswire.com/clinical-psychology-how-american-muslims-cope-911-aftermath

A Tel Aviv University clinical psychologist examines how various Islamic beliefs and practices impact the psychological well-being of its adherents; among American Muslims, he is attempting scientifically to quantify how the after-effects of the 9/11 attacks — after-effects which included many stressors, such as increasing number of security checks, harassment, and verbal abuse — have affected mental well-being and what therapeutic role Islam plays, hoping to identify a clinical path for recovery; it is the first study of its kind and has findings applicable to other religions. Albert Einstein once said that science without religion is lame, and religion without science is blind. Now a Tel Aviv University researcher is one of the first to explore the link between these two realms in the Muslim world. Clinical psychologist Dr. Hisham Abu-Raiya of Tel Aviv University's Bob Shapell School of Social Work is investigating how various Islamic beliefs and practices impact the psychological well-being of its adherents. Among American Muslims, he is attempting scientifically to quantify how the after-effects of the 9/11 attacks have affected mental well-being and what therapeutic role Islam plays, hoping to identify a clinical path for recovery. It is the first study of its kind and has findings applicable to other religions, the researcher says. Since 9/11, U.S. Muslims have faced an increasing number of security checks, harassment, and verbal abuse. Via an online questionnaire, Dr. Abu-Raiya surveyed 138 American Muslims, asking how they coped with these new stressors. His findings were reported in Psychology of Religion and Spirituality in October.

The God response

During his post-doctoral studies at New York University, Abu-Raiya had witnessed firsthand how 9/11 impacted the Muslim community. For this study, he investigated the high volume of negative events experienced by American Muslim participants. The large majority reported experiencing at least one stressful interpersonal event after the 9/11 attacks, including anti-Muslim insults, special security checks in airports, and verbal harassment. The Muslims who created support groups or became more active at their local mosques, where they found strength in communal support. Theirs were considered positive responses and included a sense that they were experiencing "a test from God." Participants in general reportedly increased religious practices such as prayer, fasting, mosque attendance, and Quran reading following the 9/11 attack. Those who described feeling isolated from others and their community were more likely to report feelings of anger and depression. They were more likely to doubt God or their faith, and to express the possibility that God was punishing them.

A tool to assess Islam

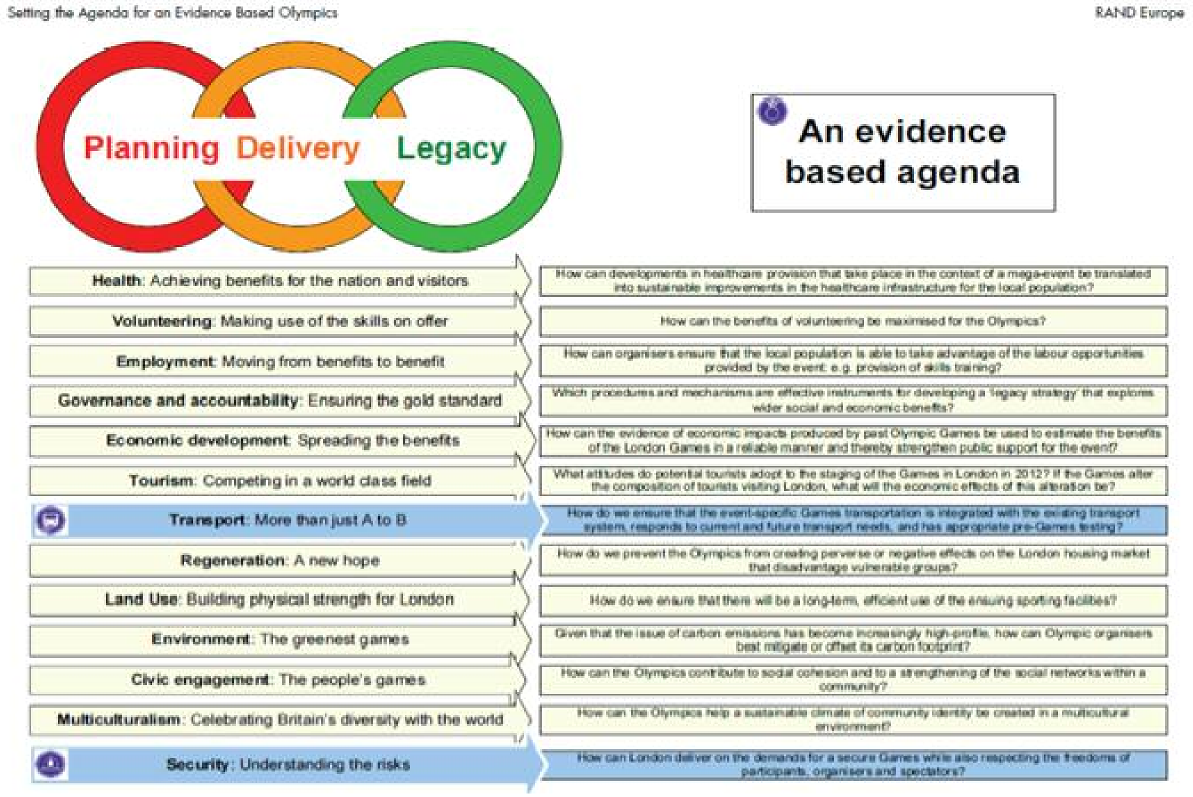
To interpret the questionnaire responses, Abu-Raiya used a tool he developed during his Ph.D. studies at Ohio's Bowling Green State University, the Psychological Measure of Islamic Religiousness (PMIR) — a scientifically-based, multi-dimensional tool for studying the psychological aspects of Islam. This assessment is similar to, yet different from, measures that quantify faith among other religious groups. "Religion can offer an immense amount of support to the individual and community," says Abu-Raiya. "My findings can help clinicians identify the kind of behavior that leads to positive responses — and how to help patients better reach their goal of healing." Religion can be used explicitly in the clinical setting as an important coping tool for life stressors, he adds, noting that the story of Job from the Quran — the same story that appears in the Old Testament — was particularly useful in guiding one patient through a long-term depression. Because all religions share universal values, Abu-Raiya's study of Islam on the emotional well-being of patients in a clinical setting can certainly be applied to other religions, including Judaism and Christianity. He notes that his research can also be used to increase awareness of the profound and traumatic impacts of the 9/11 attacks on Muslims living in the United States.

Setting the Agenda for an Evidence-based Olympics

RAND Europe Publications

Source:
http://www.rand.org/content/dam/rand/pubs/technical_reports/2007/RAND_TR516.pdf

To prepare for the London 2012 Olympic Games, it will be vital to ensure that the planning, delivery and legacy of the Games are fully accountable and based on the soundest evidence base available. The evidence base for specific policies can be built on two main foundations. Firstly, on the available evidence from previous mega-events; and secondly, through new primary research that places the challenges faced by the Olympics in the London context. In this report we present a meta-analysis of Olympic Games and mega-event policy issues based on a literature review of previous evaluations and analyses, to identify key issues that should be addressed in order to contribute to London 2012's aspiration as the most successful modern Games. We highlight two policy areas (transport and infrastructure, and security) in which specific research tools can be used to facilitate evidence-based policy making. In order to understand the evidence base required for transport and infrastructure, we have investigated the sorts of issues that can be addressed and provided a selection of potential studies that would provide high quality primary evidence for policy making for the Games. These studies make use of a number of modelling techniques in use at RAND Europe. Security is a particularly big concern for the modern Olympics. Through investigating previous threats, we can identify the likely threat types to London 2012. By understanding the interaction of hostile intent; operational capability; and potential influences on security, we can start to identify the security capabilities required to address different threats to security during London 2012.


Setting the Agenda for an Evidence Based Olympics

RAND Europe

An evidence based agenda

Health: Achieving benefits for the nation and visitors	How can developments in healthcare provision that take place in the context of a mega-event be translated into sustainable improvements in the healthcare infrastructure for the local population?
Volunteering: Making use of the skills on offer	How can the benefits of volunteering be maximised for the Olympics?
Employment: Moving from benefits to benefit	How can organisers ensure that the local population is able to take advantage of the labour opportunities provided by the event: e.g. provision of skills training?
Governance and accountability: Ensuring the gold standard	Which procedures and mechanisms are effective instruments for developing a 'legacy strategy' that explores wider social and economic benefits?
Economic development: Spreading the benefits	How can the evidence of economic impacts produced by past Olympic Games be used to estimate the benefits of the London Games in a reliable manner and thereby strengthen public support for the event?
Tourism: Competing in a world class field	What attitudes do potential tourists adopt to the staging of the Games in London in 2012? If the Games alter the composition of tourists visiting London, what will the economic effects of this alteration be?
Transport: More than just A to B	How do we ensure that the event-specific Games transportation is integrated with the existing transport system, responds to current and future transport needs, and has appropriate pre-Games testing?
Regeneration: A new hope	How do we prevent the Olympics from creating perverse or negative effects on the London housing market that disadvantage vulnerable groups?
Land Use: Building physical strength for London	How do we ensure that there will be a long-term, efficient use of the ensuing sporting facilities?
Environment: The greenest games	Given that the issue of carbon emissions has become increasingly high-profile, how can Olympic organisers best mitigate or offset its carbon footprint?
Civic engagement: The people's games	How can the Olympics contribute to social cohesion and to a strengthening of the social networks within a community?
Multiculturalism: Celebrating Britain's diversity with the world	How can the Olympics help a sustainable climate of community identity be created in a multicultural environment?
Security: Understanding the risks	How can London deliver on the demands for a secure Games while also respecting the freedoms of participants, organisers and spectators?

BAE Systems Develops Non-Lethal Laser to Defend Against Pirate Attacks on Commercial Shipping

Source:
http://www.baesystems.com/Newsroom/NewsReleases/autoGen_111010105948.html

Bristol, UK: BAE Systems has successfully demonstrated a prototype device that will serve as an effective non-lethal deterrent against pirate attacks on commercial vessels such as oil tankers and container ships. Piracy worldwide is on the rise according to reports from the ICC's International Maritime Bureau (IMB), with 430 attacks worldwide reported last year, up from 406 in 2009. As pirates increase their range of operations and their capabilities, commercial shipping agents are increasingly looking for ways of preventing attacks whilst avoiding armed guards on their ships. In order to help combat the growing piracy threat BAE Systems conducted a study of pirate's behaviour and a company-wide capability survey. This led to the development of the concept of using a non-lethal laser, which would leave only temporary effects, to distract and deter potential attackers from a distance. Leveraging the capability of its Optics and Laser Technology Department within its Advanced Technology Centre, BAE System's researchers conducted a number of experiments to assess the feasibility of laser distraction as a non-lethal weapon. The research team has now successfully demonstrated a suitable laser at the Pershore Trials Range in Worcester over a variety of distances in a variety of conditions. The laser beam is capable of providing a visual warning to pirates at distances greater than 2km, and of disorientating attackers sufficiently at lesser distances so that weapons cannot be targeted effectively. At all times the power levels of the laser remain eye safe. Roy Evans, BAE Systems capability technology lead for laser photonic systems, said: "The effect is similar to when a fighter pilot attacks from the direction of the sun. The glare from the laser is intense enough to make it impossible to aim weapons like AK47s or RPGs, but doesn't have a permanent effect." The laser was trialled during night and day in varying weather conditions at the Worcester facility. Cameras were placed at the target location to demonstrate the level of beam intensity and divergence produced by the test runs. Beam oscillation techniques were also demonstrated. The researchers have developed a bespoke Neodymium Yttrium Aluminium Garnet (Nd:YAG) laser which is an effective deterrent at relatively low power levels. By utilising targeting systems and changing beam patterns, the distraction effect can be made more pronounced and be used against multiple targets. Evans continued: "We successfully showed that the laser works not just during the night, but also in full daylight. But, there are many more requirements to meet before placing a non-lethal laser weapon on commercial ships.» When fitted on commercial ships the laser distraction system could utilise its own targeting capability or

integrate with existing ship radar and sensor systems to control the direction and power of the beam. It could therefore work semi-autonomously and would also include security features to ensure it could not be used by pirates if they boarded the ship. Bryan Hore, BAE Systems business development manager and the lead for the anti-piracy programme, said: “Laser distraction is part of a wider programme of anti-piracy technologies being developed by BAE Systems, including radar systems, which utilises expertise and knowledge from the military domain. The aim of the laser distraction project is now to develop a non-lethal deterrent to pirates, which has no lasting effects, which can work in a maritime environment, be operated by the crew at no risk, and be cost effective.”

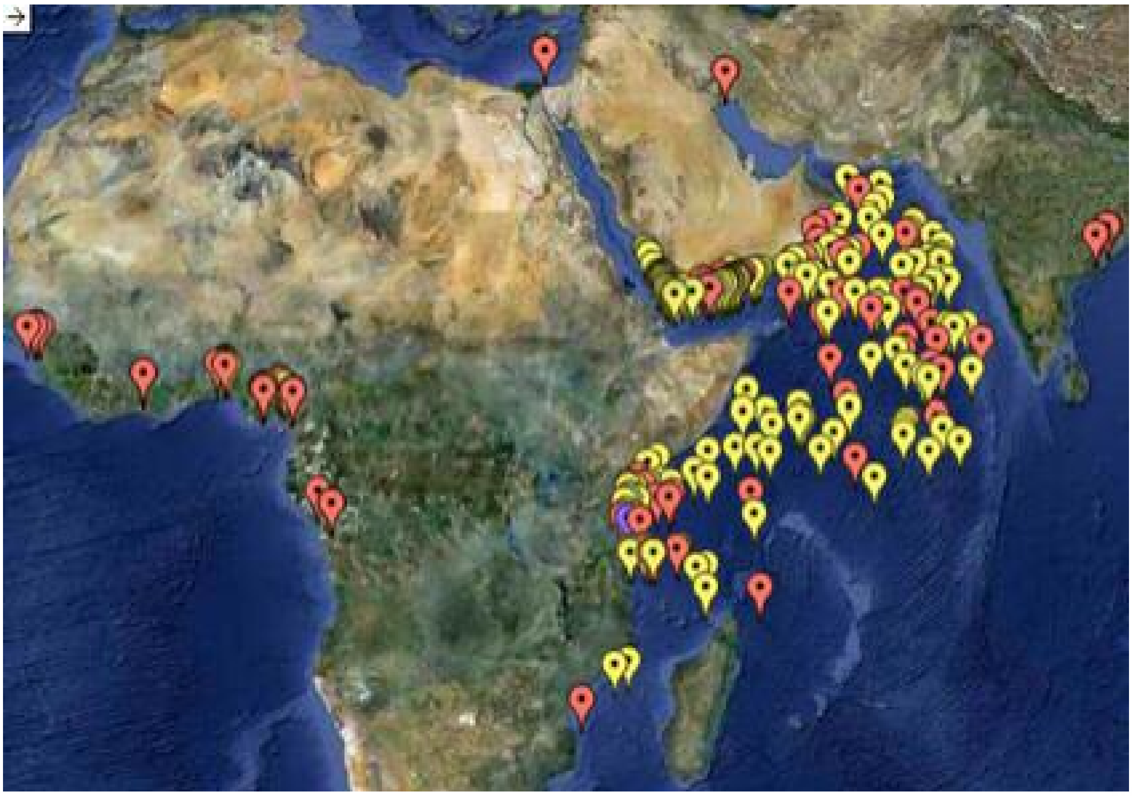
Piracy in the Horn of Africa: 2008-2010

Source:http://www.icc-ccs.org/index.php?option=com_fabrik&view=visualization&controller=visualization.google map &Itemid=219

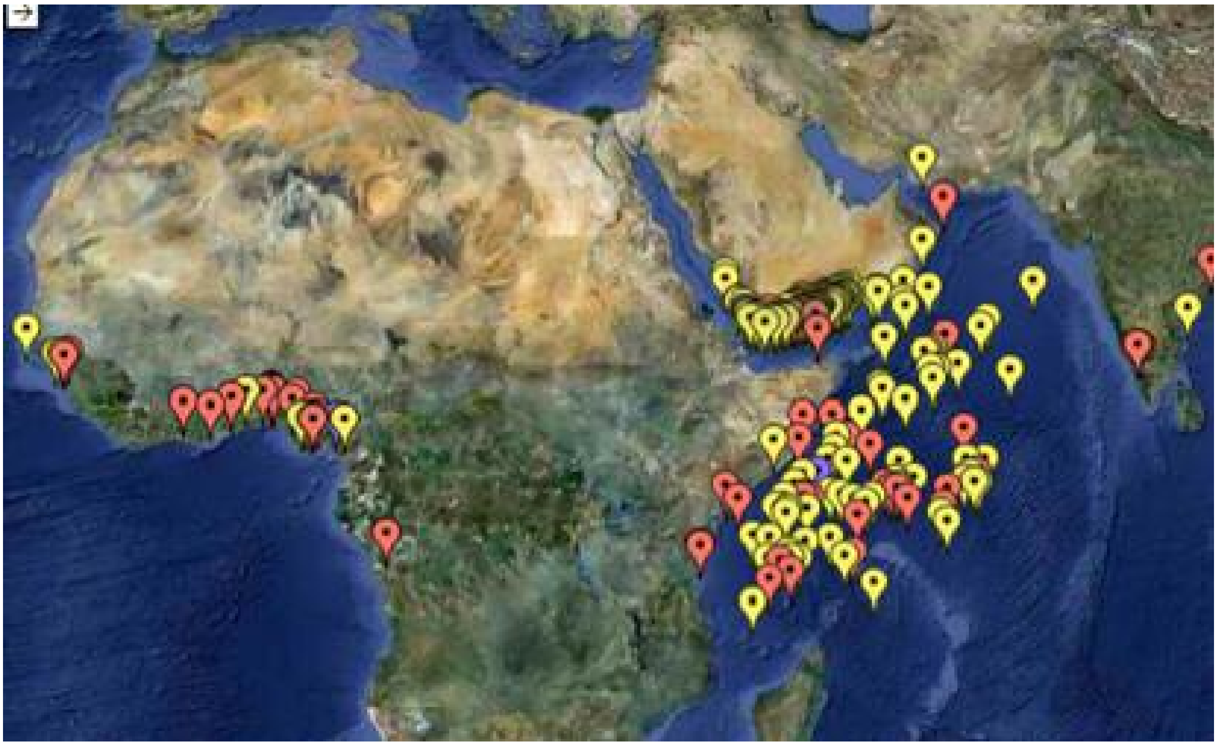
This map shows all the piracy and armed robbery incidents reported to the IMB Piracy Reporting Centre during 2010. If exact coordinates are not provided, estimated positions are shown based on information provided. Zoom-in and click on the pointers to view more information of an individual attack. Pointers may be superimposed on each other.

🔴 = Actual Attack 🟡 = Attempted Attack 🟣 = Suspicious vessel

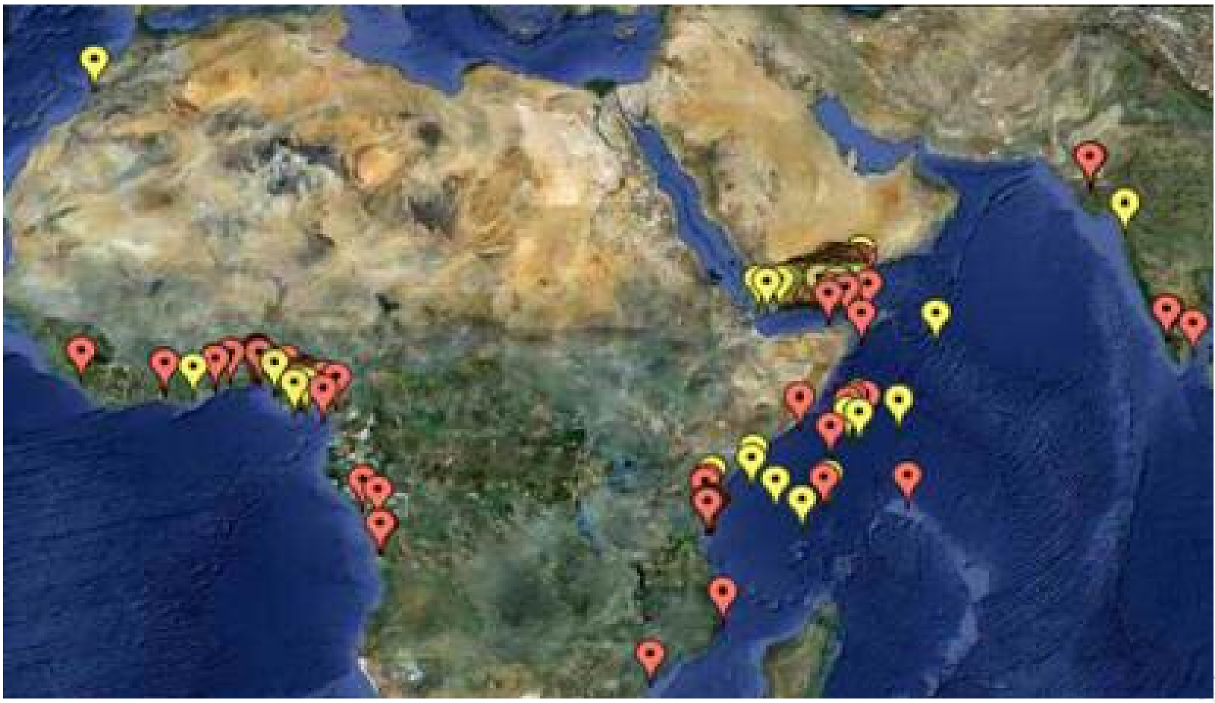
2010 (Observe the shift to the right towards India)



2009



2008



EDITOR'S NOTE: Referencing Wikileaks some claimed (2010) that the strange physical phenomenon known as "Aden Vortex" is the main reason for the international flotilla accumulated in the area. It might be interesting to look further deeper into this information. There is" no smoke without fire"!

Countdown to the Olympics – Jan 2011

By David Evans

Source: http://www.infologue.com/featured/countdown-to-the-olympics-jan-2011-part-three/

"In my first article for Infologue I described how the security planning for the 2012 Games sat within the UK's Counter Terrorist Strategy, CONTEST, and how industry was recognised as an essential partner in that strategy. In my second article I explained how implementation of CONTEST was being undertaken by Government and encouraged in the private sector, and also explained how this translated into the Olympic arena.

"The International Olympic Committee (IOC) in evaluating bids from potential host countries look at many factors, of which safety and security are of paramount importance. They are not prepared to allow responsibility for this element of the Games to lie solely with the national organising committee for the Games. They demand that the state is the guarantor of safety and security and in London's case this was determined to be the Home Secretary, on behalf of the Government.

"Safety & Security for the Games can normally be divided into 3 parts:

1. The build;
2. The Organising Committee's responsibility at venues;
3. The State's responsibility in the lead-up to and during Games time.

"This has traditionally been further complicated by organising the Olympic and Paralympic Games as entirely separate events. It is easy to view the Paralympic Games as a side-show; a follow-up to the main event. The Paralympic Games is anything but this. Whilst being approximately 40% of the size of the Olympic Games, it is nonetheless second only to the Olympic Games in size in the world as a major event. One of the winning factors in our bid to host the Games was that, for the first time, there would be one organising committee to cover both Games. This has meant that planning for both events is seamless and more effective. It has also given the Paralympic Games a higher status in relation to the Olympic Games. With that increased status comes a higher profile in terms of risk and the planning to mitigate those risks. The Olympic Security Directorate (OSD)strategy for the safety and security of the London Games has recognised this in its Olympic& Paralympic Safety & Security Strategic Risk Assessment (OSSSRA) and the Olympic & Paralympic Safety & Security Strategy (OPSSS). In keeping with the Office for Security and Counter Terrorism's open and transparent way of working with the country through CONTEST, so has the OSD been open and transparent by publishing summaries of its OSSSRA and OPSSS.

"The Olympic Security Directorate in fashioning its strategy has demonstrated its overall responsibility for safety and security at Games time. This is important in terms of its effect and comparison with planning at previous Games. From an early stage the Olympic Security Directorate has embraced all 3 parts of Olympic Safety & Security – Build (Olympic Delivery Authority), Venues (LOCOG) and

State (OSCT, MPS, ACPO and other agencies). Auditing visits by the IOC have commented favourably on how closely integrated all these elements of planning are. Prior to the OSD taking overall responsibility for planning the MPS had already demonstrated their renown professionalism bygetting underway with planning immediately the Gameswere awarded.

"The Olympic and Paralympic Safety and Security Strategic Risk Assessment utilises the same methodology as that used in the National Risk Register and the scope of the OSSSRA is aligned to the OPSSS to ensure that:

- It assesses risks that may occur both during the design and build stage and during Games time, acknowledging that the emphasis will be on impacts on safety and security during the period of the Games themselves;
- It assesses risks to all Games locations, whether that be the sporting venues or the physical or electronic infrastructure that supports them;

- It assesses risks for the purposes of all five objectives in the Strategy: Protect; Prepare; Identify and Disrupt; Command, Control, Plan and Resource; and Engage, and
- It only assesses those risks that have a safety and security element to them, not those risks that solely have an impact on the smooth running or continuity of the Games themselves; and
- It does not replace existing contingency and safety plans for Games venues or day to day emergency service activity.

The OSSSRA considers threats from five distinct areas, namely:

- Terrorism;
- Serious and organised crime;
- Domestic extremism;
- Public disorder; and
- Natural events.

It breaks each of these down into:

- Terrorism
    - Attacks on crowded places – Games venues and other organised events e.g. Live Screens;
    - Attacks on transport systems – e.g Underground system; and
    - Non-conventional attacks – this is attack by non-conventional material: chemical, biological, radiological and nuclear (CBRN).
- Serious and Organised Crime
    - Crime – previous experience shows that low-level crime falls at or in the vicinity of Games venues and focus needs to turn to high value assets and athletes at the Olympic Park and Olympic village;
    - Organised crime – of particular interest is the likelihood of fraud within the ticketing system;and
    - Cyber attack – internet technology will be fundamental to the administration of the Games and attacks are likely against the Olympic website, the electronic infrastructure of the Games and sponsors, cyber enabled ticketing, and attacks on IT, communication and transport.
- Public disorder – the Games provide a global stage on which protestors seek to publicise diverse causes in lawful and unlawful ways and also provides an opportunity for domestic extremists to seek to disrupt preparation and delivery phases.
- Natural events
    - Severe weather; and
    - Human diseases.

In addition to these threats the OSSSRA considers the impact of risk, malicious and non-malicious, on the Games critical infrastructure.

"The OSSSRA then moves into a risk identification and mitigation process using existing but tailored processes in three phases:

- Phase 1 Identifying the risks:
    - Identification – utilising current intelli

gence assessments. A comprehensive picture of the risks is built and each risk exposed to expert opinion, from government and other agencies and a reasonable 'worst case scenario' agreed for subsequent scoring in the next stages.

- Assessment – the agreed reasonable worst case scenarios are assessed for impact and likelihood by relevant experts. A number of assessment criteria are used, dependent on the risk ranging from scientific and statistical data to assessment of capacity and vulnerability of the target. Impact assessments are also undertaken to assess for each scenario, the likely number of fatalities and casualties, damage to property and assets, disruption to services and financial loss. Risk to reputation is also considered.
- Comparison of the risks – once assessed the risks are plotted onto a risk matrix. As all potential threats and hazards are plotted against the same criteria, it is possible to make a comparative assessment as to which pose the greatest risk. Mapping the risks on an 'Impact/likelihood' table allows for an 'at a glance' comparison with other risks and also enables a pre and post mitigation comparison to be made.

The OSSSRA does not cover all possible risks only those deemed significant enough for inclusion, but all risks are reviewed on a regular basis and their status assessed.

- Phase 2 Mitigating the risks

"Strategic Design Requirements (SDRs) – these are high level statements of requirement needed to mitigate a particular risk. It does this by either reducing the likelihood of it occurring or reducing the impact should it occur. SDRs are similar to Planning Assumptions made in the National Risk Register but add prevention of a risk to preparing and dealing with the consequences. The OSD uses SDRs to create commissions with partner agencies such as the police or UKBA. There are currently 27 such projects under commission. The principles of the OSSSRA and associated SDRs are being used by OSD's partners and stakeholders in their support of the security and safety strategy.

- Phase 3 Understanding residual risk
  - To ensure that commissions deliver and when combined are proportionate the OSD conducts a risk reduction assessment (RRAt).This assessment is designed to ensure that duplication of effort and resource is avoided and that any gaps are identified.
  - Following the assessment the OSD is then able to determine the residual risk and this informs Ministers, senior officials and operational commanders so that a decision can be made as to whether or not the level of residual risk is acceptable and if not what more work is needed to be done on mitigation.

The OSSSRA process is managed by the Design Authority Team (DAT) who sit within the OSD and who work closely with the Civil Contingencies Secretariat. Many agencies and subject experts across Government are involved in the input into the OSSSRA keeping it current and having the ability to comment on assessment and vulnerabilities. It is refreshed on a regular basis.

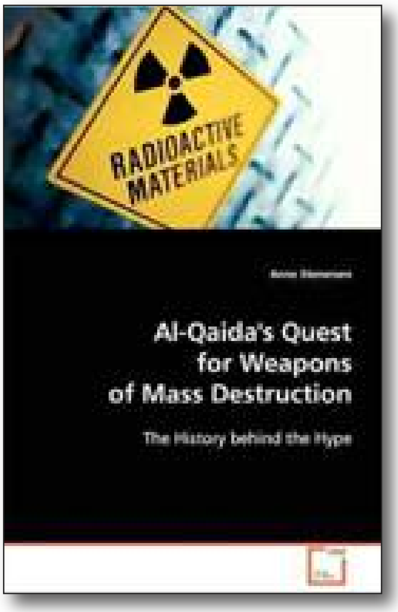
"I hope that this article on risk assessment shows the depth and joined-up nature of the work being undertaken by the OSD. I have certainly found it to be impressive in its scale, content and scope. This work will have, I think, a profound impact on the future co-ordination of security plans and inevitably there will be a beneficial impact on the private sector. In my next article I will report on the Safety and Security Strategy for the Games."

Writing exclusively for Infologue.com, David Evans, is the BSIA's Director responsible for the Olympics.

Al-Qaida's Quest for Weapons of Mass Destruction: The history behind the hype

Author: Anne Stenersen (Saarbrücken: VDM Verlag, 2009)

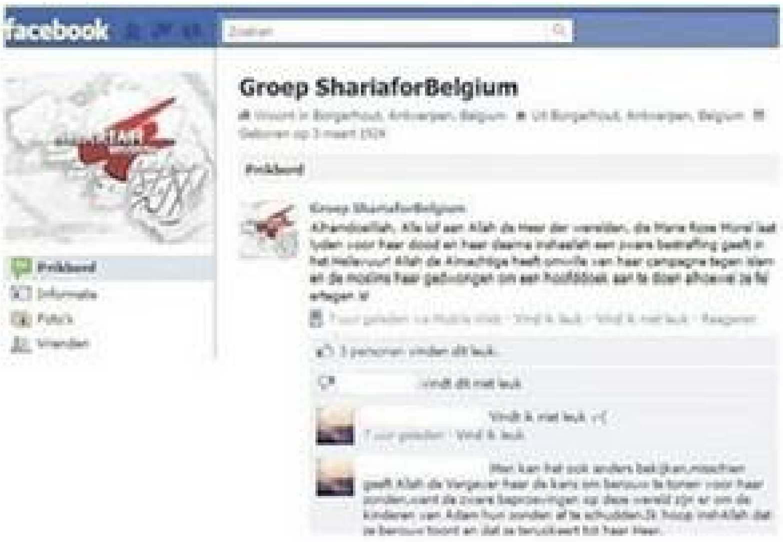
Ever since the late 1990s, it has been claimed that the threat of chemical, biological, radiological and nuclear (CBRN) terrorism from al-Qaida is real and growing. This book explores al-Qaida's interest in CBRN weapons, as reflected by statements and activities on various levels within the network between 1996-2007. Drawing on the author's extensive collection of al-Qaida CBRN-manuals, online discussions and 'chatter' on CBRN/related themes, the author finds that a high level of amateurism has characterised al/Qaida's efforts in this field. The book is aimed at students, scholars, and practitioners with an interest in the topics of CBRN terrorism and militant Islamism, and is of particular interest to professionals within the counter-terrorism community.


RADIOACTIVE MATERIALS
Anne Stenersen
Al-Qaida's Quest for Weapons of Mass Destruction
The History behind the Hype

Shariah4Belgium celebrating Vlaams Belang politician's terminal illness

Source:http://www.hbvl.be/nieuws/binnenland/aid1008150/allah-dwong-morel-tot-hoofddoek-en-bestraft -haar-in-het-hellevuur.aspx

The radical Islamist organization, Shariah4Belgium, is celebrating the terminal illness of former Vlaams-Belang politician, Marie-Rose Morel. Morel, who is fighting cancer, is currently in the terminal stage of her disease, and is too weak to receive further treatment. «Alhamdulillah, all praise to Allah the Master of the World, who makes Marie Rose Morel suffer to death and will then, inshallah, punish her severely in Hellfire! Allah the Almighty has, because of her campaign against Islam and Muslims, forced her to wear a headscarf [ed: she lost her hair due to treatments], though she's vehemently aganist it!» Vlaams Belang senator, Jurgen Ceder,wants to know when the Centre for



Groep ShariaforBelgium

Woont in Borgerhout, Antwerpen, Belgium · Uit Borgerhout, Antwerpen, Belgium · Geboren op 3 maart 1924

Prikbord

Groep ShariaforBelgium
Alhamdoelillah, Alle lof aan Allah de Heer der werelden, die Marie Rose Morel laat lijden voor haar dood en haar daarna inshaalah een zware bestraffing geeft in het Hellevuur! Allah de Almachtige heeft omwille van haar campagne tegen Islam en de moslims haar gedwongen om een hoofddoek aan te doen alhoewel ze fel ertegen is!

7 uur geleden via Mobile Web · Vind ik leuk · Vind ik niet leuk · Reageren

3 personen vinden dit leuk.

vindt dit niet leuk.

Vindt ik niet leuk :-(
7 uur geleden · Vind ik leuk

Men kan het ook anders bekijken,misschien geeft Allah de Vergever haar de kans om berouw te tonen voor haar zonden,want de zware beproevingen op deze wereld zijn er om de kinderen van Adam hun zonden af te schudden.Ik hoop insh-Allah dat ze berouw toont en dat ze terugkeert tot haar Heer.

Equal Opportunities and Opposition to Racism will act against this form of incitement to hatred. He points out that political difference can be fought out in different way in Belgium, but not by wishing people to die. With such statement «extreme Islam once again shows its backwardness and fanaticism.» Earlier former colleague Bart Debie announced on his Facebook to «put the champagne on ice», which cost him his place in Vlaams Belang.

Publications of George C. Marshall European Center for Security Studies

Source: http://www.marshallcenter.org/mcpublicweb/en/nav-pubs-per-concordiam.html

Feb 2010

Concordiam
RESOLVING 'FROZEN CONFLICTS'
The Challenges of Reconciliation

July 2010

October 2010

Suicide Terrorism

Modern ‘martyrs’ or exploited prey at the altar of politics?

By Cmdr. Ioannis Chapsos Hellenic Navy

Source:http://www.marshallcenter.org/mcpublicweb/MCDocs/files/College/F_Publications/perConcordium/perConcordiamV1N2English.pdf

The “war on terrorism” proves to be constantly changing, and every emerging terrorist action demands new techniques to counter it. Suicide terrorism has received a great deal of attention from scholars and analysts during the past decade, although terrorism is nothing new per se. The dramatically increased frequency and lethality of such incidents in the post-9/11 era have led academics and practitioners in a plethora of disciplines to try to identify what motivates, sustains and spreads terrorism.

What about "suicide terrorism?"

Numbers usually tell the truth, and the global records are indicative: Suicide bombings represent a minority of the overall terrorist attacks, but simultaneously cause the majority of human casualties related to terrorism. Between 2000 and 2004 (Atran 2006, 127) nearly 7,000 people lost their lives in 472 suicide attacks in 22 countries; even more were wounded. These numbers become even more impressive when taking into account that almost 85 percent of the incidents during the past 25 years took place between 2004 and 2008 (Wright 2008), while attacks increased to unprecedented numbers.1 The reduced number of suicide attacks recorded globally in 2008 (469 attacks, compared with 608 in 2007) is mostly ascribed to a declining number of incidents in Iraq. On the other hand, there has been a remarkable increase in the number of countries where suicide attacks are perpetrated2 (Merari et al. 2010a, 89). Additionally, in the period from 1981 to 2008, 3 only a few of the 2,937 suicide bombers around the globe acted individually and were not sent by organized groups (Merari et al. 2010b, 103).

Hoffman (2006, 132-133) and Speckhard (2006, 3) stressed the tactical advantages that make suicide bombing the preferred method of attack. The combination of high success in urban areas, inexpensive preparation and simple execution result in the creation of the "smart human bomb." The cost is $150 and a person willing to die to create the "poor insurgent's F-16." The brutal outcome incorporates agility and flexibility to maximize the lethality of the detonation, resulting in an extreme sense of horror and intimidation in the targeted society. The perpetrator needs no escape plan because his death is a precondition for the operation's success. This is a guarantee that there is no chance the bomber will be arrested and interrogated afterward. It also prevents authorities from tracking bom

Dzhennet Abdurakhmanova, 17, one of the suicide bombers in the Moscow Metro attacks in 2010, poses with her husband, Umalat Magomedov. Since 2001, there has been an increase in women participating in terrorist attacks.

A bomb blast hits the American consulate in Peshawar, Pakistan, on April 5, 2010. Islamic militants armed with guns, grenades and suicide car bombs killed 46 people. Pakistan's Taliban claimed responsibility for the attack.

bers back to their hideouts. These traits lead to the theory that suicide bombing could be considered a military innovation (Horowitz 201, 39). Media coverage of the incident is a "force multiplier" for the psychological impact on the local society. The global attention shows the strategic psychological impact of the suicide bomb. How can we stop these atrocious tactics when military means are insufficient? How could we deter or even dissuade those willing to die as pious martyrs, given that the global strategy against them appears to be futile? The first step is to learn about and understand these "human bombs."

Religious or social motivation?

In detailed research from all the recorded suicide attacks worldwide between 1985 and 2001, Pape (2003, 345) said suicide terrorism is "the threat of punishment to coerce a target government to change policy, especially to cause democratic states to withdraw forces from territory terrorists view as their homeland." He claims that it stems from a broader strategy aimed at political goals. Terrorism is used as a tool in vulnerable and weak democratic countries sustained by foreign military occupation. Weak authoritarian states are not usually targeted because it's difficult to organize such operations there. Recently, he expanded on his thesis (Pape 2008, 275), stating that suicide terrorism is usually the outcome of a foreign democratic power's military occupation of a society with different religious views. When other means are not effective in forcing this power to withdraw, suicide terrorism is used. This terrorism is not always motivated by religious extremism but often by political objectives such as self-determination, counteraction to colonization, opposition to foreign interference in internal issues and exploitation of natural resources. He clarifies that "occupation" is a broad term, referring not only to the military forces' physical presence, but also to the interaction in political terms and to financial and ideological cooperation between governments, such as the cooperation between Saudi Arabia and the United States.

Piven (2007/2008, 734) argues that suicide terrorism "is considered a reasoned response to political injustice and humiliation." He recognizes the role of religion not in initiating but in amplifying the motivation caused by the feeling of oppression. The combination of oppressive circumstances and indoctrination makes demonization of the opponent easier. This contributes to the construction of a foe even if he doesn't already exist. In his "cosmic war" theory, 4 Juergensmeyer (2008, 421) proposes that there are no innocent people, only representatives of a collective enemy. The primary enemy is the political or religious entity that threatens the terrorist group and the secondary enemy could be any individual or entity supporting the primary. One must remember that radical Muslims don't see the ongoing war as a global campaign against terrorism, but as a war against Islam (Esposito and Mogahed 2007, 29).

Hence, religion has a role to play by uniting Islamic populations under the common sacred values and political demands to fight for, but it's not the major incentive for suicide terrorism. Muslims are "attached" to their moral and spiritual values (Esposito and Mogahed 2007, 37) rising from their religion. They regard these values as critical for their cultural and social survival and progress. We have to bear in mind that Islam (Ali and Post 2008, 626. Palazzi 2008, 52-58) strictly forbids (haram) committing suicide. Islam became a tool in the hands of radical Muslims, 5 who tried to transform it from a religion to a political ideology. They misinterpreted terms such as jihad and martyrdom, exploiting the piety and the psychology of their co-religionists,6 recruiting and inculcating them with the will to die to achieve political objectives.7

According to the Quran, the defensive jihad and even the qittal8 are terms irrelevant to the ascribed translation. The real "istihad," which means martyrdom and self-sacrifice in the name of Allah, is ideologically far from suicide (Dunn 2010, 18). The word is even further from the "holy war" that Osama bin Laden waged against the foreign occupiers, since it doesn't refer to taking other people's lives. Hereof we'll search even deeper for the fundamental traits of suicide terrorism.

The social and behavioral factors

Iraq became a contemporary "case study" of suicide terrorism because of the almost daily suicide attacks.9 From the perspective of jihadists this war is a broader, global resistance against Western culture and democracy. A potential victory is as vital for al-Qaida as it is for the coalition forces and United States. The same aspects prevail in the Palestinians' conflict with Israel.

On both of these fronts, another social factor vital for suicide terrorism is indoctrination. In Palestine, children learn from kindergarten to accept shahids (martyrs) as heroes who defy death (Ali and Post 2008, 639). The martyrs are honored to be chosen for such a mission and fight inequity by punishing their enemies according to God's will. Hence, they are named "self-chosen martyrs," perceived as honored soldiers in a great war, offering their lives for the sake of the community and religion. Palestinian males grow up dreaming of being the next potential chosen one for the "honor of martyrdom" so their names will be perpetually remembered with social approval. When children are radically nurtured and brainwashed against a hated adversary (Piven 2007/2008, 740), and their psyche is programmed through the everyday terror, reprogramming is infeasible.

The media and Internet are critical multifunctional tools for suicide terrorism (Ali and Post 2008, 630). The exploitation of videos and various communication networks provides a perfect option for recruitment (Townsend 2007, 44). It is also a very effective tool for propaganda and interaction between social groups or individuals with common beliefs. Technology offers local insurgents the potential of manipulating a global audience and building a network for close connection between the country of origin and the country where immigrants from the country of origin live.

The Information Age is empowering terrorist groups seeking political legitimacy. The groups are trying to convince the local and global societies that they are fighters and insurgents, not terrorists. They are fighting against oppressive foreign occupation and their cause is just. On terrorist Web pages, immigrants see pictures and videos of "martyrs" dying for that cause and hear stories describing the pain, humiliation and catastrophe that relatives suffer. These images and sounds travel around the world, awakening sympathy and support. Support abroad grows even if the descendents of immigrants have never visited their homeland.

People are deeply influenced by the martyrdom of known or unknown people who blow themselves up to protest the political and unjust conditions in their country. This amplifies the moral obligation among immigrants to contribute to the struggle and aids recruitment. The sentimental, societal and religious attachment to the terrorist cause draws volunteers for self-sacrifice. The social structures of the areas mostly affected by the phenomenon of suicide terrorism are a derivative of nomadic culture10 (Shay 2007, 177). for amelioration (Ali and Post 2008, 640). From these components, suicide bombing is a desperate message to the global audience, an awful reaction to the hopelessness of their lives. But what is important is that their actions intend to take the lives of others as well as their own, a fact that distinguishes suicide from murder (Townsend 2007, 41).

Amid other behavioral factors, we can't disregard the “mimetic desire” among peers to express violence (Juergensmeyer 2008, 419). Inside their organization, the would-be bombers see each other as competitors, so mimesis is more plausible as motivation than aggression or religious symbols.

Left: Iraqi Sajida Mubarek Atrous al-Rishawi shows off
an explosive belt as she confesses on Jordanian state-run television to her failed bid to set off the bomb inside one of three Amman hotels targeted by al-Qaida in 2005. The media can be an effective tool in counterterrorism.

Right: Pakistani police display suicide jackets seized in
March 2010. Companies that provide bomb-making materials can prevent attacks by informing the authorities about unusual orders.

When their community is threatened, the feeling of obligation to participate is generated so as not to let down the rest of the tribe. This fosters the “self-motivation” mechanism of foreign fighters, who are determined to sacrifice even before they approach terrorist networks (Argo 2006, 3). This feeling stems mostly from images on television and reading about tribal members on the Internet or the news.

Living under the conditions in Palestine and Iraq, the inhabitants exhibit behavior strongly determined by despair, victimization, helplessness and lack of optimistic prospects

From the standpoint of religious diversity and cultural and regional factors, terrorism is a reaction stemming from revenge and the belief that this is a way to redeem lost honor (Ali and Post 2008, 643/ Townsend 2007, 40). Because a family member, a sibling or a close friend has been killed or abused by opposing forces, the would-be suicide bomber is strongly inspired by vengeance.11 In other cases, like when faith or social beliefs stigmatize rape victims and prevent them from getting married and having children, 12 ignominy is a motive and the characteristic paradigm of purification through martyrdom. These kinds of traumas, combined with a sense of injustice, misery and humiliation, prompt aggressive reactions amplified through group psychology, influence, amity and interaction (Piven 2007/2008, 739). This individual process, interacting with group mentality and indoctrination, produces the suicide attacker (Townsend 2007, 43). Simultaneously, there exists a charismatic leader who exploits the despair and manipulates the vulnerability of these people to transform them into "human bombs." Perceiving suicide bombers as "brainwashed pawns" or mentally disabled is a mistake. Their own will to die is the primary precondition for the existence of the phenomenon.

Female suicide bombers

The increased participation of women in suicide attacks can't be disregarded. The number of incidents in Iraq rose from eight in 2007 (Ghosh 2008) to 29 by September 2008 (Peter 2008) and drew the attention of many analysts. The deadliest attack in Iraq in 2010 occurred on February 12, when a woman suicide bomber detonated herself south of Baghdad, killing more than 40 Shiite women and children (Arraf 2010), all pilgrims. While other kinds of attacks decreased in Iraq, suicide bombings by women — harder to detect than male bombers — rose dramatically in 2009.

After more than 20 years of multiple female suicide bomber waves, 13 terrorist groups have leveraged the tactical advantages of using women in terrorist attacks14 (Burton and Stewart 2007). They hide the explosives under the women's idiomorphic clothing (burqa or niqab), making the women appear pregnant. There is a cultural resistance to searching women, who are generally considered nonviolent. Female suicide bombers can move through security without arousing suspicion and bypass security checkpoints to reach their target untraced. The final outcome receives even greater media attention and coverage, since the perpetrator is a woman, and this constitutes a force multiplier for the terrorist group.

The motivation of the women is similar to that of their male counterparts. Again, religion isn't the principal motive (McGirk 2007), since eternal life with 72 virgins in paradise can't be an incentive. All the social and behavioral factors that motivate males are valid in the case of "female smart bombs." Women are more likely to be seeking revenge for a personal loss or trying to regain lost honor from being a rape victim (Bloom 2007, 95). This was apparently evident in the testimony of a woman named Samira Jassim, whom Iraqi officials arrested in 2010. In a videotaped confession, she told interrogators she had recruited more than 28 women to blow themselves up. She was part of a plot in which young women were raped and persuaded to become suicide bombers as their only escape from shame and to reclaim their honor (Arraf 2010).

It's also notable that "converts" are considered to be among the most dangerous groups and the principal future resource pool for terrorist entities. That's not only because they own mostly European passports, making it easier for them to travel around. The potential need to prove that they are more pious than their co-religionists born into the faith makes them even more radical in belief and deed.

Opportunities in responding to suicide terrorism

We should focus on preventive measures to reduce the factors that affect suicidal terrorism in Europe, perpetrated mostly by homegrown Muslim extremists or converts (The Economist 2008). Europe absorbs attacks aimed at the West, although the United States is seen as the primary target. That generates an internal European counterterrorism effort, seen mostly as a law enforcement assignment in homeland defense, to deal with the "grass-root cells." The potential formation of special links between organized crime and these cells is of even greater concern to European police agencies. On the other hand, the United States' counterterrorism effort is mostly an external "war on terrorism" that it fights using military means, something that can't be done in Europe.

Another challenge is the cooperation of counterterrorism agencies at the national and multinational level. Intelligence and the free flow of information are keys to success. Even companies that provide materials for bomb building could collaborate by informing the proper agencies about clients ordering unu sual quantities. We should operate in an information channel such as al-Qaida's, where a simple call across a global network triggers a specific reaction.

As Whitelaw (2008) reveals, the Combating Terrorism Center in the United States recently released personnel records captured in Iraq containing the biographical and personal details of terrorist recruits. The records could be very helpful for intelligence agencies around the globe and the paradigm of countering suicide terrorism by prevention through intelligence. In a similar way, we could also track and disrupt the organizations that sponsor and finance terrorism.

The community involvement perspective offers a very interesting alternative (Gaylord 2008). Police officers who receive counterterrorism training could transfer their knowledge to groups of citizens, involving them in an early warning social system, a "Neighborhood Watch Program." On the one hand, it's impossible for law enforcement agencies to be everywhere; on the other hand, it's very easy for a resident to recognize something unusual where they live or work.

A similar initiative has been undertaken with the foundation of the "Daughters of Iraq" program, under the guidance of U.S. officials. The aim is to train female police officers to search suspicious women at security checkpoints. As O'Rourke (2008) said, the program does not seem to be very successful since, because of social restrictions, only 30 women offered to participate. The point is the suicide attackers target first the "occupation forces," not their countrymen. The fact that religious entities have shifted their tactics to recruiting women for suicide attacks suggests that they'll also develop new techniques to bypass security checkpoints.

Governmental cooperation should also be extended to religions. The role of Islam in suicide terrorism has already been analyzed. The false image that the radical Muslims created, concerning the oppression of their religion by Christians, and the clash between the two, raised skepticism and mistrust between Arab countries and the West. Antagonism between Sunnis and Shiites has also created another clash, an internal and bloody struggle with a vast number of Muslim victims.

The development of a cooperative program to help the Muslim population of a country face the real dimension and destructive results of suicide terrorism is critical to changing Muslim support. Religions have a new role to play, this time an educational one. An initiative by Uzbekistan's Tashkent Islamic University is an excellent model (Palazzi 2008, 58). One of its objectives is to train moderate religious scholars whose task will be to defuse religious fundamentalism and promote dialogue among all religions, including, of course, Muslims, Christians and Jews. This will help emphasize Islam's moderate message and build mutual trust and a common front in condemning suicide terrorism.

The media and Internet are powerful instruments and psychological weapons in the hands of the terrorists, but they can also be effective in counterterrorism. We could handle the media reports on suicide attacks in two ways. First — through required guidelines from experts — by limiting the quantity of news dedicated to terrorist attacks. Second, by attempting to discredit and de-romanticize their use of suicide tactics. If we carefully monitor jihadist websites and infiltrate their Internet chat rooms, we'll deny them the ability to reconfigure, survive and function as a global network. These actions could change the way some youths think. They could also change public opinion and recruitment, in broader terms. There are many indications that terrorist groups are facing difficulties in recruitment. The fact that they are recruiting children15 is not only a brutal shift in tactics — using people who don't raise suspicion — but it's also a sign that they are short of human resources (Ghazi 2007).

We have to focus on the psyche of would-be bombers to send the message that there is hope for a better solution and a peaceful way to settle disputes instead of killing themselves along with dozens of innocent people. We need to broadcast anti-suicide and anti-terrorism messages, promoting all the reasons that someone has to livefor not to die for. We have to fight the radical indoctrination by explaining the risks of terrorism and by proving that the "atrocious enemy" is human. This demands a very thorough understanding of the society to focus on, but also a well-prepared and applied public diplomacy. The objective isn’t to undermine their sacred values, but to convince them that the colonization era is over and that Western culture’s vision isn’t to exploit their natural resources, or political and religious oppression. The goal is to promote human rights and equality in economical, political, educational and social terms.

The fortification and use of advanced security measures to guard sensitive infrastructure isn’t enough to prevent suicide terrorism. NATO has to leverage “soft power” operations. Experts should study the plausible interactions between terrorism networks and organized crime. Educational programs for countering suicide terrorist ideologies should be considered in countries where migrants could be radicalized or influenced. These programs could extend into conflict zones through peacekeeping operations and reconstruction teams. Simultaneously, the West should minimize military action and apply a political and psychological strategy to thwart terrorist activities, adopting the “responsibility-to-protect” concept.

The future

The military offensive Israel launched on January 3, 2009, in Gaza has generated the next wave of Palestinian recruits, 16 which will bring into effect the “third intifada.” The revival of once-dormant suicide attacks in Russia and the Caucasus contradicts Vladimir Putin’s official declaration of the end of the Chechen War in April 2009 (Lyall 2010, 2). The failed suicide bombing attempt last December of a Nigerian on a Northwest Airlines plane17 en route to the United States fosters the perception of further evolution of suicide terrorism in terrorist groups’ operational planning.

Terrorist groups are not willing to disavow such an acute, effective and cheap strategic weapon. But they are searching for innovative technology that will be less costly to mujahedeen and martyrs. 18 Bergman (2008) expects a new insurgent strategy to emerge in two to five years, planned by “a new breed of highly educated al-Qaida terrorist.” Her words seem to be accurate, since the Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism warned that a nuclear or biological attack is likely to occur in a major city within the next five years. 19

Umar Hamza bin Laden, one of Osama bin Laden’s sons, was assigned to recruit children between the ages of 13 and 16 from West Africa, 20 especially Mauritania. On December 3, 2009, a Somali suicide bomber from Denmark killed more than 22 people, including four government ministers, at a graduation ceremony in Mogadishu. 21 In December 2009, five Americans (three of Pakistani, one of Egyptian and one of Yemeni descent) were arrested in Pakistan, suspected of links to terrorist groups. 22 All this points to Africa’s growing involvement in terrorism, but also to the significant attrition of recruits. The recruitment of foreign would-be bombers is critical.

Alas, suicide terrorists might develop even more brutal and atrocious tactics. Therefore, the international community must remain alert. In our versatile struggle against terrorism, we have to be ready and must realize that we can’t confront it solely through military means. Maybe the aerial bombings of cities, or dogmas such as “shock and awe,” are not proper responses to the more (or even less) violent terrorist tactics (Asad 2009, 20). We have to understand our enemy and deter and dissuade him from acting through radical violence. We have to exploit all means of soft power to thwart all aspects of terrorism.

Footnotes

1 Of the 2,622 martyrdom attacks that were carried out around the world in the period of 1981 through 2008, 2,218 attacks (84.5%) took place in 2004-2008.

2 17 countries in the period of 1981-2000, compared with 32 in the period of 2001-2008

3 Detailed data and annual analysis could be found in the reports of U.S. National Counterterrorism Center.

4 The elements of sacrifice and martyrdom are totally legitimate in the theory of the “cosmic war,” where the sacrificial victim represents the destruction endemic to battle. He has to fulfill criteria such as purity and anomaly, not married and free from family responsibilities, pious but not members of the clergy. The theory also includes the invention of an enemy if it doesn’t already exist. His demonization makes the confrontation procedure easier

and obvious, such as the conspiracy theories blaming the Jews for manipulating global politics and economy or the satanization of the Catholics by the Irish protestant leader the Rev. Ian Paisley.

5 “Abdallah Azzam the Wahabi Islamist whose most famous writing ‘In Defense of Muslim Lands’ became the basis for the defense of Afghanistan against the godless Soviet invasion, was Osama bin Laden’s mentor during his university years and inspired him to recruit the so-called Afghan Arabs…the event which played a seminal role in producing bin Laden’s destructive charismatic leadership. Qutb, Faraj and Azzam, all radical Sunni Muslims, were important forbears of bin Laden, Zawahiri and al-Qaida. At the same time, radical Shia theologians were sketching the basis for defensive jihad as well. Notable was Ayatollah Sayyid Muhammad Husayn Fadlallah, the spiritual mentor of Hezbollah, whose ingenious reinterpretation of the Quran provided the basis for suicide in the service of jihad, despite the prohibition against suicide, which is quite explicit in the Quran, while Muslim scholars have emphasized that anyone who commits suicide in the name of Islam is a kafir (=disbeliever).” (Ali and Post2008)

6 “In order to counter the strict prohibition against suicide, Fadlallah ingeniously equated death as a suicide bomber with soldiers entering the battle in which they knew that they would die, arguing there was no moral distinction and that the only difference was the time of death. He used this moral logic to justify suicide bombings by Shi’a forces as actions justified by oppression and the military asymmetric nature of the war against Israel.” (Ali and Post 2008)

7 A comprehensive study about recruitment of “would be” suicide bombers, as well as preparation and execution of attacks, is provided in Merari et al (2010b) (see list of references).

8 Qittal is the Arab word for fighting. According to Ali and Post (2008) “both terms, jihad and qittal, have significantly different meanings and uses in the Quran. Qittal involves killing and bloodshed and is only one aspect of armed jihad”.

9 From March 2003 to February 2006, 443 suicide attacks occurred in Iraq (Ali and Post 2008). Additionally, as of 2008, “more than 920 suicide bombings in Iraq and 260 in Afghanistan occurred after the U.S. invasions in 2001 and 2003 accordingly.” (Wright 2008)

10 Shay refers to the conflict of cultures, stressing that the ‘nomadic culture’ prevails not only in the indigenous population of these states but also in the terrorist entities such as al-Qaida, against the ‘state-oriented culture’ of the West.

11 This is a very frequent phenomenon mainly represented by Palestinians and the Chechen ‘Black Widows.’

12 The LTTE in Sri Lanka exploited that belief of the Hindu faith and used a lot of raped women as suicide bombers, who were seeking for expiation in their social and religious environment.

13 “The 1st wave occurred in Lebanon in the mid-1980s. The 2nd began on May 21, 1991, when a female member of the Liberation Tigers of Tamil Eelam assassinated former Indian Prime Minister Rajiv Gandhi after placing a garland around his neck at a political rally. Since the Gandhi assassination, the Tigers have used more female suicide bombers than any other militant group, reportedly deploying at least 46 women on suicide missions since 1991. From 1996 to 1999, the Kurdistan Workers’ Party, or PKK, carried out a series of attacks against Turkish military and police targets using female suicide bombers. From 2000 to 2004, female Chechen militants, often referred to as “Black Widows,” were involved in several suicide attacks against Russian military targets in Chechnya, civilian targets in Russia and an assassination attempt against the Chechen president. Abu Musab al-Zarqawi’s al-Qaida in Iraq got into the female suicide bomber business in late 2005, and Iraq is currently where female suicide operatives are used most frequently.” (Burton and Stewart 2007).

14 “The ‘Islamic State of Iraq’ — the al Qaeda-led jihadist group alliance — an-

nounced that it has formed a special all-female suicide bomber brigade and made an appeal for women to join it" (Burton and Stewart 2007). "Another woman, calling herself 'Um Osama', the alleged leader of the women mujahedeen of al Qaeda, was interviewed in 2003 and stated that their network claimed to have set up squads of female suicide bombers – purportedly including Afghans, Arabs, Chechens and other nationalities- under orders from bin Laden to attack the U.S." (Bloom 2007).

15 Researchers are reporting that al-Qaida tries to recruit children from refugee camps, many of whom have lost their families; it's even looking for mentally disabled kids, in order to raise them isolated from the rest of the world, except their leader, in order to use them as suicide bombers. See also Stratfor Global Intelligence. 2008. Al Qaeda: Creative Recruiting for Suicide Bombers, http://www.stratfor.com/analysis?page=48 (accessed November 28, 2008).

16 Statement during a personal discussion with an Israeli official in Macedonia, Greece, December 2009.

17 BBC News. 2009. Nigerian accused of attacking US passenger jet. BBC News (December 26, 2009), http://news.bbc.co.uk/2/hi/americas/8430699.stm (accessed December 27, 2009).

18 In one of the most important forums of al-Qaida, the website A17orya, intelligence services intercepted suggestions for new terrorist attack tactics, including the exploitation of technology, remote controls, vehicles, robots, model airplanes loaded with explosives, etc. The shortage of recruits is obvious, since they also examined the potential use of dogs suicide bombers, trained to recognize the US soldiers' uniforms (Bergman 2008).

19 See BBC News.2008. WMD strike 'likely' in five years. BBC News (December 4, 2008), http://news.bbc.co.uk/2/hi/americas/7762318.stm (accessed December 30, 2008).

See also CNN. 2008. Biological terror attack likely by 2013, panel says. CNN (December 2, 2008), http://edition.cnn.com/2008/US/12/02/terror.report/index.html (accessed December 24, 2008).

20 Stratfor Global Intelligence. 2008. Al Qaeda: Creative Recruiting for Suicide Bombers, http://www.stratfor.com/analysis?page=48 (accessed November 28, 2008).

21 See BBC News.2009. Somalia suicide bomber 'was from Denmark'. BBC News (December 10, 2009), http://news.bbc.co.uk/2/hi/africa/8406886.stm (accessed December 11, 2009).

22 See BBC News.2009. FBI investigates 'US arrests' in Pakistan. BBC News (December 10, 2009), http://news.bbc.co.uk/2/hi/south_asia/8405107.stm (accessed December 11, 2009).

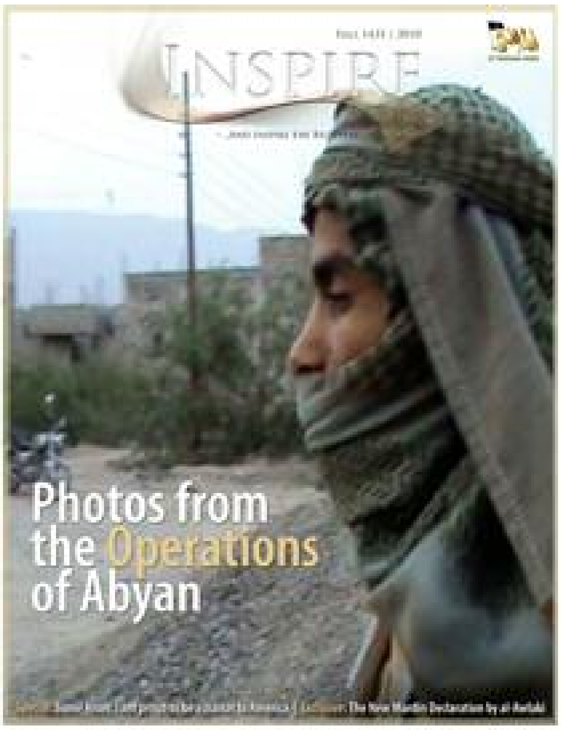
Ioannis Chapsos (Commander Hellenic Navy), Instructor at the Hellenic Supreme Joint War College (Security and Strategy Department). He is a George Marshall European Center for Security Studies alumnus Programe in Advanced Security Studies-Germany).He holds an MA in 'Terrorism, International Crime, Global Security' from Coventry University (UK). He is a Phd Candidate in 'Global security and Media'in Aristotle University of Thessaloniki- Journalism and Media department.

Inspire Al-Qaeda in the Arabian Peninsula (AQAP) Magazine

Source: http://publicintelligence.net/complete-inspire-al-qaeda-in-the-arabian-peninsula-aqap-magazine/

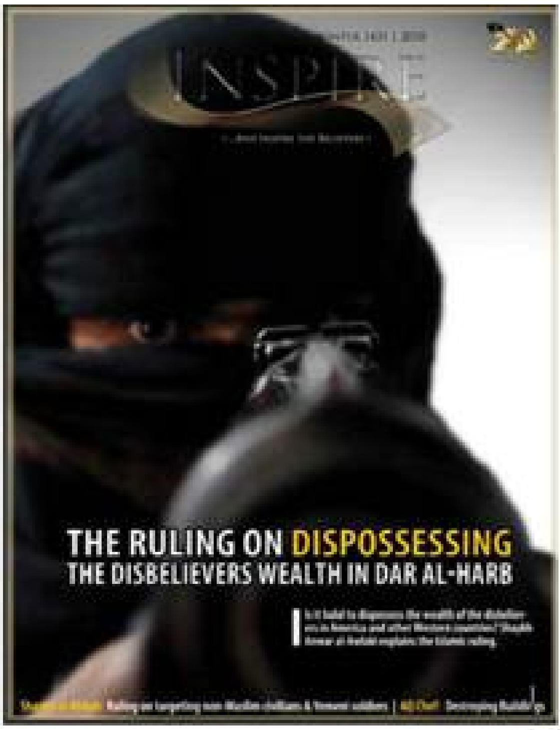
INSPIRE
May Our Souls be Sacrificed for You!
Shaykh Anwar al-'Awlaki
Exclusive Interview with Shaykh Abū Basīr
Make a Bomb in the Kitchen of your Mom
The AQ Chef
Asrar al-Mujahideen 101
The West should ban the Niqāb Covering its Real Face
Yahya Ibrahim
What to Expect in Jihād | 4 Calls of al-Anfāl | Jihādi Experiences

No1 (Summer 2010)



No2 (Fall 2010)

No 3 (Nov 2010)


INSPIRE
THE RULING ON DISPOSSESSING THE DISBELIEVERS WEALTH IN DAR AL-HARB

No 4 (Winter 2010) – latest issue

Available to download in .pdf format:
Source: http://abcnews.go.com/Blotter/issue-al-qaeda-inspire-magazine/story?id=12632256
By Matthew Cole

The latest edition of al Qaeda's English-language web magazine offers readers a new fatwa from American-born jihadi leader Anwar al-Awlaki, instructions on how to destroy buildings using gas lines, and a primer on the AK-47 rifle, in what is «Inspire»'s slickest production to date. The fourth issue of «Inspire» a publication of al Qaeda in the Arabian Peninsula (AQAP), the terror organization's Yemeni branch, follows three previous installments in the past year that gave instructions on the killing American civilians, and boasted about the failed «printer bomb» cargo plane plot that originated in Yemen. A young American citizen from North Carolina named Samir Khan apparently began editing and publishing the on-line magazine after relocating to Yemen. In this edition, Yemeni-American radical cleric Awlaki issues a religious justification for taking money and property from Americans and citizens of other Western nations.

Awlaki is at the top of the U.S. government's «kill list» because of his operational involvement in AQAP. Awlaki's message appears intended to assuage any concerns that American and European jihadis might have about resisting taxes and stealing from corporations. «Some Muslims today might feel uncomfortable consuming money that was seized by force from the disbelievers and would feel that income they receive as a salary or from business is a better form of income,» Awlaki writes. «That is not true. The best and purest form of income is booty.»

Pirates Hijacked a Record Number of Ships and Crew Last Year

Source: http://www.bloomberg.com/news/2011-01-18/pirates-hijacked-record-53-ships-in-2010-mostly-off-somalia-imb-reports.html

Pirates hijacked a record number of ships and crew in 2010, most of them off Somalia, the International Maritime Bureau reported. A total of 53 vessels were captured, with 1,181 crew members taken hostage and eight killed, the London-based unit of the International Chamber of Commerce said in an e-mailed report. That's up from 188 people seized in 2006, the IMB said. "These figures for the number of hostages and vessels taken are the highest we have ever seen," Captain Pottengal Mukundan, director of the IMB's Piracy Reporting Centre, which has monitored piracy since 1991, said in the report. "The continued increase in these numbers is alarming." Ransoms paid to Somali pirates averaged $5.4 million last year, compared with $150,000 in 2005, according to One Earth Future, a non-governmental organization based in Louisville, Colorado. A total of $238 million was paid out in 2010, the group said in a report, estimating the annual cost of piracy at $7 billion to $12 billion. That includes ransoms, insurance premiums, re-routing ships, security equipment and naval forces. Somali pirates still held 28 ships and 638 hostages as of Dec. 31, the IMB said. Pirate attacks also took place in Nigeria and Bangladesh and Indonesia reported its highest level of attacks on ships since 2007, the IMB said.

Iranian suicide-bombing book found in Arizona desert

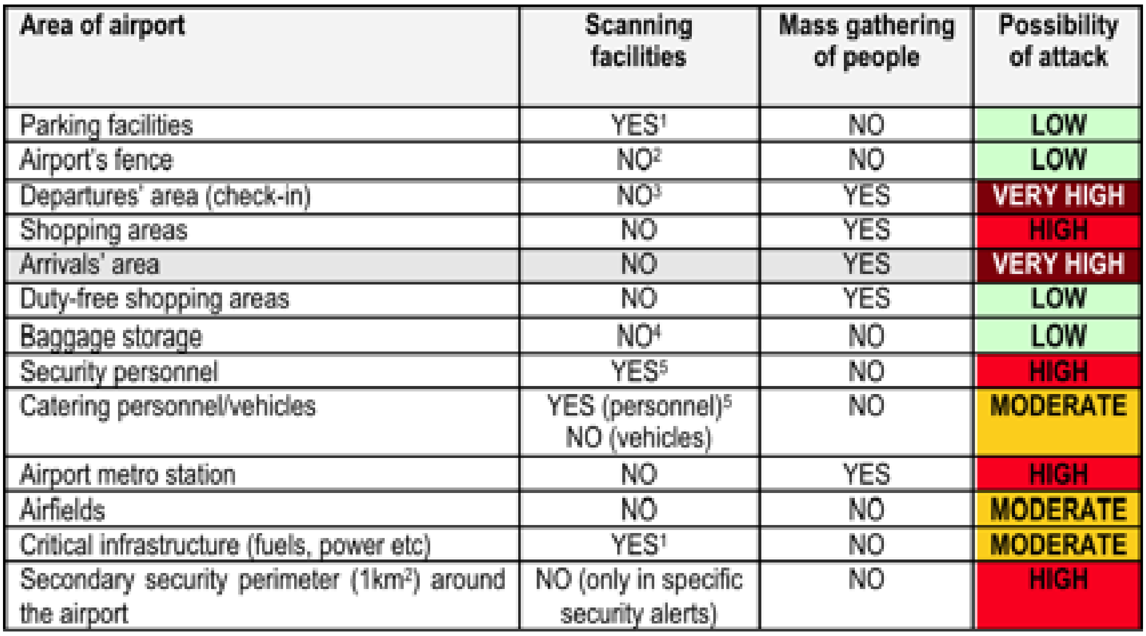
Source: http://homelandsecuritynewswire.com/iranian-suicide-bombing-book-found-arizona-desert

A book celebrating suicide bombers has been found in the Arizona desert just north of the U.S.- Mexican border; last year DHS had in custody thousands of detainees from Afghanistan, Egypt, Iraq, Iran, Pakistan, Saudi Arabia, and Yemen; U.S. Border Patrol statistics indicate that there were 108,025 OTMs — or illegal immigrants other than Mexicans — detained in 2006, compared to 165,178 in 2005 and 44,614 in 2004. A book celebrating suicide bombers has been found in the Arizona desert just north of the U.S.-Mexican border, authorities told Fox News. The book, In Memory of Our Martyrs, was spotted Tuesday by a U.S. Border Patrol agent out of the Casa Grande substation who was patrolling a route known for smuggling illegal immigrants and drugs. Published in Iran, it consists of short biographies of Islamic suicide bombers and other Islamic militants who died carrying out attacks. According to internal U.S. Customs and Border Protection documents, "The book also includes letters from suicide attackers to their families, as well as some of their last wills and testaments." Each biographical page contains "the terrorist's name, date of death, and how they died." Agents also say that the book appears to have been exposed to weather in the desert "for at least several days or weeks." Authorities told Fox News that there were no people in the area at the time the book was found, and no arrests have been made in connection with it. "At this time, DHS does not have any credible information on terrorist groups operating along the Southwest border," a DHS official said in a statement. "We work closely with our partners in the law enforcement and intelligence communities and as a matter of due diligence and law enforcement best practice, report anything found, no matter how significant or insignificant it may seem." Fox News reports that statements from U.S. officials, including FBI director Robert Mueller, have raised serious concerns in recent years over "OTMs" — or illegal immigrants other than Mexicans — who have crossed the southwest border at alarming rates. Mueller testified before the House Appropriations Committee in March 2005 that "there are individuals from countries with known al Qaeda connections who are changing their Islamic surnames to Hispanic-sounding names and obtaining false Hispanic identities, learning to speak Spanish and pretending to be Hispanic." Just last year, DHS had in custody thousands of detainees from Afghanistan, Egypt, Iraq, Iran, Pakistan, Saudi Arabia, and Yemen. U.S. Border Patrol statistics indicate that there were 108,025 OTMs detained in 2006, compared to 165,178 in 2005 and 44,614 in 2004. Authorities would not release a picture of the book to Fox News, or reveal how long they believe it was lying in the desert. Immigration officials have previously discovered items along the U.S.-Mexico border from Middle Eastern origin, including Iranian currency in Zapata, Texas, and a jacket found in Jim Hogg County, Texas, that was covered in patches including an Arabic military badge that illustrates an airplane flying into a tower.

A quick airport security vulnerability check

Source: The Editor

The reason behind this table is a personal question: "Why are terrorists always a step ahead of all of us?" Current answers: "It will not happen to us!", "we have everything under control!" or "who do you think you are?" And then it happens in Moscow or Glasgow or in other places in the world… Why surprised then?



Area of airport	Scanning facilities	Mass gathering of people	Possibility of attack
Parking facilities	YES[1]	NO	LOW
Airport's fence	NO[2]	NO	LOW
Departures' area (check-in)	NO[3]	YES	VERY HIGH
Shopping areas	NO	YES	HIGH
Arrivals' area	NO	YES	VERY HIGH
Duty-free shopping areas	NO	YES	LOW
Baggage storage	NO[4]	NO	LOW
Security personnel	YES[5]	NO	HIGH
Catering personnel/vehicles	YES (personnel)[5] NO (vehicles)	NO	MODERATE
Airport metro station	NO	YES	HIGH
Airfields	NO	NO	MODERATE
Critical infrastructure (fuels, power etc)	YES[1]	NO	MODERATE
Secondary security perimeter (1km^2) around the airport	NO (only in specific security alerts)	NO	HIGH

[1] CCTV surveillance – occasional security patrolling

[2] With the exception of certain airports i.e. Ben Gurion International Airport

[3] With the exception of certain airports i.e. Ben Gurion International Airport

[4] With the exception of certain airports i.e. Terminal 5 Heathrow Airport – in general: availability of detection equipment

[5] Simple security cards – bar-coded to the best

Nedžad Balkan: The Face of Southeastern Europe's Newest Radical Threat

Anes Alic

Source: http://www.jamestown.org

MILITANT LEADERSHIP MONITOR
Personalities Behind the Insurgency

A Vienna-born Serbian Muslim named Nedžad Balkan (a.k.a. Ebu Muhammed) is believed to have been behind the most recent terror attack in the central Bosnian town of Bugojno, and his connection to Bosnia and Herzegovina signals the rise of a new and avowedly violent sect of Wahhabis that has regional intelligence agencies on alert.

Nedžad Balkan, born in Vienna, Austria, is the son of Bosniaks from Serbia's predom nately Muslim Sandžak region straddling the border of the Republic of Montenegro. A former boxer and night club bouncer in his younger days, Balkan, now in his mid-30s, is the leader of the Sahaba Mosque in Vienna's Seventh bezirk (district) and the alleged financier of the Serbia-based Sandžak Wahhabis.

Similar to many regional Wahhabi clerical leaders, Balkan studied at the Islamic University in Medina, Saudi Arabia in the early 1990s. Reportedly disappointed with the insufficiently Islamist politics of the Saudi regime, Balkan departed before graduating. Upon his return to the West, Balkan preached at Vienna's al-Tawhid mosque, but left due to a disagreement with another radical cleric and purported leader of the Bosnian Wahhabis, Muhamed Porča, [1] and other members of the mosque. [2]

Importantly, intelligence sources believe that Balkan is the leader of the Bosnian and Serbian Takfiri followers. Takfiri ideology is classified as a violent offshoot of the Salafi movement, sanctioning acts of violence, particularly against fellow Muslims, as legitimate methods of achieving religious or political goals. Takfiris believe that one who deliberately kills himself whilst attempting to kill his enemies is a martyr and ascends directly to heaven. The followers of Takfiri ideology believe in violence against everyone who is not as devout a Muslim as they, and they refuse to recognize the secular authority of the Bosnian legal system.

Unlike other radical Islamist groups in Bosnia, most of them founded as the remnants of various organizations operating during the 1992-1995 Bosnian war and which profess more of a "missionary" objective, the members of the Takfiri ideology advocate violent clashes with peer competitors who profess differing objectives.

Aside from the recent terrorist attack on a police station in the Bosnian city of Bugojno, in which one police officer was killed and which intelligence officials believe was orchestrated by Balkan, the former boxer has a rather full police record. In 2005, Balkan was placed under observation by the Austrian police for publicly condoning the July 7, 2005, London bombings and for making extremist statements to the Austrian press.

In 2006, Balkan, along with six other Wahhabis (three of them Austrian citizens), was involved in the beating of Bosnian Serb Mihajlo Kisic in the Bosnian city of Brcko. After a short trial, the seven attackers were given symbolic sentences and released on parole. Some of them returned to Vienna. In 2007, the Sahaba Mosque also came under scrutiny during the terror investigation of Bosnian Muslims who tried to attack the American Embassy in Vienna in 2007. In 2008, the Sahaba Mosque was placed under surveillance when it became known that the suspected producer of a video threatening violence against the Austrian Government frequented the prayer room.

Balkan is also believed to be a religious authority for several radical groups from Bosnia and Serbia. Balkan leads the Vienna-based Kelimetul Haqq organization of Bosnian and Serbian Muslims, which belongs to the Al-Takfir w'al-Hijra movement (BH Dani [Sarajevo], August 12, 2008).

The group, which has a "branch office" in the Montenegrin half of the Sandžak region, has been publishing sermons online advocating an aggressive posture. Kelimetul Haqq is actively promoting the concept of armed jihad and disseminating Islamist videos and diatribes. [3] It has also become very vocal about Bosnia and Herzegovina, decrying the Islamic community there as comprised of people who are not "true believers."

On June 27, 2010, a terrorist set off a bomb at the Bugojno police station, some 70 kilometers southwest of Sarajevo. One police officer was killed in the attack and six others were wounded (AFP, June 28, 2010). Five people were indicted on terrorism charges in connection with the attack. Today, prosecutors are focusing more on the international aspect of the case. Leads in the investigation show that the attack may have been organized by Balkan from abroad, as he is believed to be leading a new generation of jihadists that may be overstepping their local Wahhabi brethren who have, so far, focused mostly on attempting to interfere with the moderate Islamic Community of Bosnia.

One suspect in the June 2010 bombing, Haris 'Oks' Causevic, from Bugojno, confessed to having placed a bag with 15 kilograms of explosive material against the back wall of the police station, setting it off and attempting to flee before being seized by police. While attempting to escape, he also threw a grenade at police officers.

In the last few years, Causevic, a computer expert, had become more active in online forums, using the nickname "Oks 315." He is believed to have sabotaged several "secular" websites, including government ones (Start magazine, December 28, 2010).

Another suspect, Bosnian Naser Palislamovic, is believed to have organized the attack on the Bosnian side. Investigators believe that he hired Causevic, his brother-in-law, to carry out the attack. Three others were indicted for supplying the explosives.

Bosnian police and intelligence officials claim that both Palislamovic and Causevic received instructions to bomb the Bugojno police station from Vienna, where the leader of Bosnian and Serbian Takfiri followers resides. In the ongoing investigation, police established that Causevic and Palislamovic traveled several times to Vienna during the past two years and visited the mosque run by Balkan.

While the motive behind the June terrorist attack was most likely revenge for the arrest of the Rustempasic brothers and others currently being tried for terrorism and illegal trafficking of weapons and military equipment (Dnevni Avaz [Sarajevo], July 4, 2010), it reveals a dangerous new trend: the rise of a new sect within the Balkan region's Wahhabi movement, which through its intolerant and violent activism is threatening to further endanger the country's security and also to provoke incidents between Bosnia's moderate Muslims and followers of an illiberal, Saudi-inspired Wahhabi ideology.

Currently, there are two ongoing terrorism trials in Bosnia – both of them linked to Balkan and his congregation. All the key defendants – Causevic and Palislamovic, charged in the Bugojno attack, and Rijad and Muhamed Rustempasic, charged with illegal possession of dangerous materials - were frequent visitors to Balkan's mosque, while Muhamed Rustempasic lived in Vienna.

In October 2009, Bosnian border officers arrested Muhamed Rustempasic on suspicion of trafficking weapons from Austria and Germany to radical groups in Bosnia. Shortly before that, his brother, Rijad Rustempasic, and the three members of his group - Muhamed Meco, Abdulah Handzic and Edis Velic - were arrested and indicted for terrorism. All three were members of the El-Mujahid unit, headquartered in central Bosnia, and following the 1992-1995 Bosnian war they are said to have spent time in Jordan, Saudi Arabia and possibly Chechnya.

A Jamestown source from the Bosnian prosecution said last year that investigators suspected that Muhamed Rustempasic supplied his brother Rijad with most of the military equipment confiscated in the Sarajevo and Bugojno raids. Given the fact that Muhamed is unemployed and lives in Vienna with his wife and two children, the prosecution plans to open an additional investigation in coordination with Austrian authorities, which should lend more insight to the group's financial situation as well as into Balkan's true capabilities.

The police have concluded that the group was specifically planning to target the Sarajevo central cathedral and the Franciscan monastery in the central Bosnian city of Fojnica. Aside from Catholic institutions, police also have reason to believe that the group was planning to sabotage electricity supply stations and launch attacks against European Forces (EUFOR) in Bosnia.

It is clear that Bosnian security agencies will face an uphill battle in preventing any further attacks similar to Bugojno, despite the fact that many of the country's most radical Muslim activists are under surveillance. The Bugojno attack showed that the new generation of radicals is keen to make its presence felt and has no qualms about violent attacks on institutions they despise, including the Bosnian state, the country's traditionally moderate Muslims and the Bosnian Islamic community, as well as all others who do not share their religious views. The additional problem for Bosnian security forces and its citizens is that such attacks could happen anywhere and would require only basic organization and modest resources. The bomb used for the police station attack was made out of explosives collected by Causevic and Rijad Rustempasic, who visited former 1990s-era front lines looking for unexploded ordinance (Oslobodjenje [Sarajevo], July 1, 2010).

Until recently, all attention had been on Porča, considered the paramount Bosnian Islamist. Porča's activities, however, seem rather amateur in comparison to those of Nedžad Balkan. Today, Balkan appears to have sidelined Porča – a process that began when he parted with the cleric in 2005. Today, Nedžad Balkan is the new face of an openly violent jihadi group that creates bad news for his geographical namesake in southeastern Europe.

Notes:

1. For a biography of Bosnian Islamist Muhammed Porča, see Anes Alic, "Muhammad Porča: The Man Behind Bosnia's Wahhabi Movement," Militant Leadership Monitor, July, 2010.
2. See Juan Carlos Antúnez, Wahhabism in Bosnia-Herzegovina-Part One, Section 4, Part B, Section II, Bosnia Report, September 16, 2008, Bosnian Institute
3. Ibid.

Anes Alic is the Executive Director of ISA Consulting, www.isaintel.com

Canadian border poses bigger terror threat to U.S. than Mexico border: report

Source:http://www.nydailynews.com/news/national/2011/02/02/2011-02-02_canadian_border_poses_ bigger_terror_threat_to_us_than_mexico_border_report.html#ixzz1CtDLZ9DG

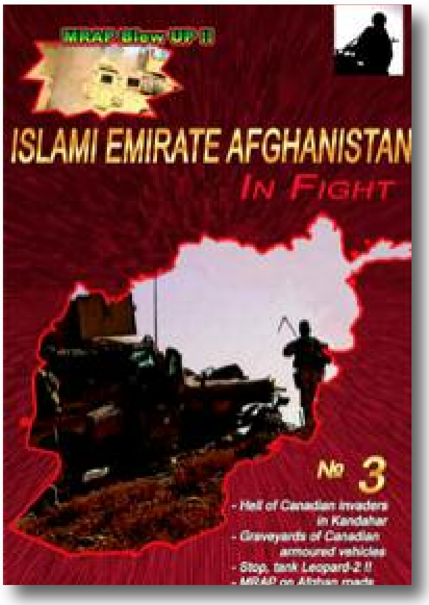
Worried about terrorists sneaking into the United States? You might want to look north. It turns out that even as Mexico grapples with drug and gang violence, the U.S.-Canadian border poses a bigger terror risk, according to a new government report. Just 32 of the 4,000 miles - less than 1% - along the northern border have an «acceptable level» of security, according to the Government Accountability Office report, released Tuesday. Sen. Joe Lieberman (I-CT) called the report «absolutely alarming» during a news conference on Capitol Hill. He fears the northern border provides «easy passage into America by extremists, terrorists and criminals whose purpose it to harm the American people.» Sen. Susan Collins (R-ME), who released the report alongside Lieberman, said potential crossers include illegal immigrants, criminals trafficking humans and drugs, and, potentially, terrorists. The report by the watchdog arm of Congress said federal officials can only detect illegal border crossings along 1,007 miles of the border, and blasted federal agencies for not cooperating with each other. It also found that illegal crossings by terrorists are more likely to occur across the northern border than the southern border. A spokesman for the Department of Homeland Security said the agency has taken steps to secure the northern border, like deploying more border patrol agents and adding better technology and infrastructure. He also said the department was working to address the GAO's findings. Collins called the report «shocking» and said Homeland Security was distributing money to the southern border «to the detriment» of the

northern border. «It is very clear from this report that the United States remains very vulnerable,» she said. Some members of the Canadian Parliament shrugged off U.S. worries. Immigration Minister Jason Kenney told The Canadian Press that his country has worked hard to improve security along the border and that added measures would simply hamper trade and travel between the two countries.

Afghan Taliban issue guidelines for establishment of Islamic Emirate

Source: http://www.jamestown.org

One of the major weaknesses of most militant Islamist groups is their almost complete lack of a political program or consideration of how an Islamic State should be run beyond a general commitment to Shari'a and the creation of an Islamic caliphate. Details as to how this caliphate is to be administered or who is to be its leader are rarely considered by militants. The last Caliph, Abdul Mejid II, was deposed by Turkish secularist Mustafa Kemal "Ataturk" in 1924. A notable exception to this trend is Afghanistan's Taliban movement, which actually has experience running a country, as it did in Afghanistan from 1996 to 2001. The Afghan model as pursued by the Taliban is more realistic in seeking an Emirate (a regional command) rather than a Caliphate (the latter encompassing the entire Islamic world).


MRAP Blow UP !
ISLAMI EMIRATE AFGHANISTAN
IN FIGHT
№ 3
- Hell of Canadian invaders in Kandahar
- Graveyards of Canadian armoured vehicles
- Stop, tank Leopard-2 !!
- MRAP on Afghan roads

Nevertheless, the Emirate is "based upon the principles of the Islamic Caliphate… in dividing the country into provinces, appointing pious and righteous governors, guiding workers to piety and justice, encouraging the establishment of a religious and worldly policy, tending to the needs of the people, instructing them in matters of religion and encouraging them to make the utmost effort in promoting virtue and preventing vice."

Discussion of the Taliban's administrative plans for Afghanistan has been stirred by a detailed outline of these plans in the movement's *Voice of Jihad* website (January 27). The outline, written by Ikram Miyundi, was previously published in the movement's *al-Somood* Magazine (Issue 55, December 25, 2010).

For guidance, the Islamic Emirate must draw on the Koran, the Sunnah (sayings and habits) of the Prophet Muhammad, the Sunnah of the Khulafa ur-Rashidun (The Caliphs of Righteousness, i.e. the first four caliphs after Muhammad), the sayings of the Companions (of the Prophet), as well as various fatwas (religious-based legal decisions) issued by respected scholars of Islam.

Administratively, the Emirate divides Afghanistan into 34 provinces, which are in turn divided into directorates and villages:

- The village is run by a leader appointed by the Emirate who is responsible for civilian and military affairs. In this he is assisted by a group of ten to 50 mujahideen.
- The directorate is administered by a governor «of known piety» who is assisted by a deputy familiar with the region. Under them are committees dealing with dispute resolution, education, development and local military affairs.
- Provincial administration is handled by a governor, «a man of religion and morality who fears no one but Allah,» and a deputy. The governor directs the province's military, civilian, financial and legal affairs and is responsible for the implementation of Shari'a laws and statutes. The governor is appointed and dismissed by the Supreme

Commander after consultation with the High Shura Council.

Just below the High Shura Councils are the "Main Committees," which in effect replace the existing ministries of the Afghan government. These include:

- The Military Committee – Overseeing the mujahideen and replacing the Ministry of Defense.
- Preaching and Guidance Committee – Senior scholars issuing fatwas and advice on matters of Islamic jurisprudence.
- Culture and Information Committee – Responsible for broadcasting statements of the Amir al-Mu'minin and other government directors. This committee is also responsible for news dissemination and refuting claims of enemies of the Emirate on internet websites.
- Political Committee – Replaces the Foreign Ministry.
- Education Committee – Responsible for spreading "Islamic and contemporary learning."
- Financial Committee – Responsible for all financial affairs and resources.
- Committee for Prisoners and Orphans – Works for the release of mujahideen prisoners and provides resources for the upbringing of their children and the children of martyrs.
- Health Committee – Responsible for treating wounded and sick mujahideen.
- Committee for Foreign Establishments – This committee directs the operations of foreign relief and aid agencies and makes sure they do not do anything contrary to Islamic theology and beliefs.

Directing the committees is the High Shura Council, appointed by the Amir al-Mu'minin and responsible for drafting laws and regulations in accordance with Islamic principles.

At the peak of the administration is the Amir al-Mu'minin (Commander of the Faithful): "The leader is the axis around which matters pivot. He employs the community to achieve his goals and directs people to goodness and happiness. He warns them against evil and danger according to his lights." The Amir must be male, of sound mind and emotion, and possess the qualities of knowledge, vision, strength, courage and wisdom. He must have excellent organizational skills as well as other qualities mentioned in the existing books of *fiqh* (Islamic jurisprudence) and '*aqidah* (Islamic theology).

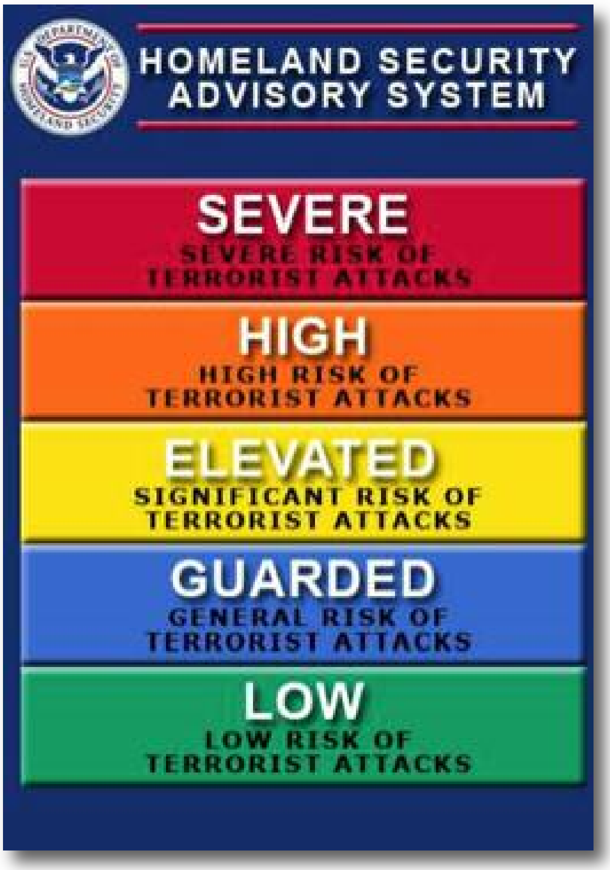
This title, first used by the second Caliph, Umar ibn al-Khattab, has been used in various capacities by both the Sunni and Shiite communities. It became widely used by the leaders of the Sahelian sultanates in Africa (such as Darfur) and continues to be used by the Sultan of Morocco. Mullah Omar has used the title since founding the Taliban in 1994.

End of Color-Coded Threat Alert System Widely Welcomed

Source: http://www.globalsecuritynewswire.org/gsn/nw_20110128_8078.php

U.S. Homeland Security Secretary Janet Napolitano yesterday formally did away with the agency's much maligned color-coded threat advisory system to the approval of lawmakers and security experts.

«Because of the trust we have in Americans to share in our collective security, today I would like to announce the end of the old system of color-coded alerts,» Napolitano said in her first «State of Homeland Security» address. «In their place, we will implement a new system that is built on a clear and simple premise: when a threat develops that could impact you, the public, we will tell you. We will provide whatever information we can so you know how to protect yourselves, your families, and your communities.» The previous system, which used five colors to convey threat levels, was initiated shortly after the department was stood up in 2002. It has been widely criticized for being overly vague when a potential threat did arise. The threat color level has largely not changed since 2006. The threat is set in the middle at yellow, or elevated, although federal officials put the level to the airline sector at orange, meaning high. Yesterday marked the beginning of a 90-day implementation period to help state and local governments, law enforce, airports, transport hubs and others switch over to the new system. Under the new two-tiered structure, Homeland Security would coordinate with other federal entities to issue formal, detailed alerts regarding information about a specific or credible terrorist threat, according to Napolitano. «These alerts will include a clear statement that an 'imminent threat' or an 'elevated threat' is present,» she said the event sponsored by George Washington University's Homeland Security Policy Institute. In language that mirrored the department press release on the decision, Napolitano said the new alerts would also «provide a concise summary of the potential threat, information about actions being taken to ensure public safety, and recommended steps that individuals and communities can take.» An alert could be limited to a particular audience, such as law enforcement, or a segment of the private sector, such as shopping malls or hotels, Napolitano told the audience. It also could be issued more broadly to the general population, distributed through a DHS statement, the media or social networks, she added. The alerts might urge certain responses to a situation or call on people to watch for particular types of questionable behaviour, according to Homeland Security. In addition, the alerts «will have a specified end date. You can clap on that one. Yeah, that's all right,» Napolitano joked to laughter and applause from the audience. News of the move was welcomed on Capitol Hill. «The new system of homeland security alerts will be more easily understood and more helpful than the existing color-coded system,» Senate Homeland Security and Governmental Affairs Committee Chairman Joseph Lieberman (I-Conn.) said yesterday in a statement to Global Security Newswire. «The alerts may be sector specific or national, and will contain guidance to help the American people protect themselves against the particular threat contained in the alert.» House Homeland Security Committee Chairman Peter King (R-N.Y.) issued a statement on Wednesday saying that the proposed changes «make sense.» Ranking panel Democrat Bennie Thompson (Miss.) also praised the decision to scrap the old system. «The old color-coded system taught Americans to be scared, not prepared,» he said in a statement. Homeland security experts also hailed the decision to do away with the rainbow approach. «The old system didn't really help you in any way. It didn't tell people what the threat was. Most importantly, it didn't tell people what to do or what to be on the lookout for,» said Rick Nelson, director of the Homeland Security and Counterterrorism Program at the Center for Strategic and International Studies. «Simply saying there's an elevated level of terrorist threat is just useless information,» he told GSN yesterday in a telephone interview. Nelson cited the America's Missing: Broadcast Emergency Response system, commonly known as AMBER Alert, as an successful program because it lets people know

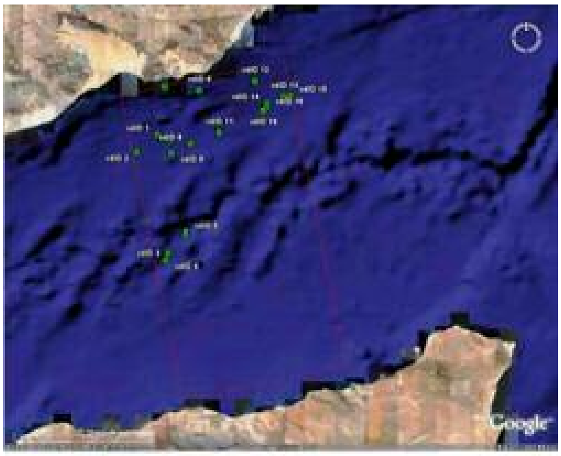

HOMELAND SECURITY
ADVISORY SYSTEM
SEVERE
SEVERE RISK OF TERRORIST ATTACKS
HIGH
HIGH RISK OF TERRORIST ATTACKS
ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS
GUARDED
GENERAL RISK OF TERRORIST ATTACKS
LOW
LOW RISK OF TERRORIST ATTACKS

to look for an abducted child; provides information, such as the model and color of a vehicle; and gives them a phone number to call. «If you can equip your general population with useful information that they can use to protect themselves, or use to help mitigate the threat, then it's a force multiplier,» Nelson said. The color-code system had «served its purpose» and was useful in the early days of the Homeland Security Department, according to former DHS Assistant Secretary Randy Beardsworth, a principal of Washington-based Catlayst Partners. «When the department was first stood up, there was no common language of what preparations should be or what measures should be in place to mitigate risk,» said Beardsworth, who also was a member of the joint task force that examined replacing the color-code system. «The system helped agencies at the federal, state and local levels» to prepare across the various threat levels. He noted that over time the system became more tailored to particular threats, including a 2004 warning to the New York and New Jersey financial sectors. However, the system was not particularly effective at informing the public of what it was supposed to do regarding a threat, Beardsworth told GSN this morning. The new tiered scheme will be more nuanced than its predecessor, so its success will rest on how well Homeland Security and the federal government communicate with law enforcement officials at the state and local levels, he predicted. The color-code system was a «clumsy response» to the dilemma the Bush administration faced in being the first White House to address the country's heightened homeland security imperative following the September 11 attacks, according to Stephen Flynn, president of the Center for National Policy. «The only thing that's kept it going is the politics of retreat, the sense that somehow eliminating a flawed system would indicate a lack of seriousness about dealing with the threat itself, instead of a frank acknowledgment that we often do rash things in response to new crises and they deserve to be re-examined when we have the benefit of a calmer moment,» he said yesterday. While the new DHS system is an improvement, it does not engage the U.S. public about what they must do to deal with terrorist threats, according to Flynn. The new alert program is «geared toward professional protectors, the folks who have an explicit obligation to deal with safety or security,» he said. «As we've seen time and again, most recently with the incident in Tucson, Ariz., the first responders are almost always bystanders, the neighbours and the family,» Flynn added, referring to the January 8 shooting of U.S. Representative Gabrielle Giffords (D) and more than a dozen others. Still, Flynn and the others doubt the color-coded approach would ever make a comeback. «I don't think there's anybody out there except for maybe late-night talk show comics who will miss the opportunity to play with the colors,» he said.

Pirate attack prediction model developed

Source: http://homelandsecuritynewswire.com/pirate-attack-prediction-model-developed

A mathematician has developed a piracy prediction model based on wind, waves, currents, as well as on the ground intelligence that could help predict the probability of a pirate attack on a given day; the system would function like a tornado warning system using weather data to project high risk areas on a map; the map could be further refined by adding in real time shipping traffic to indicate which ships are most likely to be attacked; piracy has grown worse in the last year, despite stepped up naval patrols; 80 percent of the world's cargo still travels by sea. A math-



ematician has developed a piracy prediction model based on wind, waves, currents, as well as on the ground intelligence that could help predict the probability of a pirate attack on a given day. James Hansen, an applied mathematician with the U.S. Naval Research Laboratory, believes that by compiling weather data and an understanding of pirate behavior he has developed a pirate warning system. According to Hansen, "It's sort of like tornado warnings." Just as meteorologists can fairly accurately predict the likelihood that a tornado will appear or head in a certain direction, Hansen believes his model could do the same for pirate attacks. "These guys are running around in tiny ships," Hansen said, which means that it is difficult for them to operate in rough seas making good weather critical for their ability to sail. Hansen's model would generate a map that shows the highest-risk areas and could be of further use by adding up to the minute on shipping traffic to identify likely targets for pirates. Gordan Van Hook, senior director for innovation and concept development for shipping giant Maersk Line Limited, said that the high profile 2009 hijacking of the cargo ship Maersk Alabama occurred on a calm day in April. In response to Hansen's model, he said, "If they would publish areas that are highly likely to have pirate activity, that would be valuable." The world's navies are struggling to protect ships sailing through the Indian Ocean, especially in areas around the Horn of Africa and the Straits of Malacca. Securing these shipping lanes is critical as 80 percent of the world's cargo still travels by sea, and a majority of ships must pass through these areas. Pirate attacks have increased, despite a fleet of forty warships from thirty countries patrolling the waters near Somalia. The Seattle Times reports that last year there were nearly 450 attacks, with 53 ships captured and an economic cost of $10 billion. In 2009 there were a total of 406 attacks by pirates. Hansen presented his findings at the American Meteorological Society meeting, which was held from 23 January to 27 January in Seattle.

Making 3-D face from 2D photo for security applications, forensics

Source: http://www.sify.com/news/making-3-d-face-from-2d-photo-for-security-applications-forensics-news-scitech-lbunaqdfdci.html

Scientists have found that it is possible to construct a three-dimensional face from flat 2D images. The discovery could be used for biometrics in security applications or in forensic investigations. Biometrics is the technology of performing personal identification or authentication via an individual's physical attributes. Xin Guan and Hanqi Zhuang of Florida Atlantic University on Boca Raton explain how Biometrics is becoming an increasingly viable solution for identity management, information protection and homeland security. They have developed a computer algorithm that can analyze the viewing angle and illumination of a face in an image and generate a 3D view of the face based on the results. A 3D image of a person's face might be used in biometrics alongside or instead of fingerprint, iris, face, voice and DNA, recognition techniques for so-called identity management and in security, coupled with smart cards and passwords computer recognition of a real face based on a 3D version of known personnel in a security database could be used to reduce false identification. The same technique might also be applied to analysis of security footage from CCTV cameras in crime investigation or in searching for missing persons. Ultimately, the same technology might also be adapted by the entertainment industry where 2D images of famous people from the past might be rendered in 3D and so allow a face to be animated. The study result has been published in the International Journal of Biometrics this month. (ANI).

The Negative Effects Of Watching Terror Coverage On TV

Source: http://www.medicalnewstoday.com/articles/215072.php

Viewing TV coverage of terrorist events causes deterioration of psychological resources, such as commitment and a sense of success, and to feeling threatened, which in turn can also lead to loss of resources and other negative affects. This has been found in a new study at the University of Haifa. «Mass media plays a central role in reporting on terrorism and political violence. The present study shows that watching this type of coverage on television has negative effects, even for someone who was not at all involved in an event being viewed,» said Prof. Moshe Zeidner, who headed the study.

40 PEOPLE HELD HOSTAGE INSIDE TRIDENT
MUMBAI UNDER SIEGE 101 KILLED IN ATTACK
TAJ, TRIDENT & NARIMAN HOUSE TARGETED
LIVE
WAR ON MUMBAI
CAR NOs
WAR ON MUMBAI
Smoke coming out of Taj Hotel
NDTV LIVE
WARZONE MUMBAI
PM ADDRESSES NATION ON ATTACKS IN MUMBAI
INDIA'S 9/11

The current research, which Prof. Zeidner conducted with Prof. Hasida Ben-Zur and Shlomit Reshef, set out to examine whether exposure to television reportage of terror events or political violence toward Israelis could pose some form of «indirect threat» on the viewer, even if he or she had no involvement in the event, and whether such an indirect threat might weaken the viewer's psychological resources - much like a direct threat would do. 78 students took part in the study, representing the diverse cultural sectors of Israeli society. Of these students, 39 watched video clips of terror attacks or political attacks on Israelis, as broadcast in the news over the past decade. The control group watched same-length videos showing non-violent everyday events as they appeared in the news. The results showed that the students who had viewed terror events felt more personally threatened and reported a significantly lower level of psychological resources (such as their sense of success, importance and commitment) after watching, compared to the control group. The first group also reported higher levels of negative feelings and mood. The researchers noted that earlier studies that examined first-hand exposure to threats showed that compromised psychological resources and heightened levels of negative feelings can trigger secondary trauma and post-trauma symptoms. This could also be the case for individuals who feel threatened from indirect exposure to terrorism and political violence. An interesting finding in the current study was a difference between the responses of its Jewish and Arab participants. The level of threat that the Arabs felt after watching a violent clip was significantly higher than for the Jewish participants. «It is early yet to relate to the long-term effects of viewing terror events in the mass media, but the current study does show that there are definite short-term effects. In an age when many violent events around the world are immediately broadcast in everyone's living room and office, we ought to be aware of the negative effects that this sort of exposure could have,» the researchers noted.

The Strong Arm of High-Security

Source: http://www.1stsecuritynews.com/security/strong-arm-highsecurity/#more-429

Avon Barrier Company has launched its latest rising arm barrier – the EB1400CR Trojan which is also the strongest barrier of its type it has designed and manufactured to-date. The barrier has been specifically developed to meet threats posed by extreme Vehicle Borne Improvised Explosive Device (VBIED) attack and offers one of the highest levels of protection available anywhere in the world, states Avon Barrier Company. The new Trojan barrier recently passed comprehensive independent physical testing by the Transport Research Laboratory (TRL) in compliance with PAS 68*, one of the highest criteria – resisting a 7500KG truck travelling at 80kph (50MPH). The barrier can withstand direct impact forces of 1852KJ and its design combines the very highest levels of protection, with ease and speed of installation, thanks to its shallow-mount requirements. It is suitable for sites where central roadway foundations may not be possible or practical. Commenting on the new EB1400CR Trojan, Paul Jeffrey, Managing Director of Avon Barrier Company, said; "As hostile terrorist attacks become potentially more extreme we have designed and produced one of the world's strongest rising-arm barriers to provide the ultimate in protection. This will ensure that sites are not only protected now, but in the future against rising threat levels. The EB1400CR Trojan barrier offers the convenience of a rising-arm type barrier, with additional levels of protection, thanks to its unique design and construction." The barrier is available in a range of widths and can be configured to interface with almost all types of control equipment, remaining fully operational even under power failure conditions. With its robust design and heavy gauge construction, the Trojan also provides a very strong visual deterrent to mitigate against hostile attack. Avon Barrier Company Ltd. (www.avon-barrier.co.uk) design, manufacture and install a range of specialist crash-tested high-end physical security protection including crash-tested barriers, road-blockers, gates and bollards. The company operates internationally and has its headquarters in the United Kingdom.

New Approach to cop better with Homeland Security issues

Arab and Muslim Terror – A Double Edged Sword to Their Native Lands

Source: http://www.securityacademy.com/

Throughout History we have learned how great an effect extremist activity can have, even though most of those extremists are only a small part of their communities, these "noisy" activists, some who were very militant and powerful had in their actions caused, from very early on, a negative attitude and resistance against themselves within their own communities. Their movements have since gained momentum and dominance through the use of intimidation and terror, first in their local areas and then spilling out into the global arena.

This kind of process of expansion through terror and intimidation had a great impact on the 20th century as seen in examples such as the rise of the Nazi party in Germany. They began as a very small but militant and "noisy" group that eventually led the silent majority to disaster whose terrible effects were felt for many years after. All this because of the inability to silence this violent minority even though they dictated a violent and frightening regime of internal violence and intimidation which caused suffering and despair to large parts of the German nation long before Hitler's violent means were brought to the rest of Europe.

Other similar examples continued and still continue to spring up all over the globe, where a violent minority takes control of its people or state and steers it and other groups into a cycle of religious wars, ideological struggles, wars and genocides. Violence in recent years and the threat of a nuclear Iran has only highlighted these dangers and the need for a proper understanding of this problem.

Violent terrorist attacks against countries, peoples, organisations and individuals did not just begin in the heyday of terror around Arafat's Fatah movement dominating the PLO in the mid 1960's but shortly thereafter did see the advent of gaining recognition and legitimacy from most Muslim and Arab states as well as many of the non-aligned states largely because PLO violence was not directed against them and was therefore 'not their problem'.

Thus in the 1970's the Arab and Muslim leaders did not expect that their support for such terrorist movements would bring upon themselves suffering, violence and many casualties.

In recent years everyone can see the familiar cycle becoming apparent where a small extremist minority, which is militant, powerful. It has been granted legitimacy by various Muslim and Arab leaders and even some Western countries who have not understood that this is a **double edged sword** that will at some point or another hurt its wielder.

Today Millions of righteous and life-loving Muslims and Arabs have had forced upon them the "halo and image" which the small, violent minority sought to achieve through carrying out acts of terror and intimidation in the name of Islam or their Nation and in doing so polarised the entire world by religious and ethnic divide between "light" and darkness"

Sadly for the world population and for Arab states, Muslim and non-Muslim, in particular there is today no radical or cutting separation among those within the Islamic world who have used and continue to use terror against Jews and Christians who are in my view, a smaller problem compared to the attacks and killing sprees they have brought against other sects within their own nations in the name of their religious or ideological struggle.

Even at a short glance it is apparent that the number of casualties within the internal clashes of the Arab and Muslim world inflicted by these terrorist elements is higher than the casualties caused by their attacks on their perceived non-Arab and non-Muslim enemies in the name of Jihad and other such causes.

Intimidation and Terrorism used against the Arab and Muslim nations by these small, violent, fanatic minorities is becoming a tool for gaining strength and influence both financially and organisationally, as well as to diminish the influence of the moderate yet tragically silent majority.

Insight

Throughout the Muslim and Arab world, many leaders and businessmen are living under the shadow of fear and terror. Now they are recognizing that the extortion and violence which emanates from those terrorist groups that they had allowed them to build the basis for attacking Israel and the West, Christians and Infidels is also turning against themselves and their own people, very fast.

It is not a secret that a large amount of Multinationals Close Protection operatives from various countries are employed to both sectors Governmental & Civilian, permanently in provision of Protection services to Arab/Muslim VIPs and their families.

It is known that there are also misunderstandings and sometimes, even conflicts between these VIPs and their protectors that occur, mainly, because of the lack of familiarization with the culture, manners or mentality from both sides.

Recently we all realize how the Afghan President Hamid Karzai struggles against the western security companies that have protected him and his Government during the very dangerous last few years of the Afghanistan chaos and his reaction came as a result of the lack of familiarization with the culture, manners or mentality of the local population.

ISA – Group contribution

We at ISA - **I**nternational **S**ecurity **A**cademy - ISRAEL have decided to open and share our knowledge, gained by Israelis and by our many associates overseas, from security and protection professionals from all over the world, Arabs, Muslims and Westerners.

The major aim of this New-born innovative is **to integrate** these Protection professionals laying aside all possible barriers, such as religion, political conflicts, deferent concepts, methods, tactics etc in order to reduce and mitigate together the violent crime & Terrorism worldwide.

Since July 2011, ISA - Group will start a new innovative project:

Integration by training together

Israeli protection Instructors of ISA – ISRAEL in conjunction with a Multinational team of Protection & Counter Terrorism Instructors trained and certified by ISA- ISRAEL will impart their exceptional expertise, proven concepts and methods for the goal of qualification and preparation of Close Protection Operatives **Arab/Muslim** & **Western** operatives active in the Protection of Arab/Muslim VIPs worldwide.

This will be a **joint training program** for Protection operatives from a variety of countries organized by **IPT** (Integrated Protection Teams Network) and operated by ISA – Group in Germany, Switzerland, UK, USA and South Africa.

Russia's counter terrorism woes

Source: http://homelandsecuritynewswire.com/russias-counter-terrorism-woes

A recent editorial in the Washington Post illustrates Russia's difficulties in successfully deterring terrorist attacks; the Post blasts Russian leaders citing corruption as a significant reason for their inability to successfully develop counter-terrorism policing abilities, intelligence agencies, and to secure public areas; the editorial also blames Putin's hard line stance on the northern Caucasus region as fuelling extremist movements; in 2010 terrorist attacks in the Caucasus doubled; as a stark warning, the Post reminds readers that the 2014 Winter Olympic Games is scheduled to be held on the border of the Caucuses.

The 2009 Nevsky Express train attack // Source: abc.net.au

A recent editorial in the Washington Post illustrates Russia's difficulties in successfully deterring terrorist attacks. The identification of last week's suicide bomber as a twenty year old man from the northern Caucasus highlights the volatile situation in the predominately Muslim republics of Chechnya, Ingushetia, and Dagestan. These areas have increasingly turned to extremism in their quest for more autonomy from Moscow.

and have often resorted to violent acts of terrorism. In December of 2009, Chechen rebels bombed crowded passenger trains in Moscow, derailing one and killing twenty-six people and injuring eighty-seven in the process. Other attacks include the deadly2004 Beslan school hostage crisis in which armed militants occupied a school and took more than 1,100 people hostage for three days. Russian security forces stormed the building setting off a frenzied gun battle in which tanks, rockets, and other heavy weapons were used. In the end, at least 334 hostages were killed, among them 186 children. Official Russian reports indicate that terrorist attacks in the Caucasus doubled in 2010. The editorial blames Prime Minister Putin's authoritarian regime for perpetuating this volatile political situation that often results in fatal attacks. The Washington Post writes, "Mr. Putin's autocratic form of rule and imperialist policy toward non-Russian nations has made it impossible for him to resolve — or even seriously address - the underlying problem that fuels most of the attacks." It goes on to say, "Russia's brutal response, including Mr. Putin's scorched-earth campaign in Chechnya, fueled the rise of Muslim extremist groups that have been growing steadily stronger despite non-stop counterterrorism operations." The editorial also blames rampant corruption in Russia for their inability to successfully form counter terrorist police forces, intelligence networks, and secure major public areas. Putin has continued to solidify his power turning Russia into a "domestic police state," yet Moscow has suffered eight major attacks including the destruction of two airplanes. The Post alleges that political leaders in Russia are unwilling to shift the focus of the federal secret police and other security services "which are more skilled at protection rackets and the persecution of political dissidents than in detecting terrorist plots." As evidence, the Post cites the fact that in the aftermath of the most recent bombing, President Dmitry Medvedev blamed private security forces, "rather than federal officials responsible for counterterrorism." The editorial ends with the stark reminder that Russia is set to host the 2014 Winter Olympics in Sochi, on the edge of the Caucasus. "The International Olympic Committee's unwise decision to accept Russia's bid means that athletes and governments around the world have to depend on the Putin-Medvedev regime to prevent terrorist disruption of the Games. Monday's attack was a reminder of how risky a bet that is."

Air Force to deploy supercomputer aboard a superblimp

Source: http://homelandsecuritynewswire.com/air-force-deploy-supercomputer-aboard-superblimp

SIGINT
FMV
GMTI
Ground Component

Superblimp's super data handling capability
Source: techalps.com

The U.S. Air Force is developing a massive blimp to gather and process all intelligence feeds from Afghanistan; the air ship will be longer than a football field and seven times the size of the Goodyear Blimp and will be able to stay afloat for nearly a week at nearly four miles up; the key feature of the ship will be its sophisticated supercomputer which can process 300 terabytes of data an hour; this computer will help limit data overload as surveillance sensors become increasingly complex; it currently takes fourteen analysts to monitor a single feed from a predator and the next generation drones will have ninety-six cameras; the blimp's first test flight is scheduled for 15 October.

As police departments in the United States continue to float the idea of using blimps as surveillance vehicles, the Air Force is pressing ahead with its plan to launch a massive blimp that would function as a centralized intelligence command center in Afghanistan. The air ship, seven times the size of the Goodyear Blimp, would fly at 20,000 feet and collect data from the various unmanned surveillance drones patrolling the skies. The supercomputer housed aboard the blimp will sift the various data streams and automatically direct sensors to collect critical information. The Air Force already monitors all the video and audio streams from surveillance drones, but the time it takes to personnel to determine which bits of information are critical have sometimes allowed the enemy to escape. The supercomputer is designed to cut down on this lag time and feed coordinated information to troops on the ground in less than fifteen seconds. Lt. Gen. David Deptula, the recent head of the Air Force's intelligence operations believes the project "could change the nature of overhead surveillance." He says, "There's huge potential there." The next generation of surveillance equipment, Gorgon Stare and wide-area airborne surveillance systems (WAAS), use hives of a dozen cameras to film areas within a 2.5 mile radius. With as many as ninety-six cameras, these drones can cause massive data overloads for both human operators and digital networks. It currently requires nineteen analysts to watch a single feed from a Predator drone. With the next generation surveillance equipment, a single drone would generate 274 terabytes of data every hour from its ninety-six cameras. Gen. James Cartwright, vice chairman of the Joint Chiefs of Staff, said that he would need 2,000 analysts to process the information collected by a single drone using WAAS sensors. To prevent this information overload from overwhelming intelligence analysts, the Air Force is designing the supercomputer to be housed aboard the Blue Devil. The computer will have the equivalent of 2,000 single-core servers and process up to 300 terabytes an hour. Instead of sending all of this processed information to troops, like with today's sensors, the Blue Devil's processors will calculate the data and filter it into an easily searchable format. Troops on the ground will then be able to search the ship's computer for relevant information. Lt. Gen. Deptula explains that this process will reduce bandwidth consumption. "People ask: 'With all these sensors, how're you gonna transmit all that data down to the ground?' Well, we don't necessarily need to send it all down," said Deptula." A potential solution is to process part of the data on-board, and only send what is of interest. That reduces the bandwidth requirements." The ambitious project dubbed "Blue Devil" will cost $211 million and is currently in its second phase of development. According to Wired Magazine's Danger Room, a source close to the project says the Blue Devil will be "one of the largest airships produced since World War II."

"It's freakishly large," the source adds. When completed, the airship will be longer than a football field at 350 feet and seven times the size of the Goodyear Blimp at 1.4 million cubic feet. The blimp's unprecedented size will help it carry enough fuel and helium to stay afloat for as long as a week at nearly four miles up. Most blimps fly at 3,000 feet or less. The U.S. Army is also at work on a competing airship project, the Long Endurance Multi-Intelligence Vehicle, that could stay afloat for nearly three weeks thanks to a sophisticated hybrid hull. The Air Force is focusing its efforts on designing a complex set of onboard sensors and a supercomputer, rather than concentrating on hull design. In addition to the supercomputer, the airship will carry on-board listening devices, a WAAS system, day and night cameras, and communications relays and receivers for ground sensors. **The Blue Devil's first test flight is scheduled for 15 October.**

Dark Side of Social Network: al-Qaida Recruiting

Source:http://www.newsmax.com/Newsfront/alQaida-radicalIslamists-recruitment-Facebook/2011/02/ 09/id/385499

A new study says the online social network Facebook and the video-sharing Web service YouTube are just some of Internet services being used effectively for the recruitment and training of Islamic terrorists, the National Journal reports. Such sites allow terror groups including al-Qaida to recruit under radar and around the world by reaching potential new members in their homes, says the Pentagon-funded paper by the Center for Strategic and International Studies. Through social media, Web video, e-mail and other content and communications applications, terrorist leaders also can train and instruct new recruits without having to physically transport them to hidden base camps, the study says. According to CSIS, the growing reach of the Internet since 9/11 has allowed al-Qaida, even in a weakened state, to disseminate its ideas to an ever-larger audience: “Despite extensive counterterrorism success against the group responsible for 9/11, the al-Qaida ‘brand’ now resonates with an increasingly diverse (though still narrow) cross-section of Muslims around the world,” the study says.

Abdelmalek Droukdel, head of Al-Qaida in the Islamic Maghreb (AQIM) is pictured on the U.S. monitoring group SITE Intelligence, on November 19, 2010 in Paris.

Only 32 miles of U.S. Canada border secure

Source: http://homelandsecuritynewswire.com/only-32-miles-us-canada-border-secure

A GAO report found that only thirty-two miles along the nearly 4,000 mile border had «an acceptable level of security»; the report also found that the northern border posed a greater terrorist threat due to its size and limited law enforcement coverage that could allow terrorists to enter undetected; the U.S. Canada border stretches nearly 4,000 miles and is difficult to patrol due to its varied terrain; the report was released days before President Obama and Canadian prime minister Stephen Harper signed an agreement to expand cooperation along the border and expedite the flow of goods; in 2010 DHS spent nearly $3 billion to secure the northern border, making roughly 6,000 arrests and interdicting approximately 40,000 pounds of illegal drugs. With so much attention on the U.S.-Mexico border, the U.S. government has overlooked its northern border leaving it largely unguarded. A recent investigation by the Government Accountability Office (GAO) found that only thirty-two miles along the nearly 4,000 mile border had “an acceptable level of security.” Senator Joe Lieberman (I – Connecticut), the chairman of the Senate Homeland Security and Governmental Affairs Committee, said “These findings should sound a loud alarm to the Department of Homeland Security, the Canadian government, and our committee.” The report found that while the southern border is more susceptible to drug trafficking and illegal immigration, the northern border poses a greater terrorist threat. Due to its sheer size and limited law enforcement coverage, terrorists have more entry points and can more easily avoid detection. This has also made the Canadian border attractive to drug traffickers, currency smugglers, and illegal immigrants. The U.S.

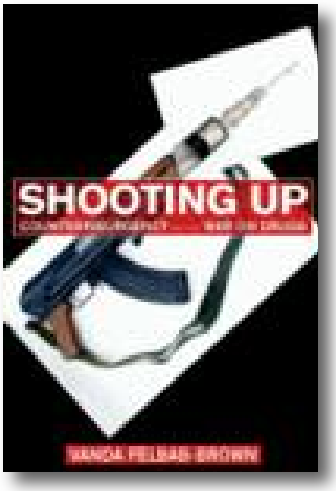
Canada border is difficult to patrol as a result of its diverse terrain and sheer size. Stretching from Washington to Maine, the border includes dense forests, vast open plains, and large remote sections that are far from inhabited areas. The report found that U.S Customs and Border Protection (CBP), the agency tasked with preventing the illegal entry of goods and people, lacked "the ability to detect illegal activity across most of the northern border" and did not possess "situational awareness." DHS works with local, state, tribal, and federal agencies to secure the border. GAO reported, however, that that, "long-standing coordination challenges between CBP's Office of Border Patrol and ICE, ICE and DEA, and Border Patrol and Forest Service that may impede achieving border security goals." GAO recommends that DHS take the lead on interagency coordination and clarify mission goals, establish forums between various agencies, and reduce duplicate tasks. In response to the report, DHS spokesman Matt Chandler said, the department has "made critical security improvements along the northern border, deploying additional Border Patrol agents, technology and infrastructure" and is in the midst of establishing a "northern border strategy" to address concerns. Last year DHS spent nearly $3 billion to secure the northern border, making roughly 6,000 arrests and interdicting approximately 40,000 pounds of illegal drugs. The GAO report was released days before President Obama and Canadian Prime Minister Stephen Harper signed an agreement to expand trade and security along the border. In the wake of 9/11, the United States imposed stricter measures along its bordersto prevent terrorists or weapons from entering. To streamline the process and expedite the flow of goods and people, the two leaders announced the creation of the United States-Canada Regulatory Cooperation Council (RCC). In a joint statement, they announced, "we intend to pursue a perimeter approach to security, working together within, at, and away from the borders of our two countries to enhance our security and accelerate the legitimate flow of people, goods, and services between our two countries." Every day roughly 300,000 people cross the border, while each minute nearly $1 million in goods and services travel between the two countries.

Shooting Up Counterinsurgency and the War on Drugs

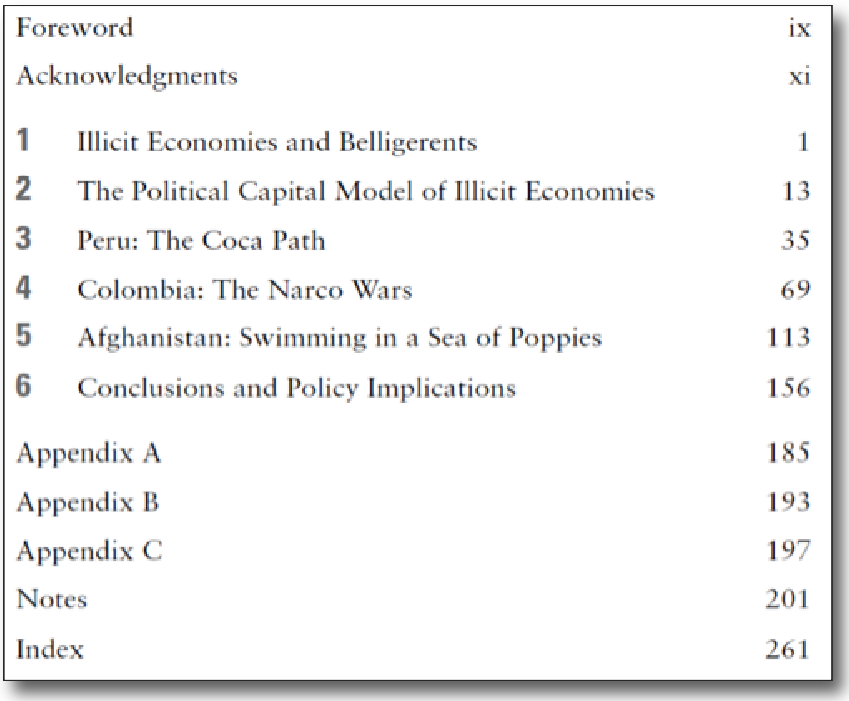
By Vanda Felbab-Brown, PhD

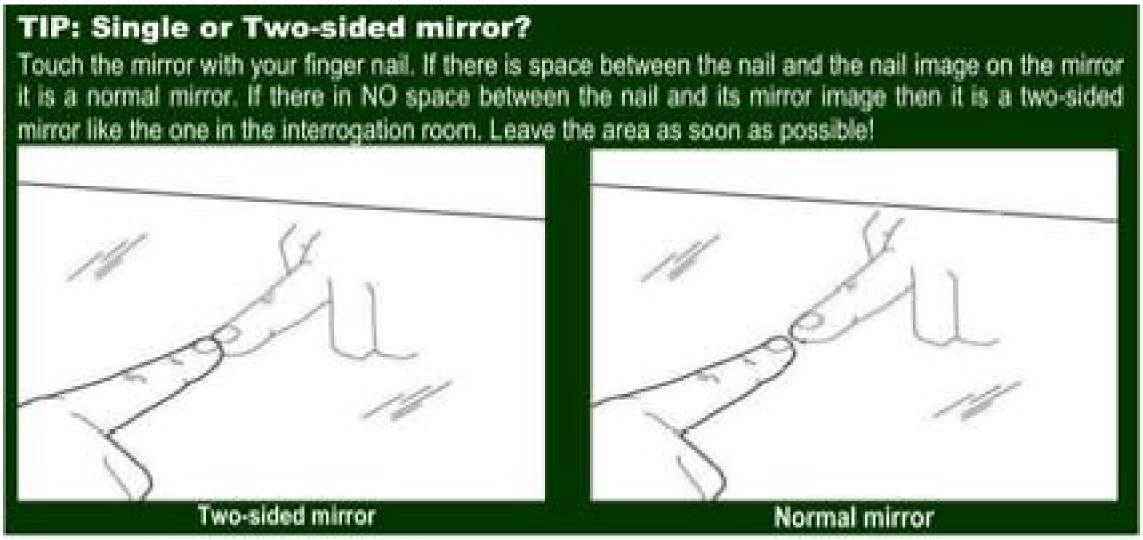
Brookings Institution Press 2009 c. 273pp.

Source: http://www.brookings.edu/press/Books/2009/shootingup.aspx



Most policymakers see counterinsurgency and counternarcotics policy as two sides of the same coin. Stop the flow of drug money, the logic goes, and the insurgency will wither away. But the conventional wisdom is dangerously wrongheaded, as Vanda Felbab-Brown argues in Shooting Up. Counternarcotics campaigns, particularly those focused on eradication, typically fail to bankrupt belligerent groups that rely on the drug trade for financing. Worse, they actually strengthen insurgents by increasing their legitimacy and popular support. Felbab-Brown, a leading expert on drug interdiction efforts and counterinsurgency, draws on interviews and fieldwork in some of the world's most dangerous regions to explain how belligerent groups have become involved in drug trafficking and related activities, including kidnapping, extortion, and smuggling. Shooting Up shows vividly how powerful guerrilla and terrorist organizations—including Peru's Shining Path, the FARC and the paramilitaries in Colombia, and the Taliban in Afghanistan—have learned to exploit illicit markets. In addition, the author explores the interaction between insurgent groups and illicit economies in frequently overlooked set tings, such as Northern Ireland, Turkey, and Burma. While aggressive efforts to suppress the drug trade typically backfire, Shooting Up shows that a laissez-faire policy toward illicit crop cultivation can reduce support for the belligerents and, critically, increase cooperation with government intelligence gathering. When combined with interdiction targeted at major traffickers, this strategy gives policy-makers a better chance of winning both the war against the insurgents and the war on drugs.





TIP: Single or Two-sided mirror?

Touch the mirror with your finger nail. If there is space between the nail and the nail image on the mirror it is a normal mirror. If there in NO space between the nail and its mirror image then it is a two-sided mirror like the one in the interrogation room. Leave the area as soon as possible!

Extremist groups active inside UK universities

Towards London 2011

Source: http://www.guardian.co.uk/uk/2005/sep/16/politics.students

From a 2005 article in The Guardian (UK)

Anthony Glees, the director of Brunel University's centre for intelligence and security studies, lists more than 30 institutions - including some of the most high-profile universities in the country - where «extremist and/or terror groups» have been detected. The study states that the Islamist groups Hizb ut-Tahrir and al-Muhajiroun, which are subject to a «no-platform policy» by the National Union of Students, are active on many campuses and often operate under different names. The report catalogues the activities of far-right organisations and animal rights extremists. Among the universities named are Cambridge, where the BNP were detected; Oxford, where the report said animal rights extremists had been active; and the London School of Economics and Manchester University, which both had active Islamist extremist groups.

British universities where extremist or terror groups have been detected:
Birmingham (Islamist); Brunel (BNP, Islamist); Cambridge (BNP); City (Islamist); Coventry (Islamist); Cranford Community College (Islamist); Derby (Islamist); Dundee (Islamist); Durham (Islamist); Greenwich (BNP); Imperial College (Islamist); Kingston (Islamist); Leeds (BNP, Islamist); Leicester (Islamist); LSE (Islamist); Luton (Islamist); Manchester (BNP, Islamist); Manchester Metropolitan (BNP); Newcastle (Islamist); Nottingham (Islamist); Oxford (Animal rights extremists); Reading (Islamist); Salford (BNP); South Bank (Islamist); SOAS (Islamist); Sussex (BNP); Sunderland (BNP, Islamist); Swansea (Islamist); Wolverhampton (Islamist); York (BNP).

The following correction was printed in the Guardian's Corrections and clarifications column, Saturday September 24 2005:

Cranford Community College, which was listed in the article below as a university campus, is in fact a secondary school for 11- to 18-year-olds. There were, nevertheless, reported links to an Islamist organisation, as indicated in the list.

Selected Literature on Terrorism and Organized Crime

Source:http://www.terrorismanalysts.com/pt/index.php?option=com_rokzine&view=article&id=148&Itemid=54

PERSPECTIVES ON TERRORISM
a journal of the Terrorism Research Initiative

Monographs, Edited Volumes, Non-conventional Literature and Prime Articles published since 2001, selected by **Eric Price** (Professional Information Specialist, Editorial Assistant TRI)

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.

Amoore, L. & de Goede, M. (eds.) (2008) *Risk and the war on terror.* London & New York: Routledge.[* http://www.loc.gov/catdir/toc/ecip085/2007047895.html]

Barnhart, S.R. (2002) *International terrorism and political violence: the entity of transnational criminal organisations and new terrorisms in the Balkans-Middle East and Eastern Europe, and its effect on the entire world.* Victoria, B.C.: Trafford.[*http://www.loc.gov/catdir/toc/fy0711/2002489193.html]

Bayley, D.H. & Perito, R.M. (2010) *The police in war: fighting insurgency, terrorism, and violent crime.* Boulder: Lynne Rienner Publishers.

Becker, G.S. & Posner, R.A. (2009) *Uncommon sense: economic insights, from marriage to terrorism.* Chicago & London: The University of Chicago Press.

Benedek, W. (et al.) (eds.) (2010) *Transnational terrorism, organized crime and peace-building: human security in the Western Balkans.* New York: Palgrave Macmillan.

Berg, B. L. (2008) *Criminal investigation.* Boston: McGraw-Hill Higher Education. [*http://www.loc.gov/catdir/toc/ecip0713/2007010569.html]

Birzer, M. L. & Roberson, C. (2008) *Police field operations: theory meets practice.* Boston, MA.: Pearson/Allyn & Bacon. [*http://www.loc.gov/catdir/toc/ecip0717/2007017170.html]

Blair, I. (2009) *Policing controversy.* London: Profile Books.

Canter, D & Youngs, D. (2009) *Investigative psychology: offender profiling and the analysis of criminal action.* Chichester, Hoboken, NJ.: John Wiley & Sons.

Charles, R.B. (2004) *Narcotics and terrorism: links, logic, and looking forward.* Philadelphia: Chelsea House Publishers. [*http://www.loc.gov/catdir/toc/ecip043/2003009501.html]

Chaudhary, D.R. & Chaudhary, A.N. (2004) *The Maharashtra Control of Organised Crime Act, 1999 (Maharashtra Act 30 of 1999) as extended to NCT of Delhi.* Pune, C.T.J. Publications: Delhi Distributors: Capital Pub. House.

Choo, K-K. R. (et al.) (2007) *Future directions in technology-enabled crime: 2007-09.* Canberra: Australian Institute of Criminology.

Clark, L. & Algaier, W.E. (2005) *Surveillance detection: the art of prevention : an effective early warning system for preventing criminal and terrorist acts.* Bloomington: Ind.: AuthorHouse. [*http://www.loc.gov/catdir/toc/fy0802/2005905934.html]

Cracknell, D.G. (comp.) (2008) *Constitutional and administrative law, 2007-2008.* London & New York, NY.: Routledge-Cavendish. [*http://www.loc.gov/catdir/enhancements/fy0745/2007035780-d.html]

Crawford, A. (ed.) (2011) *International and comparative criminal justice and urban governance: convergence and divergence in global, national and local settings.* Cambridge, New York: Cambridge University Press.

De Becker, G. (2002) *Fear less: real truth about risk, safety, and security in a time of terrorism.* Boston, Little: Brown. [*http://www.loc.gov/catdir/toc/fy0711/2001097790.html]

Delpech, T. (2002) *International terrorism and Europe.* Paris: European Union Institute for Security Studies.

Demet Ulusoy, M. (ed.) (2008) *Political violence, organized crimes, terrorism, and youth.* [NATO Advanced Research Workshop on Political Violence, Organized Crimes, Terrorism and Youth (2007: Ankara, Turkey] Amsterdam, Washington, DC.: IOS Press.

Dijk, J. V. (2008) *The world of crime: breaking the silence on problems of security, justice, and development across the world.* Los Angeles: Sage Publications. [*http://www.loc.gov/catdir/toc/ecip081/2007040209.html]

Eterno, J.A. & Das, D.K. (2010) *Police practices in global perspective.* Lanham: Rowman & Littlefield Publishers.

Forst, B. (2009) *Terrorism, crime, and public policy.* Cambridge, New York: Cambridge University Press [*http://www.loc.gov/catdir/enhancements/fy0903/2008008301-t.html]

Gaouette, M. (2010) *Cruising for trouble: cruise ships as soft targets for pirates, terrorists, and common criminals.* Santa Barbara, Calif.: Praeger.

Giraldo, J.K. & Trinkunas, H.A. (eds.) (2007) *Terrorism financing and state responses: a comparative perspective.* Stanford, Calif.: Stanford University Press. [*http://www.loc.gov/catdir/toc/ecip073/2006035059.html]

Goredema, C. (2004) *African commitments to combating organised crime and terrorism: a review of eight NEPAD countries.* African Human Security Initiative.

Green, P. (2004) *State crime: governments, violence and corruption.* London: Sterling, Va.: Pluto Press. [*http://www.loc.gov/catdir/enhancements/fy0904/2004271801-t.html]

Hagan, F. E. (2011) *Introduction to criminology: theories, methods, and criminal behavior.* Los Angeles: Sage Publications.

Hamm, M. S. (2007) *Terrorism as crime: from Oklahoma City to Al-Qaeda and beyond.* [*http://www.loc.gov/catdir/toc/ecip0620/2006029835.html]

Hayworth, J.D. & Eule, J.J. (2006) *Whatever it takes: illegal immigration, border security, and the war on terror.* Washington, DC.: Regnery Pub.: Lanham, MD.: National Book Network. [*http://www.loc.gov/catdir/toc/ecip064/2005033948.html]

Hertzberger, E. R. (2007) *Counter-terrorism intelligence cooperation in the European Union.* Turin, Italy: UNICRI.

Hesterman, J. L. (2005) *Transnational crime and the criminal-terrorist nexus: synergies and corporate trends.* Maxwell Air Force Base, Ala.: Air University Press.

Holmes, L. (ed.) (2007) *Terrorism, organised crime and corruption: networks and linkages.* Cheltenham, UK: Northampton, MA.: Edward Elgar. [* http://www.loc.gov/catdir/toc/ecip0620/2006028689.html]

Hatalak, O. (ed.) (2002) *Papers from the seminar, «The New International Terrorism: Prevention Strategies», UNICRI 19-20 April 2002*. Turin, Italy: UNICRI.[*http://www.loc.gov/catdir/toc/fy0711/2003380113.html]

Hough, M & Kruys, G.P.H. (eds.) (2009) *Non-military threats to security: selected United Nations and other multilateral documents.* Pretoria, Institute for Strategic Studies: University of Pretoria.

Innes, B. (2003) *International terrorism.* Broomall, PA.: Mason Crest Publishers.

Kelly, R.J & Rieber, R.W. (2003) *Terrorism, organized crime & social distress: the new world order.* New York: Psycke-Logo Press. [* http://www.loc.gov/catdir/toc/fy0602/2003100950.html]

Konstadinides,T. & Eckes, C. (eds.) (2011) *Crime within the area of freedom, security and justice: A European public order.* Cambridge, New York: Cambridge University Press. [*http://www.loc.gov/catdir/enhancements/fy1101/2010045713-t.html]

Kruger, A. (2008) *Organised crime and proceeds of crime law in South Africa.* Durban: LexisNexis.

Langewiesche, W. (2004) *The outlaw sea: a world of freedom, chaos, and crime.* New York: North Point Press. [*http://www.loc.gov/catdir/toc/ecip0412/2003028112.html]

Leong, A. (2007) *The disruption of international organised crime: an analysis of legal and non-legal strategies.* Aldershot,Hants, UK: Burlington, VT.: Ashgate. [*http://www.loc.gov/catdir/toc/ecip0719/2007021821.html]

Lilley, P. (2006) *Dirty dealing: the untold truth about global money laundering, international crime and terrorism*. London & Philadelphia: Kogan Page. [*http://www.loc.gov/catdir/enhancements/fy0912/2005035377-b.html]

Lyman, M. D. (2011) *Criminal investigation: the art and the science.* Boston: Prentice Hall.

Madsen, F.G. (2009) *Transnational organized crime.* London & New York: Routledge.

Maguire, M. (et al.) (eds.) (2007) *The Oxford handbook of criminology.* Oxford, New York: Oxford University Press Inc. [*http://www.loc.gov/catdir/toc/ecip077/2006102290.html]

Malisow, B. (2008) *Terrorism.* New York, NY.: Chelsea House. [*http://www.loc.gov/catdir/toc/ecip0814/2008012306.html]

McFarlane, J. (2002) *Organised crime and terrorism in the Asia-Pacific Region: the reality and the response*. Canberra, Australia: Strategic and Defence Studies Centre, Australian National University.

Maniscalco, P.M. (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. (2002) *Terrorism response: field guide for law enforcement.* Upper Saddle River, N.J.: Prentice Hall, Boston, Mass.: Pearson Custom Pub. [*http://www.loc.gov/catdir/toc/fy0711/2002514449.html]

Manwaring, M.G. (2008) *Insurgency, terrorism, and crime: shadows from the past and portents for the future.* Norman: University of Oklahoma Press. [*http://www.loc.gov/catdir/toc/ecip0814/2008012870.html]

Newman, G.R. & Clarke, R.V. (2008) *Policing terrorism: an executive's guide.* Washington, DC.: U.S. Dept. of Justice, Office of Community Oriented Policing Services, Center for Problem-Oriented Policing.

Occhipinti, J.D. (2003) *The politics of EU police cooperation: toward a European FBI?* Boulder, Colo.: L. Rienner. [*http://www.loc.gov/catdir/toc/fy038/2003041369.html]

O'Connor, D. (2005) *Closing the gap: a review of the «fitness for purpose» of the current structure of policing in England & Wales.* London: HM Inspectorate of Constabulary. [*http://www.loc.gov/catdir/toc/fy0611/2006373439.html]

Orttung, R.W. & Latta, A. (eds.) (2008) *Russia's battle with crime, corruption and terrorism.* Abingdon, Oxon.: New York, NY.: Routledge.

Payne, R. J. (2011) *Global issues: politics, economics, and culture*. Boston: Longman.

Perlmutter, D. (2004) *Investigating religious terrorism and ritualistic crimes.* Boca Raton: CRC Press. [*http://www.loc.gov/catdir/enhancements/fy0646/2003046210-d.html]

Philbin, T. (2007) *The killer book of true crime: incredible stories, facts and trivia from the world of murder and mayhem.* Naperville, Ill.: Sourcebooks, Inc. [*http://www.loc.gov/catdir/toc/ecip076/2006100786.html]

Regoli, R. M. & Hewitt, J.D. (2010) *Exploring criminal justice: the essentials.* Sudbury, Mass.: Jones and Bartlett Publishers.

Rimington, S. (2008) *Secret asset.* New York: Vintage Crime/Black Lizard.

Robb, J. (2007) *Brave new war: the next stage of terrorism and the end of globalization.* Hoboken, N.J.: John Wiley & Sons. [*http://www.loc.gov/catdir/toc/ecip0620/2006029354.html]

Roleff, T.L. (ed.) (2002) *War on drugs: opposing viewpoints.* San Diego, Calif.: Greenhaven Press.

Ronczkowski, M. (2007) *Terrorism and organized hate crime: intelligence gathering, analysis, and investigations.* Boca Raton: CRC Press. [*http://www.loc.gov/catdir/toc/ecip0615/2006018580.html]

Ruggiero, V. (2006) *Understanding political violence: a criminological approach.* Maidenhead, Berkshire: New York: Open University Press. [*http://www.loc.gov/catdir/toc/fy0716/2007618760.html]

Ryan, K.J. (2007) *Radical eye for the infidel guy: inside the strange world of militant Islam.* Amherst, N.Y.: Prometheus Books. [*http://www.loc.gov/catdir/toc/ecip077/2007000021.html]

Salisbury, S. (2010) *Mohamed's ghosts: an American story of love and fear in the homeland.* New York: Nation Books.

Scarry, E. (2010) *Rule of law, misrule of men.* Cambridge, Mass.: MIT Press.

Schmalleger, F. (2010) *Criminology: a brief introduction.* Boston: Prentice Hall.

Schmalleger, F. (2009) *Criminology today: an integrative introduction.* Columbus, Ohio: Pearson/Prentice Hall. [*http://www.loc.gov/catdir/toc/ecip0723/2007030308.html]

Schweitzer, G.E. & Schweizer, C.D. (2002) *Superterrorism.* Cambridge, MA.: Basic Books.

Simpson, A. (2010) *Duplicity and deception: policing the twilight zone of the troubles.* Dingle, Ireland: Brandon Books

Smith, P (ed.) *Terrorism and violence in Southeast Asia: transnational challenges to states and regional stability.* Armonk, New York: M.E. Sharpe. [*http://www.loc.gov/catdir/toc/ecip0416/2004007994.html]

Somervill, B. A. (2008) *Graphing crime.* Chicago, Ill.: Heinemann Library.

South Pacific Forum Secretariat. (2003) *Regional framework: including model legislation to address terrorism and transnational organised crime.* Suva, Fiji: South Pacific Forum Secretariat.

Thobaben, R.G. (et al.) (2006) *Issues in American political life: money, violence, and biology.* Upper Saddle River, N.J.: Pearson Prentice Hall. [*http://www.loc.gov/catdir/toc/ecip0518/2005025181.html]

Upadhyay, A. (2009) *India's fragile borderlands: the dynamics of terrorism in north east India.* London & New York: I.B. Tauris.

Van Brunschot, E.G. (2009) *Risk balance &*

security. Thousand Oaks: Sage Publications. [*http://www.loc.gov/catdir/toc/ecip0714/2007011267.html]

Walner, A.H. (2006) *Wake up America to crime prevention and anti-terrorism.* Bloomington, IN.: Author House.

Weiss, T.G & Daws, S. (eds.) (2007) *The Oxford Handbook on the United Nations.* Oxford, New York: Oxford University Press. [*http://www.loc.gov/catdir/toc/ecip077/2006103221.html]

Welch, M. (2009) *Crimes of power & states of impunity: the U.S. response to terror.* New Brunswick, N.J.: Rutgers University Press. [*http://www.loc.gov/catdir/toc/fy0904/2008016718.html]

White, J. R. (2004) *Defending the homeland: domestic intelligence, law enforcement, and security.* Belmont, CA.: Wadsworth/Thomson Learning. [*http://www.loc.gov/catdir/toc/fy0711/2003107885.html]

Williams, P.L. (2005) *The Al Qaeda connection: international terrorism, organized crime, and the coming apocalypse.* Amherst, NY.: Prometheus Books. [*http://www.loc.gov/catdir/toc/ecip0512/2005013880.html]

Yonah, A. (ed.) (2010) *Terrorists in our midst: combating foreign-affinity terrorism in America.* Santa Barbara, Calif.: Praeger Security International.

Zedner, L. (2009) *Security*. London & New York: Routledge. [http://www.loc.gov/catdir/toc/ecip0826/2008036736.html]

Non-conventional Literature

Albania, Republic of (2007) *Crosscutting strategy: fighting against organized crime, trafficking and terrorism.* [Meeting held in Tirana] [http://www.dsdc.gov.al/dsdc/pub/crosscutting_str_fight_against_organised_crime_177_1.pdf]

Albrecht, H-J. (n.d.) *Concepts of terrorism and organized crime.* Max-Plank Institut: Germany. [http://www.etc-graz.at/cms/fileadmin/user_upload/humsec/SAc_08_PPP/PPP_Hans_J_rg_Albrecht.pdf]

Albrecht, H-J. (n.d.) *Terrorism, organized crime and society.* Max-Plank Institut: Germany. [http://www.etc-graz.at/cms/fileadmin/user_upload/humsec/SAc_07_PPP/ALBRECHT_P,PP:pdf]

Berry, L. (et al.) (2003) *Nations hospital to organized crime and terrorism.* Library of Congress. [http://www.fas.org/irp/cia/product/frd1003.pdf]

Yvon Dandurand, Y & Chin, V. (2004) *Links between terrorism and other forms of crime.* Foreign Affairs Canada/UNDOC. [http://www.icclr.law.ubc.ca/Publications/Reports/TNOC_LINKS_STUDY_REPORT.pdf]

De Andres, A. P. (2008) *West Africa under attack: drugs, organized crime and terrorism as the new threat to global security.* UNISCI. [http://www.ucm.es/info/unisci/revistas/UNISCI%20DP%2016%20-%20Andres.pdf]

Elleman, B.A. (et al.) (eds.) (2010) *Piracy and maritime crime: historical and modern case studies.* Newport, R.I.: Naval War College Press. [*http://www.usnwc.edu/Publications/Naval-War-College-Press/Newport-Papers/Documents/35.aspx]

Engel, D. (2006) *Organized crime and terrorism in the Balkans: future risks and possible solutions.* HUMSEC. [se1.isn.ch/serviceengine/Files/ISN/102344/...6D58.../3b_Engel_1.pdf]

Fulga, G. (2005) *Combating international terrorism & cross-border organized crime. Strenghening the FIS' international partnerships.* Conflict Studies Research Centre: Russia. [http://studies.agentura.ru/centres/csrc/combating.pdf]

Helfand, N.S. (2003) *Asian organized crime and terrorist activity in Canada, 1999-2002.* Library of Congress. [http://www.loc.gov/rr/frd/pdf-files/AsianOrgCrime_Canada.pdf]

Hollywood, J. (et al.) (2004) *Out of the ordinary: finding hidden threats by analyzing unusual behavior.* Santa Monica, CA.:

RAND. [http://www.rand.org/publications/MG/MG126/]

Hudson, R. (2003) Terrorist and organized crime groups in the Tri-Border Area (TBA) of South America. Library of Congress. [http://www.jamesforest.com/wp-content/uploads/2010/05/TerrOrgCrime_TBA.pdf]

IMF (2004) *Financial Intelligence Units: An Overview.* International Monetary Fund and The World Bank Group. [http://www.imf.org/external/pubs/ft/fiu/fiu.pdf]

Joseph, J.M. (n.d.) *Organised crime and terrorism exploring linkages in South Asia.*

Institute of Peace and Conflict Studies: New Delhi. [http://www.securitytransformation.org/images/even_wor_des/Mallika_Joseph_presentation.pdf]

Kukhianidze, A. (2007) *Strengthening cooperation in the struggle against terrorism and organized crime.* CORDAID. [http://policy-traccc.gmu.edu/georgia/publications/kukhianidze/Terrorism_Org_Crime_2007_eng.pdf]

Lloyd, R.M (ed.) (2007) *Economics and maritime strategy: implications for the 21st century* . Newport, R.I.: Naval War College. [http://www.nwc.navy.mil/academics/courses/nsdm/documents/RugerPaper2Web.pdf]

Marelli, F (et al.) (2003) *Organised crime and terrorism: dancing together.* UNICRI. [http://members.multimania.co.uk/ocnewsletter/SGOC0903/marelli.pdf]

McFarlane, J. (2003) *Organised crime and terrorism in the Asia-Pacific Region: the reality and the response.* Philipps University Marburg, Germany. [http://members.multimania.co.uk/ocnewsletter/SGOC0104/JMcF.pdf]

Ouagrham-Gormley, S.B. (2007) *An unrealized Nexus? WMD-related trafficking, terrorism, and organized crime in the former Soviet Union.* Arms Control Association. [http://www.gees.org/documentos/Documen-02410.pdf]

Shelley, L.I. (et al.) (2005) *Methods and motives: exploring links between transnational organized crime & international terrorism.* NCJRS. [http://www.ncjrs.gov/pdffiles1/nij/grants/211207.pdf]

Shelley, L.I. (2003) *Organized crime , terrorism and cybercrime.* Nomos Verlagsgesellschaft, Germany. [http://www.crime-research.org/library/Terrorism_Cybercrime.pdf]

Stanislawski, B.H. & Hermann, M.G.(2004) *Transnational organized crime, terrorism, and WMD.* Syracuse University. [http://www.cidcm.umd.edu/carnegie/papers/stanislawski_hermann.pdf]

Treverton, G.F. (2005) *Making sense of transnational threats: workshop reports.* Santa Monica, CA.: RAND National Security Research. [http://www.rand.org/publications/CF/CF200/]

Treverton, G.F. (et al.) (2009) *Film piracy, organized crime and terrorism.* RAND. [http://www.rand.org/pubs/monographs/2009/RAND_MG742.pdf]

UN (2007) *Strengthening the United Nations Crime Prevention and Criminal Justice Programme, in particular its technical co-operation capacity*. [Resolution adopted by the General Assembly][http://www.iom.int/jahia/webdav/shared/shared/mainsite/policy_and_research/un/61/A_RES_61_181_EN.pdf]

UNODC (2009) *Political declaration on combating illicit drug trafficking, organized crime, terrorism and other serious crime in the Caribbean.* UNODC. [http://www.unodc.org/documents/frontpage/PolDecl-Caribbean-Feb09.PDF]

US GAO (2006) *International financial crime: Treasury's roles and responsibilities relating to selected provisions of the USA PATRIOT Act: report to the Chairman, Committee on the Judiciary, House of Representatives.*

US GAO (2006) *International financial crime: Treasury's roles and responsibilities relating to selected provisions of the USA Patriot Act.* Washington, D.C.: U.S. Govt. Accountability Office.[http://www.gao.gov/new.items/d06483.pdf]

US National Capital Planning Commission.

Interagency Task Force. (2002) *The national capital urban design and security plan.* Washington, DC.: National Capital Planning Commission. [http://www.ncpc.gov/publications/udsp/Final%20UDSP.pdf]

Vermeulen, G. (2002) *EU strategy to combat organized crime, EU anti-terrorism policy and EU-US-candidate states law enforcement.* IRCP. [http://www.ircp.org/uploaded/2002-02-07%20-%20EU%20Criminal%20Policy%20Sofia%20-A.ppt%20%5BAlleen-lezen%5D.pdf]

Wagley, J.R. (2006) *Transnational organized crime: principal threats and U.S. reponses.* CRS. [http://www.fas.org/sgp/crs/natsec/RL33335.pdf]

Walker, Justine. (2009) *Drugs trafficking and terrorism in Central Asia: an anatomy of relationships.* St.Andrews University, UK.

Wannenburg, G. (2003) *Catching the middleman fuelling African politics.* The South African Institute of International Affairs. [http://members.multimania.co.uk/oc-newsletter/SGOC0903/wburg.pdf]

Williams, P. (2006) *Strategy for a New World: combating terrorism and transnational organizations.* Oxford University Press. [http://www.oup.com/uk/orc/bin/9780199289783/baylis_chap09.pdf]

Wilson, G.I & Sullivan, J.P. (2007) *On gangs, crime, and terrorism.* Special to Defense and the National Interest. [http://www.dracosecurityconsultants.com/draco_docs/GANGS%20CRIME%20TERRORISM.pdf]

Woehrel, S. (2005) *Islamic terrorism and the Balkans*. CRS. [http://www.law.umaryland.edu/marshall/crsreports/crsdocuments/RL339012_07262005.pdf]

Prime Journal Articles

Angjeli, A. (2003) The Challenge of Terrorism and Organized Crime*. Mediterranean Quarterly* Vol.14 (3, Summer) ,pp:34-40.

Antonopoulos, G.A. (2007) Cigarette Smugglers: A Note on Four 'Unusual Suspects'. *Global Crime* Vol.8 (4) ,pp:393-398.

Bibes, P. (2001) Transnational Organized Crime and Terrorism. *Journal of Contemporary Criminal Justice* Vol.17 (3, August) ,pp:243-258. [http://www.sagepub.com/Martin2Study/pdfs/Chapter%209/Bibes%20article.pdf]

Chalk, P. (2003) Non-Military Security in the Wider Middle East. *Studies in Conflict and Terrorism* Vol.26 (3, May-June) ,pp:197-214.

Clarke, R, (2008) The PIRA, D-Company, and the Crime-Terror Nexus. *Terrorism and Political Violence* Vol. 20 (3) ,pp:376-395.

Cornell, S. (2007) Narcotics and Armed Conflict: Interaction and Implications. *Studies in Conflict and Terrorism.* Vol.30 (3, March) ,pp:207-227.

Davies, S. (2006) A case of mistaken identity. *Significance* Vol.3 (3, September) ,pp:114-117.

Di Filippo, M. (2008) Terrorist Crimes and International Co-operation: Critical Remarks on the Definition and Inclusion of Terrorism in the Category of International Crimes. *European Journal of International Law* Vol.19 (3, June) ,pp:533-570.

Fletcher N.B. & DiPerna, T.A. (2007) The rule of law: An essential component of the financial war against organized crime and terrorism in the Americas. *Journal of Financial Crime* Vol.14 (4) ,pp:405-437.

Flyghed, J. (2005) Crime-Control in the Post-Wall Era: The Menace of Security. *Journal of Scandinavian Studies in Criminology and Crime Prevention* Vol.6 (2, December) ,pp:165-182.

Fox, J.A.& Levin, J. (2003) Mass Murder: An Analysis of Extreme Violence. *Journal of Applied Psychoanalytic Studies* Vol.5 (1, January) ,pp:47-64.

Garoupa, N., Klick, J. & Parisi, F. (2006) A law and economics perspective on terrorism. *Public Choice* Vol.128 (1-2) ,pp:147-168.

Helms, L. (2009) The liberal-democratic foundations of the European nation-state and the challenges of internationalization. *International Politics* Vol.46 (1, January) ,pp:48-64..

Jasparro, C. & Taylor, J. (2008) Climate

Change and Regional Vulnerability to Transnational Security Threats in Southeast Asia. *Geopolitics* Vol.3 (2, April) ,pp:232-256.

Keyzer, M. (2002) Labeling and the Realization of Cultural Values. *De Economist* Vol.150 (4, October) ,pp:487-511.

Leong, A. & Mei, V. (2005) Definitional analysis: the war on terror and organised crime. *Journal of Money Laundering Control* Vol.3 (1) ,pp:19-36.

Levi, M. (2006) The Media Construction of Financial White-Collar Crimes. *British Journal of Criminology* Vol.46 (6, November) ,pp:1037-1057.

Makarenko, T. (2004) The Crime-Terror Continuum: Tracing the Interplay between Transnational Organised Crime and Terrorism. *Global Crime* Vol. 6 (1) ,pp:129-124.

Mares, D. (2009) Institutions, the Illegal Drug Trade, and Participant Strategies: What Corrupt or Pariah States Have In Common with Liberal Democracy and the Rule of Law. *International Interactions* Vol.35 (2, April) ,pp:207-239

McDougall, D. (2007) Insecurity in Oceania: An Australian perspective. *The Round Table* Vol.96 (4, August) ,pp:415-427.

Mullins, S. (2009) Parallels Between Crime and Terrorism: A Social Psychological Perspective. *Studies in Conflict and Terrorism* Vol.39 (9, September) ,pp:811-830.

Nemeth, E. (2007) Cultural Security: The Evolving Role of Art in International Security. *Terrorism and Political Violence* Vol.19 (1, March) ,pp:19-42.

O'Connor, Denis (2010) Performance from the Outside-In. *Policing* Vol. 4 (2) ,pp:152-6.

Orlova, A.V. (2008) Russia's anti-money laundering regime: law enforcement tool or instrument of domestic control? *Journal of Money Laundering Control,* Vol.11(3) ,pp:210-233

Picarelli, J.T. (2006) The Turbulent Nexus Of Transnational Organised Crime and Terrorism: A Theory of Malevolent International Relations. *Global Crime* Vol.7 (1) ,pp:1-24.

Pratt, A. (2004) Human Trafficking: The Nadir of an Unholy Trinity. *European Security* Vol.13 (1-2) ,pp.55-71.

Ridley, N. (2008) Organized Crime, Money Laundering, and Terrorism. *Policing* Vol.2 (1) ,pp:28-35.

Roth, M.P. & Sever, M. (2007) The Kurdish Workers Party (PKK) as Criminal Syndicate: Funding Terrorism through Organized Crime, A Case Study. *Studies in Conflict and Terrorism* Vol.30 (10, October) ,pp:901-920.

Rudner, M. (2001) Canada's Communications Security Establishment from Cold War to Globalization. *Intelligence and National Security* Vol.16 (1, Spring),'pp:97-128.

Saw, D. G. (2004) Interdicting tainted wealth - the perspective from Hong Kong. *Journal of Money Laundering Control* Vol.7 (3), pp: 275-280.

Shelley, L.I. & Melzer, S.A. (2008) The Nexus of Organized Crime and Terrorism: Two Case Studies in Cigarette Smuggling. *International Journal of Comparative and Applied Justice* Vol.32 (1, Spring) , pp:1-21. [http://policy-traccc.gmu.edu/resources/publications/Shelley_Melzer.pdf]

Shelley, L.I. & Picarelli, J.T. (2002) Methods Not Motives: Implications of the Convergence of International Organized Crime and Terrorism. *Police Practice and Research* Vol.3 (4), pp. 305-318.

Singh, S. (2007) The risks to business presented by organised and economically motivated criminal enterprises. *Journal of Financial Crime* Vol.14 (1) ,pp. 79-83.

Sörensen, J.S. (2006) The Shadow Economy, War and State Building: Social Transformation and Re-stratification in an Illiberal Economy (Serbia and Kosovo). *Journal of Contemporary European Studies* Vol.14 (3) ,pp. 317-351.

Stodiek, T. (2009) OSCE's police-related activities: Lessons-learned during the last decade. *Security and Human Rights* Vol.20(3) ,pp. 201-220.

Thorne, K. (2005) Designing virtual organizations? Themes and trends in political and organizational discourses. *The Journal of Management Development* Vol.24

(7) ,pp. 580-607.

Trim, P. R.J. (2003) Disaster management and the role of the intelligence and security services. *Disaster Prevention and Management: An International Journal* Vol.12(1) ,pp. 6-15.

UN (2005) Poverty, Infectious Disease, and Environmental Degradation as Threats to Collective Security: A UN Panel Report. *Population and Development Review* Vol.33 (3, September) ,pp. 595-600.

Walker, C. (2006) Clamping Down on Terrorism in the United Kingdom. *Journal of International Criminal Justice* Vol.4 (5), pp. 1137-1151.

Wiebes, C. (2001) Dutch Sigint during the Cold War, 1945-94. *Intelligence and National Security* Vol.16 (1, Spring), pp:243-284.

Yusuf, I. (2007) The Southern Thailand Conflict and the Muslim World. *The Southern Thailand Conflict and the Muslim World* Vol.27 (2, August), pp:319-339.

Zhu, L. (2010) Chinese Practice in Public International Law: 2009. *Chinese Journal of International Law* Vol.9 (3, September) , pp:607-662.

Providing clean and safe air in hostile environments

CBRN Protection for asymmetric warfare scenarios

Beth-El Industries Ltd.

Beth-El Industries is a leading developer, designer and manufacturer of Environmental Protection Systems. We cover the whole spectrum of CBRN/TIC protection applications as well as air-conditioning systems for vehicles, containers, army tents, large bomb shelters and biological isolation systems. At this time, Beth-El's cutting edge CBRN/TIC filtration technology is being used by more than 60 armies worldwide, many of which are NATO and PfP forces.

Vehicle Filtration/AC System

Tent Filtration System

Container Filtration System

CERTIFIED QMS SI ISO 9001 2115
THE STANDARDS INSTITUTION OF ISRAEL

nqa.
AS EN 9100
Registered

NATO-Supplier-No.
SH785

Certified Quality
Assurance Program
according to AQAP-2110

New Upcoming Events

Conferences, Workshops and Important events around the globe

Public Health Emergency Medical Countermeasures Enterprise Stakeholders Workshop (January 10-12; Washington, DC) The workshop will cover the Health and Human Services Secretary's Medical Countermeasure Review and Recommendations, the National Health Security Strategy and Biennial Implementation Plan, medical countermeasures as a foundation of national health security, pre-event positioning of medical countermeasures, and medical countermeasure development. ***View event website***

EMERGENCY
MANAGEMENT ASIA 2010

(January 12-13; Bangkok, Thailand) In its inaugural year, this conference will address interoperability in both risk management and crisis management. Drawing on regional and international expertise, delegates can expect to project lessons learned and real scenarios onto their own current and future projects and plans. Emergency Management Asia will also focus on the development phase of disaster management to implement best practice planning and policy execution. This event is supported by the International Emergency Management Society, which will initiate a chapter in the Association of Southeast Asian Nations. ***View event website***

State Border Coordination Workshop (January 24-25; Gettysburg, PA) This workshop presented by the All Hazards Consortium aims to update the Regional Catastrophic Planning Grant Program, determine the next steps in other initiatives, and look to a long-term coordinated plan covering transportation, interoperability and situational awareness, mass care, credentialing, and resource management for North Carolina, Virginia, Maryland, West Virginia, Pennsylvania, Delaware, New Jersey, New York, and Washington, DC. ***View event website***

DISASTER
MANAGEMENT
SHOWCASE & CONFERENCE

(January 24-26; Vienna, VA) The showcase and conference will focus on the acquisition priorities and gaps in communication plans with easily understandable terminology and methods; proper maintenance and training of emergency services, including mass human resources such as community emergency response teams; developing and exercising emergency population warning methods combined with emergency shelters and evacuation plans; and stockpiling, inventorying, and maintaining disaster supplies and equipment. ***View event website***

25 WORKING TOGETHER
EMERGENCY SERVICES MIDWEST
CONFERENCE & EXPOSITION

(January 26-29; Milwaukee) The conference presents classes on firefighting and rescue operations, the latest information for emergency service providers of all types, and a 90,000-square-foot exhibit hall. ***View event website***

21st ANNUAL MONROEVILLE FIRE SHOW (February 12-13; Monroeville, PA) One of the nation's largest and best-attended trade shows for firefighters, paramedics, emergency medical technicians, and other emergency services personnel brings together over 100 companies to showcase thousands of products and services. ***View event website***

CBRNE Defense (February 14-16; Vienna, VA) This forum will discuss preparedness, incident management, threat reduction, advanced technologies, interoperability, and medical countermeasures to prevent, detect, protect against, and respond to chemical, biological, radiological, nuclear, and high-yield explosives attack. ***View event website***

AFCEA Homeland Security Conference (February 22-24; Washington, DC) The theme of this Armed Forces Communications & Electronics Association conference is "Working Together Today for a More Secure Tomorrow." It will cover identity management and interagency collaboration, Homeland Security Department and state and local secure information sharing, border security, person-centric screening, situational awareness, training and education, and privacy vs. security. Roundtables will feature chief information officers, procurement executives, and executives from the Federal Emergency Management Agency, the National Weather Service, and the National Communications System. ***View event website***

EMS TODAY (March 1-5; Baltimore) Emergency Medical Services Today offers clinical topics, presented by leaders in the field; hundreds of the newest products and technologies in the exhibit hall; and networking events to connect thousands of emergency medical services professionals. ***View event website***

Campus Fire Safety and Risk Management Professional Development Conference & Expo (March 7-8; Columbus, OH) This annual conference provides educational workshops on campus fire safety, security, and risk management. It will include a Campus Fire Department Symposium specifically for campus fire departments and fire departments that respond on campus and rely on students as part of their emergency response staffing. ***View event website***

GLOBAL SECURITY ASIA 2011 (March 15-17; Singapore) The conference seeks to discuss the challenges that governments and homeland security professionals face in their fight against terrorism and to offer possible technological solutions to counter the lurking threats. Highly qualified and established experts in the homeland security industry will be assembled to present a well-balanced program covering geopolitical and technological topics. ***View event website***

50th Annual Emergency Management Conference (February 22-23; Wellington, New Zealand) This conference provides an early opportunity to hear from those who played crucial roles in responding to the September Canterbury earthquake and to learn from those who have expertise and experience in disaster risk management in a wider sense. It is an opportunity to learn, to check assumptions against the realities of an emergency, and to contribute to further enhance capability and capacity to cope with a major emergency. ***View event website***

Bridging the Gaps: Public Health and Radiation Emergency Preparedness (March 21-24; Atlanta) The Radiation Studies Branch at the Centers for Disease Control and Prevention is sponsoring this conference on public health preparedness for radiation emergencies and the need for mass-casualty education and emergency response planning resources. ***View event website***

(March 29-30; London) This conference on resilience to chemical, biological, radiological, or nuclear attack promises a panel of senior experts, first responders, and military personnel. It will address key developments in response and recovery; provide a forum for sharing experiences, best practices, and ideas; and focus on training and interoperability during the build-up to the 2012 Olympics. ***View event website***

Government Security Expo and Conference (March 29-31; Washington, DC) This conference offers training and skills to meet the challenges facing safety, security, and law enforcement professionals. Experts will discuss solutions to pressing issues in physical and cybersecurity, critical infrastructure protection, advanced persistent threats, attacks and emergencies, and law enforcement. ***View event website***

The main theme of the International Disaster and Emergency Resilience conference, hosted by the University of Florence, Centre for Civil Protection and Risk Studies, will be "The Impact of Climate Change," with particular focus on community resilience and integrated disaster management. It will include case studies, community resilience, integrated emergency response, vital resources in disaster response, and medical aspects of disasters. ***View event website***

International Conference on Intelligence and Security Informatics (July 10-12; Beijing) This conference of the Institute of Electrical and Electronics Engineers will focus on information sharing and data/text mining, infrastructure protection and emergency responses, terrorism informatics, and enterprise risk management and information systems security. The deadline for submitting papers is March 1. ***View call for papers***

Second International Workshop on Intelligent Technologies for Counter Terrorism and Security (July 20-24; Kochi, Kerala, India) In conjunction with the International Conference on Advances in Computing and Communications, this workshop will bring together academics and security and counterterrorism practitioners and developers to present the latest intelligent technologies to combat terrorism and to protect critical infrastructures, people, and society and provide a venue to present early work in applying various intelligent technologies. The deadline for submitting papers is March 1. ***View call for papers***

European Intelligence & Security Informatics Conference (September 12-14; Athens, Greece) This conference will gather people from previously disparate communities—researchers in information technologies, computer science, public policy, bioinformatics, medical informatics, and social and behavior studies as well as local, state, and federal law enforcement and intelligence experts, along with information technology in-

dustry consultants and practitioners—to support counterterrorism and homeland security missions of anticipation, interdiction, prevention, preparedness, and response to terrorist acts. The deadline for submitting papers is April 11. ***View call for papers***

International Defense and Homeland Security Simulation Workshop (September 28-30; Rome) This workshop will focus on the advances and potential of using modeling and simulation in defense and homeland security applications. It will bring experts together to present and discuss all type of innovation: new concepts, methods, techniques, and tools. The submission deadline is April 15. ***View call for papers***

Sponsored by:
ARINC, Cassidian Systems, CAE Aviation, Foster & Freeman, L-3 WESCAM, Regula Baltija, Senstar Corporation, Southwest Microwave

SMi 's 4th annual Border Security conference, is Europe's leading event dedicated to bringing together industry experts to examine the latest challenges facing the international border management community.

Held in partnership with Borderpol, *the World Border Organisation,* this must attend event will present an exceptional line-up of key speak ers, special addresses from Borderpol and an outstanding programme covering themes including border crime, interoperability and biometrics – this is an event not to be missed!

2011 NATIONAL SPORTS SAFETY AND SECURITY
CONFERENCE & EXHIBITION
AUGUST 2 - 4 | NEW ORLEANS

"An opportunity for vendors to showcase safety and security solutions for pre-game crowd surge issues to Sports Industry management/ security personnel, as well as a chance for security and stadium operators to explain operational/ technological needs for gate crowding issues at sports venues for today and tomorrow."

http://www.ncs4.com/conference/

17th World Congress on Disaster and Emergency Medicine
31 May–3 June 2011 Beijing, China

http://www.wcdem2011.org/

WADEM is an academic, international, humanitarian association dedicated to the improvement of prehospital and emergency health care, public health, and disaster health and preparedness. It is a non-operational, non-governmental organization with a primary focus on education and research. Its members are multidisciplinary and span the globe, representing 55 countries. WADEM publishes a widely read, peer-reviewed medical journal, *Prehospital and Disaster Medicine,* which is currently in its 25th volume.
NOTE: There will be a CBRN section too!

International Congress Secretariat:
International Conference Services Ltd.
2101 - 1177 West Hastings St.,
Vancouver, BC Canada V6E 2K3
Phone: +1 (604) 681 2153
Fax: +1 (604) 681 1049

Preliminary program
http://www.wadem.org/documents/17th_wcdem_preliminary_prog.pdf

International Symposium on Agroterrorism

The food and agricultural sectors of all nations are vulnerable to terrorism incidents or threats. With worldwide cooperation, collaboration, and information-sharing among representatives from governments, the private sector, and academia, the potential for agroterrorism can be reduced.
The main mission of the International Symposium on Agroterrorism (ISA) is to protect the food supply worldwide while illustrating the importance of a coordinated effort.

http://www.fbi-isa.org/

More than 1,000 individuals from 21 different countries have attended past ISAs, participating in break-out educational sessions and case studies, hearing world-renowned experts discuss agroterrorism, and interacting with each other. Attendance is expected to be even greater in 2011. An exhibit hall will provide ISA sponsors and exhibitors an opportunity to showcase relevant products and services. Coming together under one roof is the first step toward working together to solve the problem.

Goals of the Symposium

- Prevent acts of Agroterrorism through well-coordinated intelligence collection, analysis, and dissemination processes.
- Develop technical and tactical response strategies to neutralize and eliminate a potential attack.
- Provide an opportunity for education across a variety of disciplines regarding threats directed at the world's food supply.
- Provide an avenue to share ideas and information among attendees through meaningful dialogue and networking opportunities.

http://www.icbrnevents.com/

Turkey has always been the cross-roads of the world. Poised with one foot on the European side of the Bosphorous while the other is in Asia, it has the second largest land army in Nato and many security challenges.

A secular government faces the threat from fundamentalists and from radical terrorists - with state sponsors. Istanbul, while not the capitol, is at the heart of this challenge, the largest city in Turkey, home to its major religious and cultural centres, yet at the same time it has the challenge of millions of Western tourists and waves of arrivals from the Turkish interior and beyond. The security challenges that Turkey faces are very similar to many other parts of the world and Turkey has been steadily developing it's CBRN defence, to go along with its advanced Counter IED capability. This is your chance to learn what Turkey and some of the best minds in CBRN and Counter IED have been developing. Along with the Conference will be a pre-conference workshop and we are hoping the final day will also have a dynamic demonstration.

Need a professional speaker?

Source: http://www.speakersite.com

Find a Speaker

...or try one of our featured speakers.

Search for your topic or speaker

Are you a Speaker? Click here to Create a Profile

Dr. Ronald G. Shapiro PhD, CHFP

Who Searches at SpeakerSite:

Hospital Management of Chemical, Biological, Radiological, Nuclear & Explosive Incidents (January 31–February 4; Aberdeen, MD) This postgraduate course for emergency planners, hospital administrators, clinicians, and emergency responders, presented by the U.S. Army Medical Research Institute of Chemical Defense, offers an overview of all chemical, biological, radiological, nuclear, and explosive fields, including the psychology of such events, as well as principles of hospital emergency management, regulatory frameworks, equipment and procedure demonstrations, and a multi-station practical exercise. ***View course website***

Earthquakes: Mean Business (February 4; St. Louis) This free seminar at St. Louis University, offered by the regional geoscience, engineering, and emergency management community, will showcase the issue of earthquake hazards and earthquake risk in the central United States and how we can better prepare for it. ***View seminar website***

Anhydrous Ammonia Awareness Training Tour (February 15–July 16; California, Arizona, Iowa, and Nebraska) Transcaer's 2011 tour to provide emergency responder training on anhydrous ammonia and transport will offer more than 60 training days in four states. The complete schedule is on the Transcaer website. ***View course website***

Behind the Scenes Seminar of Israel's Counter-Terrorism and Security Operations (February 19-26; Israel) The sessions and site visits provide a unique inside look at Israel's security threats and mitigation methods, with emphasis on protecting critical infrastructure and key national and local assets: airports, mass-transit hubs, government facilities, border crossings, and shopping malls. The curriculum covers many Israeli agencies involved in counterterrorism, threat identification and mitigation, emergency preparedness and response, and innovations in security technology. Discussions will focus on the key concepts underlying the Israeli practices, their application to the participants' counterterrorism strategies, and challenges in adopting and sustaining the concepts and practices in diverse environments. ***View seminar website***

Field Management of Chemical and Biological Casualties (February 28–March 4, April 11-15, June 6-10; Aberdeen, MD) This course, presented by the U.S. Army Medical Research Institute of Chemical Defense, offers pre-hospital training for medics, early responders, Chemical Corps, and health care personnel. It comprises three days of field training with lab time, procedure practice, and three field training exercises, plus classroom work and time using advanced simulators. ***View course website***

C-TPAT Supply Chain Security Training Seminar (March 29-31; San Diego) This Customs-Trade Partnership Against Terrorism is free, but only companies certified or validated by the partnership may attend. ***View seminar website***

Medical Management of Chemical and Biological Casualties (March 20-26, May 1-6; Aberdeen, MD, and Fort Detrick, MD) This course, presented by the U.S. Army Medical Research Institute of Chemical Defense, offers postgraduate training for definitive health care providers, combining lab work in cholinergic crisis, patient diagnosis, treatment, and procedures; patient triage and interview exercises; crisis management in a mega-code environment with robotic manikins; a visit to a Biosafety Level 4 laboratory; and practical field training, performed in protective gear. ***View course website***

4th Conference on Global Preparedness and Resilience (March 16-17; Melbourne, FL) This conference, organized by the Florida Tech Global Center for Preparedness and Resilience, will focus on global resilient technologies and infrastructure. It has four interlinked themes presented over the two days of the conference: “Global Demand for Integrated Preparedness,” “Resilient Technological Applications,” “Resilient Infrastructure Applications,” and “Resiliency Forecasting–New Global Index.” ***View event website***

Bridging the Gaps: Public Health and Radiation Emergency Preparedness (March 21-24; Atlanta) The Radiation Studies Branch at the Centers for Disease Control and Prevention is sponsoring this conference on public health preparedness for radiation emergencies and the need for mass-casualty education and emergency response planning resources. ***View event website***

(February 14-16; Vienna, VA) This forum will discuss preparedness, incident management, threat reduction, advanced technologies, interoperability, and medical countermeasures to prevent, detect, protect against, and respond to chemical, biological, radiological, nuclear, and high-yield explosives attack. ***View event website***

European Intelligence & Security Informatics Conference (September 12-14; Athens, Greece) This conference will gather people from previously disparate communities—researchers in information technologies, computer science, public policy, bioinformatics, medical informatics, and social and behavior studies as well as local, state, and federal law enforcement and intelligence experts, along with information technology industry consultants and practitioners—to support counterterrorism and homeland security missions of anticipation, interdiction, prevention, preparedness, and response to terrorist acts. The deadline for submitting papers is April 11. ***View call for papers***

MeMC MEDITERRANEAN EMERGENCY MEDICINE CONGRESS

KOS, Greece

10-14 September 2011

The European Society for Emergency Medicine (EuSEM) is a non-profit making scientific organisation whose aim is to promote and foster the concept, philosophy and the art of Emergency Medicine throughout Europe. The ultimate objective of the Society is to help and support European nations to achieve the specialty of Emergency Medicine.
Born as a Society of individuals in 1994 from a multidisciplinary group of experts in Emergency Medicine (the Club of Leuven), EuSEM changed its Statutes in 2005, so that the Society now also represents national societies of Emergency Medicine as well as its members.
Call for papers: http://www.eusem.org/

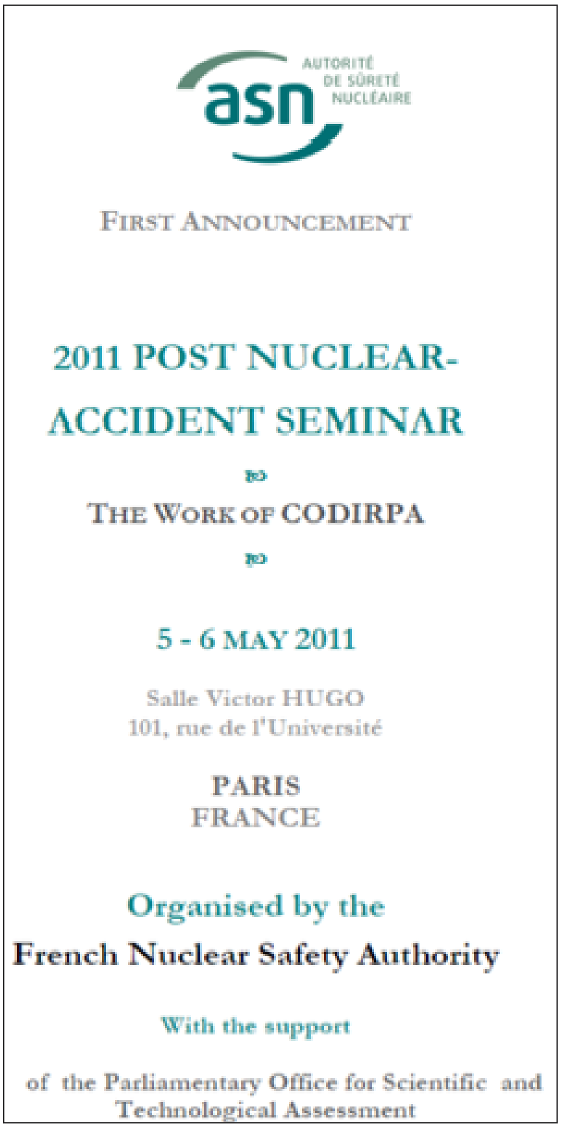
CBRN Training Curriculum End-User Workshop (March 10; The Hague, Netherlands) At this chemical, biological, radiological, and nuclear advanced training curriculum workshop, national and international organizations will present training programs and curricula. Attendees will develop an inventory of end-user requirements. The project aims to meet the demand for education, training, and exercising of first responders to potential CBRN incidents in The Hague, eventually providing a European standard. ***View event website***

CBMTS Industry VII - «World Congress on the CBRN Threat and Terrorism»
Hotel Croatia, Cavtat - Dubrovnik, Croatia ; 10 - 15 April 2011)

- Organizing Committee: Security Magazine Zaštita (Protection) – TECTUS d.o.o. and DEFIMI d.o.o. R&D services in the field of protection and defense
- Under the high patronage of the Government of the Republic of Croatia
- **Pre-Congress Workshop:** OPCW International Workshop (Hotel Croatia, Cavtat - Dubrovnik, Croatia; 09 - 10 April 2011)
- Official language of CBMTS Industry VII is English without interpretation!

View event website

2011 Post-nuclear Accident Seminar



AUTORITÉ DE SÛRETÉ NUCLÉAIRE
asn

FIRST ANNOUNCEMENT

2011 POST NUCLEAR-ACCIDENT SEMINAR

THE WORK OF CODIRPA

5 - 6 MAY 2011

Salle Victor HUGO
101, rue de l'Université

PARIS
FRANCE

Organised by the
French Nuclear Safety Authority

With the support

of the Parliamentary Office for Scientific and Technological Assessment

Nuclear activities are undertaken in a fashion designed to avoid accidents, and to limit their possible consequences. Conforming with the principle of defence in depth, many mechanisms and approaches are put in place to address radiological accident situations, even those of low probability. Historically, focus is aimed towards the management of the accident situation itself, however it now seems necessary to focus more on the management of the post-accident phase of an accident.

The CODIRPA programme was started in June 2005 by the ASN, and was charged with developing French policy for the management of the post-accident phase of a nuclear or radiological accident situation. An ambitious programme mobilising more than 200 people was put in place, including representatives of relevant national administrations and their local representatives, utility and industrial representatives, technical service organisations, nuclear safety authorities from bordering countries to France, NGOs and local elected officials.

To compliment activities addressing policy at the national level, several dialogue processes were engaged with organisations and officials from local governmental administrations, with relevant services from the agricultural ministry, and with civil society representatives in order to test ideas and approaches against local realities. In this context, the first operational CODIRPA product, the guide for leaving the urgent phase, is currently being adapted for local application.

Registration: Participation is by invitation, and without fee
Registration Deadline: 14 January 2011
The number of invitees for this conference is limited, and as such we invite you to confirm you participation as soon as possible at the following web-site: seminairepostaccident@asn.fr

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:

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.

Who should attend?

- First responders
- Proprietors of critical infrastructure
- Private security staff and personnel
- Policy makers

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.

*subject to final confirmation

POST-CONFERENCE WORKSHOP B 13TH APRIL 2011

In association with:

Countering the Terrorist Threat of an IED with a Chemical Payload

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.

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

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.

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 assesed 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.

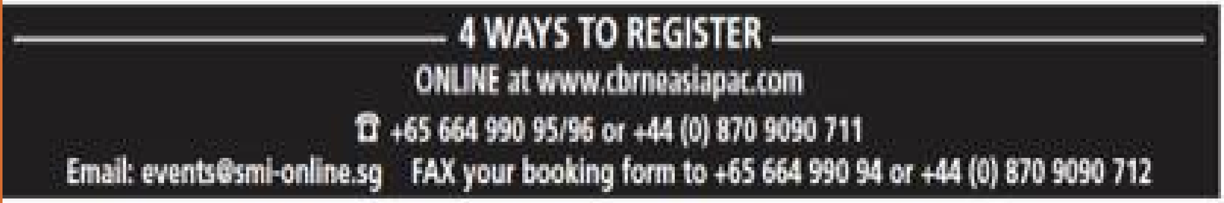
Who should attend?

- 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

CBRN-E Asia-Pacific

Preparing for the Modern Threat

11th & 12th April 2011
Grand Copthorne Waterfront Hotel, Singapore



4 WAYS TO REGISTER

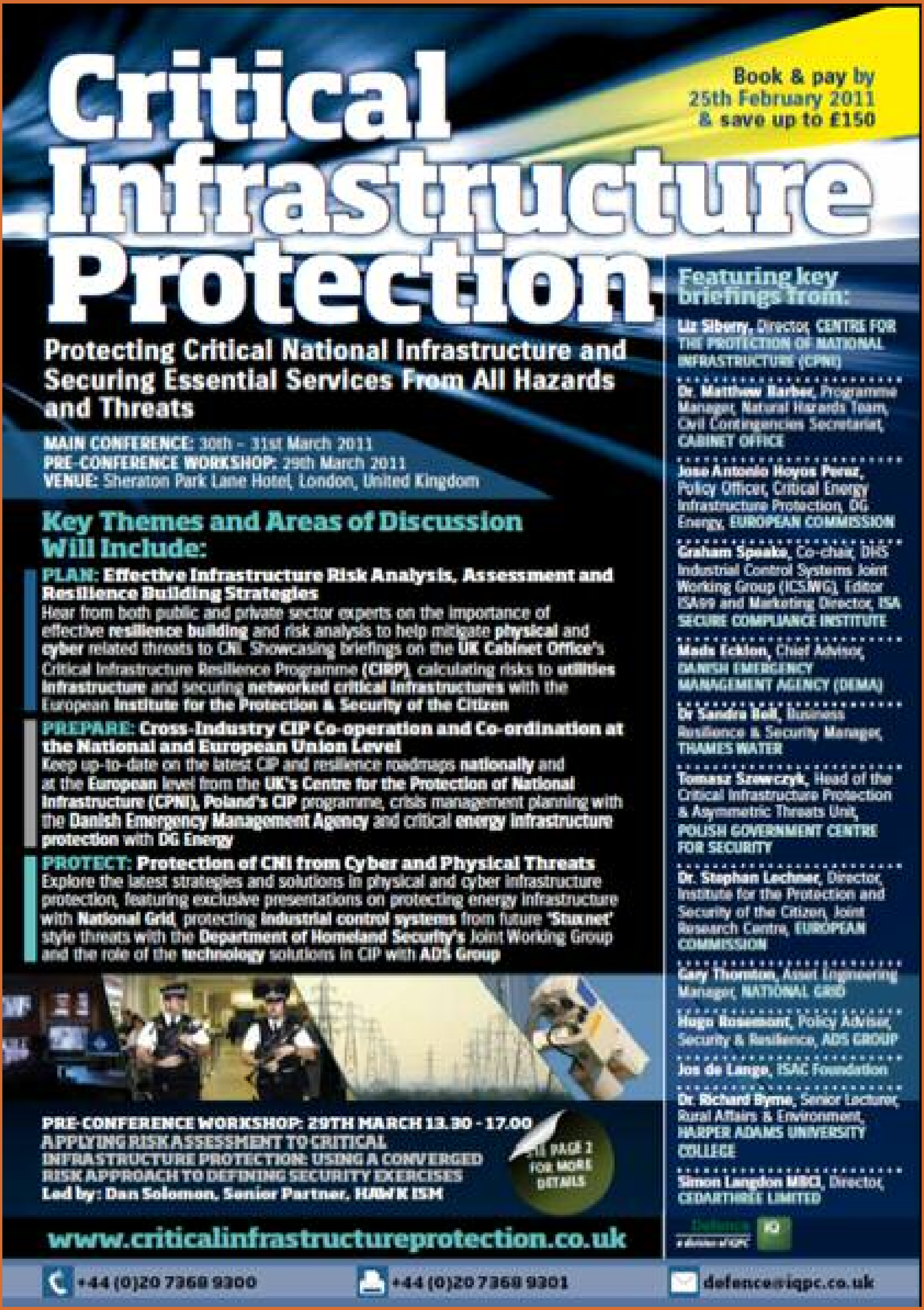
ONLINE at www.cbrneasiapac.com

☎ +65 664 990 95/96 or +44 (0) 870 9090 711

Email: events@smi-online.sg FAX your booking form to +65 664 990 94 or +44 (0) 870 9090 712

Conference and Exhibition Supported By:

RIEAS (www.rieas.gr) supports this very important CBRN conference



Critical Infrastructure Protection

Book & pay by 25th February 2011 & save up to £150

Protecting Critical National Infrastructure and Securing Essential Services From All Hazards and Threats

MAIN CONFERENCE: 30th - 31st March 2011
PRE-CONFERENCE WORKSHOP: 29th March 2011
VENUE: Sheraton Park Lane Hotel, London, United Kingdom

Key Themes and Areas of Discussion Will Include:

PLAN: Effective Infrastructure Risk Analysis, Assessment and Resilience Building Strategies
Hear from both public and private sector experts on the importance of effective **resilience building** and risk analysis to help mitigate **physical** and **cyber** related threats to CNI. Showcasing briefings on the **UK Cabinet Office**'s Critical Infrastructure Resilience Programme **(CIRP)**, calculating risks to **utilities infrastructure** and securing **networked critical infrastructures** with the European **Institute for the Protection & Security of the Citizen**

PREPARE: Cross-Industry CIP Co-operation and Co-ordination at the National and European Union Level
Keep up-to-date on the latest CIP and resilience roadmaps **nationally** and at the **European** level from the **UK's Centre for the Protection of National Infrastructure (CPNI), Poland's CIP** programme, crisis management planning with the **Danish Emergency Management Agency** and critical **energy infrastructure protection** with **DG Energy**

PROTECT: Protection of CNI from Cyber and Physical Threats
Explore the latest strategies and solutions in physical and cyber infrastructure protection, featuring exclusive presentations on protecting energy infrastructure with **National Grid**, protecting **industrial control systems** from future **'Stuxnet'** style threats with the **Department of Homeland Security's** Joint Working Group and the role of the **technology** solutions in CIP with **ADS Group**

PRE-CONFERENCE WORKSHOP: 29TH MARCH 13.30 - 17.00
APPLYING RISK ASSESSMENT TO CRITICAL INFRASTRUCTURE PROTECTION: USING A CONVERGED RISK APPROACH TO DEFINING SECURITY EXERCISES
Led by: Dan Solomon, Senior Partner, HAWK ISM

SEE PAGE 2 FOR MORE DETAILS

Featuring key briefings from:

Liz Sibury, Director, CENTRE FOR THE PROTECTION OF NATIONAL INFRASTRUCTURE (CPNI)

Dr. Matthew Barber, Programme Manager, Natural Hazards Team, Civil Contingencies Secretariat, CABINET OFFICE

Jose Antonio Hoyos Perez, Policy Officer, Critical Energy Infrastructure Protection, DG Energy, EUROPEAN COMMISSION

Graham Speake, Co-chair, DHS Industrial Control Systems Joint Working Group (ICSJWG), Editor ISA99 and Marketing Director, ISA SECURE COMPLIANCE INSTITUTE

Mads Ecklon, Chief Advisor, DANISH EMERGENCY MANAGEMENT AGENCY (DEMA)

Dr Sandra Bell, Business Resilience & Security Manager, THAMES WATER

Tomasz Szewczyk, Head of the Critical Infrastructure Protection & Asymmetric Threats Unit, POLISH GOVERNMENT CENTRE FOR SECURITY

Dr. Stephan Lechner, Director, Institute for the Protection and Security of the Citizen, Joint Research Centre, EUROPEAN COMMISSION

Gary Thornton, Asset Engineering Manager, NATIONAL GRID

Hugo Rosemont, Policy Adviser, Security & Resilience, ADS GROUP

Jos de Lange, ISAC Foundation

Dr. Richard Byrne, Senior Lecturer, Rural Affairs & Environment, HARPER ADAMS UNIVERSITY COLLEGE

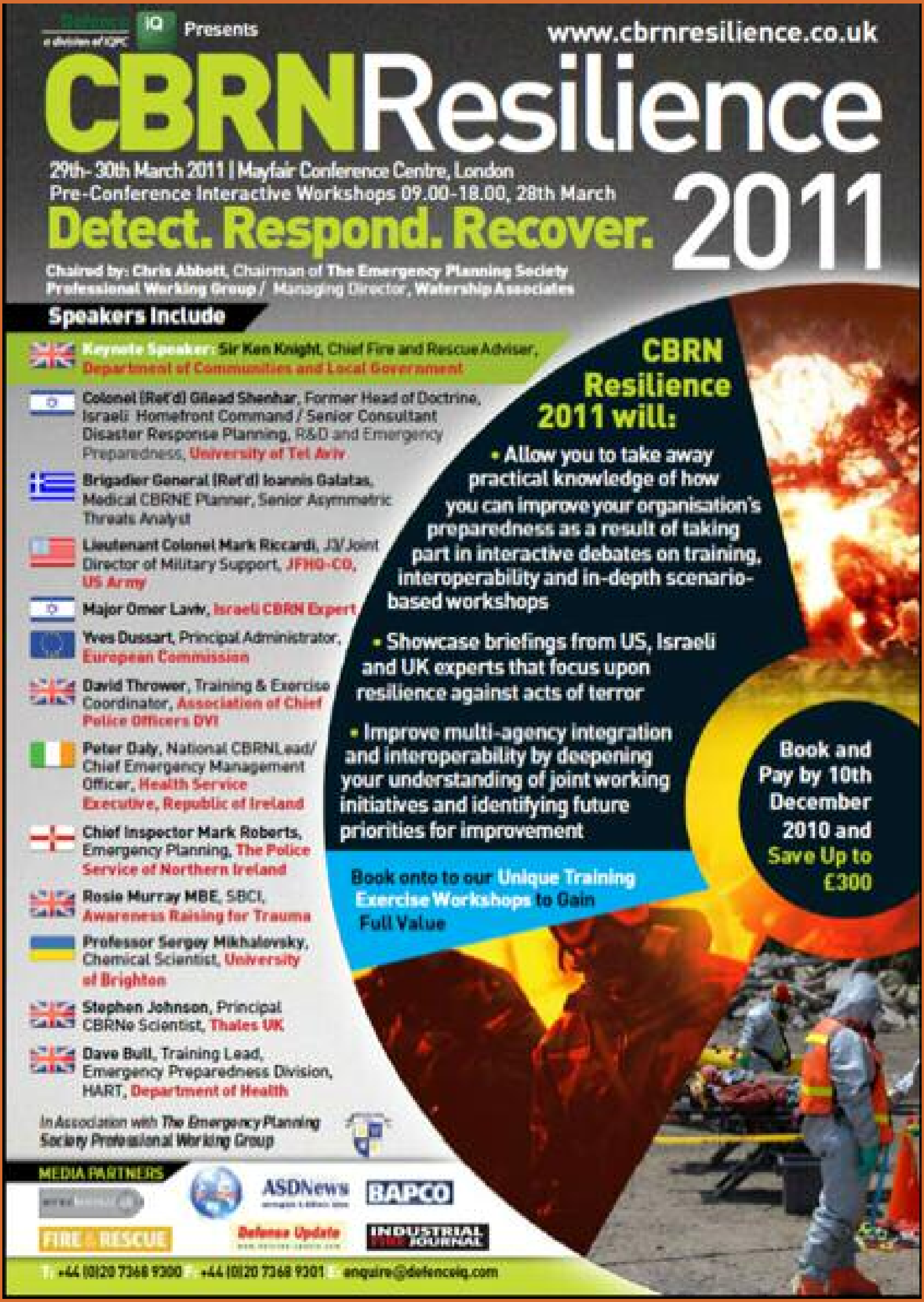
Simon Langdon MBCI, Director, CEDARTHREE LIMITED

www.criticalinfrastructureprotection.co.uk

☎ +44 (0)20 7368 9300

+44 (0)20 7368 9301

defence@iqpc.co.uk



Defence IQ a division of IQPC Presents

www.cbrnresilience.co.uk

CBRNResilience 2011

29th- 30th March 2011 | Mayfair Conference Centre, London
Pre-Conference Interactive Workshops 09.00-18.00, 28th March

Detect. Respond. Recover.

Chaired by: **Chris Abbott**, Chairman of **The Emergency Planning Society Professional Working Group** / Managing Director, **Watership Associates**

Speakers Include

- **Keynote Speaker: Sir Ken Knight**, Chief Fire and Rescue Adviser, **Department of Communities and Local Government**
- **Colonel (Ret'd) Gilead Shenhar**, Former Head of Doctrine, Israeli Homefront Command / Senior Consultant Disaster Response Planning, R&D and Emergency Preparedness, **University of Tel Aviv**
- **Brigadier General (Ret'd) Ioannis Galatas**, Medical CBRNE Planner, Senior Asymmetric Threats Analyst
- **Lieutenant Colonel Mark Riccardi**, J3/ Joint Director of Military Support, **JFHQ-CO, US Army**
- **Major Omer Laviv**, **Israeli CBRN Expert**
- **Yves Dussart**, Principal Administrator, **European Commission**
- **David Thrower**, Training & Exercise Coordinator, **Association of Chief Police Officers DVI**
- **Peter Daly**, National CBRNLead/ Chief Emergancy Management Officer, **Health Service Executive, Republic of Ireland**
- **Chief Inspector Mark Roberts**, Emergency Planning, **The Police Service of Northern Ireland**
- **Rosie Murray MBE**, SBCI, **Awareness Raising for Trauma**
- **Professor Sergey Mikhalovsky**, Chemical Scientist, **University of Brighton**
- **Stephen Johnson**, Principal CBRNe Scientist, **Thales UK**
- **Dave Bull**, Training Lead, Emergency Preparedness Division, HART, **Department of Health**

In Association with *The Emergency Planning Society Professional Working Group*

CBRN Resilience 2011 will:

- Allow you to take away practical knowledge of how you can improve your organisation's preparedness as a result of taking part in interactive debates on training, interoperability and in-depth scenario-based workshops
- Showcase briefings from US, Israeli and UK experts that focus upon resilience against acts of terror
- Improve multi-agency integration and interoperability by deepening your understanding of joint working initiatives and identifying future priorities for improvement

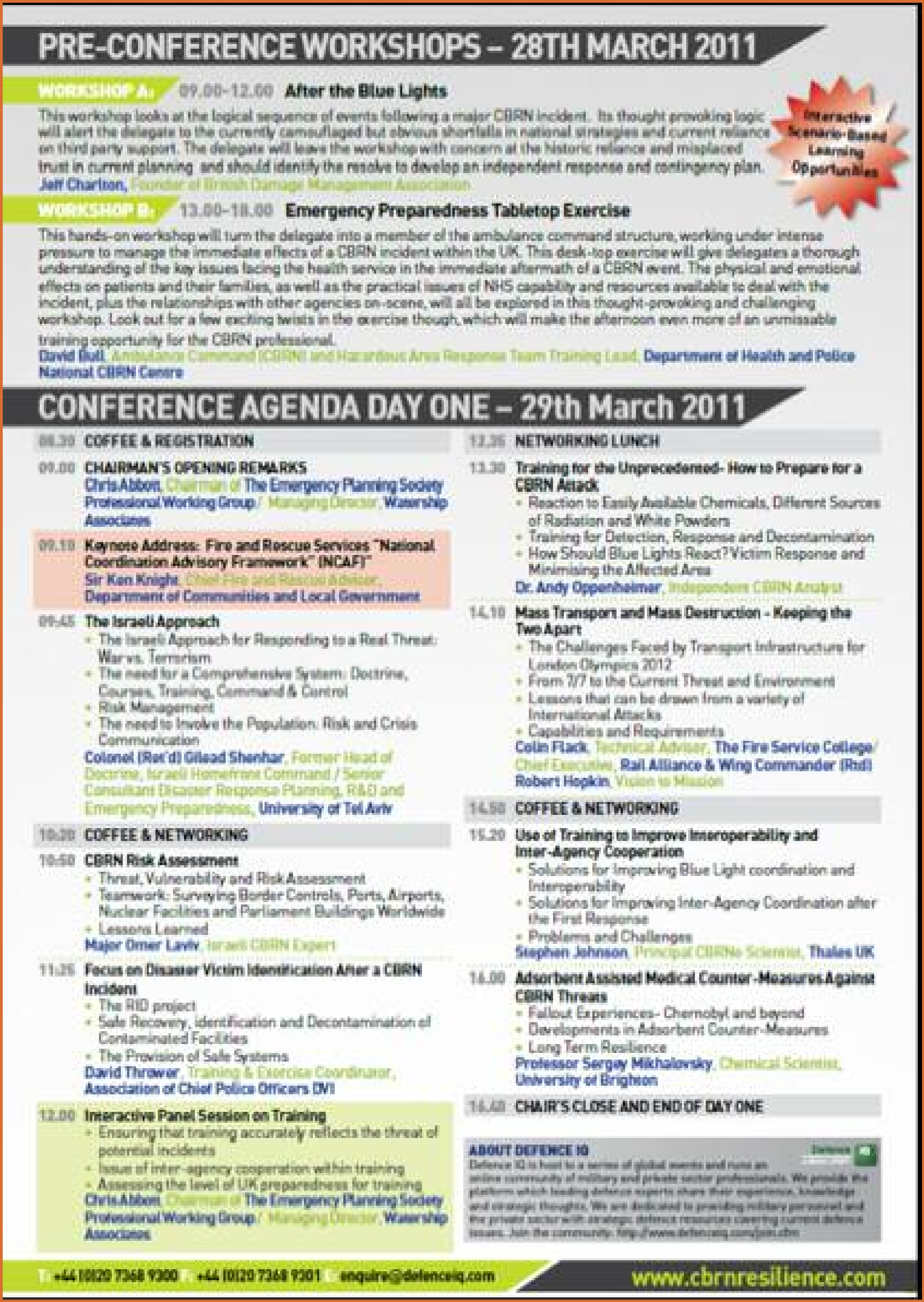
Book onto to our **Unique Training Exercise Workshops** to Gain Full Value

Book and Pay by 10th December 2010 and **Save Up to £300**

MEDIA PARTNERS

ASDNews BAPCO FIRE & RESCUE Defense Update INDUSTRIAL FIRE JOURNAL

T: +44 (0)20 7368 9300 F: +44 (0)20 7368 9301 E: enquire@defenceiq.com



PRE-CONFERENCE WORKSHOPS – 28TH MARCH 2011

Interactive Scenario-Based Learning Opportunities

WORKSHOP A: 09.00-12.00 **After the Blue Lights**

This workshop looks at the logical sequence of events following a major CBRN incident. Its thought provoking logic will alert the delegate to the currently camouflaged but obvious shortfalls in national strategies and current reliance on third party support. The delegate will leave the workshop with concern at the historic reliance and misplaced trust in current planning and should identify the resolve to develop an independent response and contingency plan.
Jeff Charlton, Founder of British Damage Management Association

WORKSHOP B: 13.00-18.00 **Emergency Preparedness Tabletop Exercise**

This hands-on workshop will turn the delegate into a member of the ambulance command structure, working under intense pressure to manage the immediate effects of a CBRN incident within the UK. This desk-top exercise will give delegates a thorough understanding of the key issues facing the health service in the immediate aftermath of a CBRN event. The physical and emotional effects on patients and their families, as well as the practical issues of NHS capability and resources available to deal with the incident, plus the relationships with other agencies on-scene, will all be explored in this thought-provoking and challenging workshop. Look out for a few exciting twists in the exercise though, which will make the afternoon even more of an unmissable training opportunity for the CBRN professional.
David Bull, Ambulance Command (CBRN) and Hazardous Area Response Team Training Lead, **Department of Health and Police National CBRN Centre**

CONFERENCE AGENDA DAY ONE – 29th March 2011

08.30 **COFFEE & REGISTRATION**

09.00 **CHAIRMAN'S OPENING REMARKS**
Chris Abbott, Chairman of **The Emergency Planning Society Professional Working Group** / Managing Director, **Watership Associates**

09.10 **Keynote Address: Fire and Rescue Services "National Coordination Advisory Framework" (NCAF)"**
Sir Ken Knight, Chief Fire and Rescue Advisor, **Department of Communities and Local Government**

09:45 **The Israeli Approach**
- The Israeli Approach for Responding to a Real Threat: War vs. Terrorism
- The need for a Comprehensive System: Doctrine, Courses, Training, Command & Control
- Risk Management
- The need to Involve the Population: Risk and Crisis Communication

Colonel (Ret'd) Gilead Shenhar, Former Head of Doctrine, Israeli Homefront Command / Senior Consultant Disaster Response Planning, R&D and Emergency Preparedness, **University of Tel Aviv**

10:20 **COFFEE & NETWORKING**

10:50 **CBRN Risk Assessment**
- Threat, Vulnerability and Risk Assessment
- Teamwork: Surveying Border Controls, Ports, Airports, Nuclear Facilities and Parliament Buildings Worldwide
- Lessons Learned

Major Omer Laviv, Israeli CBRN Expert

11:25 **Focus on Disaster Victim Identification After a CBRN Incident**
- The RID project
- Safe Recovery, Identification and Decontamination of Contaminated Facilities
- The Provision of Safe Systems

David Thrower, Training & Exercise Coordinator, **Association of Chief Police Officers DVI**

12.00 **Interactive Panel Session on Training**
- Ensuring that training accurately reflects the threat of potential incidents
- Issue of inter-agency cooperation within training
- Assessing the level of UK preparedness for training

Chris Abbott, Chairman of **The Emergency Planning Society Professional Working Group** / Managing Director, **Watership Associates**

12.35 **NETWORKING LUNCH**

13.30 **Training for the Unprecedented- How to Prepare for a CBRN Attack**
- Reaction to Easily Available Chemicals, Different Sources of Radiation and White Powders
- Training for Detection, Response and Decontamination
- How Should Blue Lights React? Victim Response and Minimising the Affected Area

Dr. Andy Oppenheimer, Independent CBRN Analyst

14.10 **Mass Transport and Mass Destruction - Keeping the Two Apart**
- The Challenges Faced by Transport Infrastructure for London Olympics 2012
- From 7/7 to the Current Threat and Environment
- Lessons that can be drawn from a variety of International Attacks
- Capabilities and Requirements

Colin Flack, Technical Advisor, **The Fire Service College** / Chief Executive, **Rail Alliance & Wing Commander (Rtd) Robert Hopkin,** Vision to Mission

14.50 **COFFEE & NETWORKING**

15.20 **Use of Training to Improve Interoperability and Inter-Agency Cooperation**
- Solutions for Improving Blue Light coordination and Interoperability
- Solutions for Improving Inter-Agency Coordination after the First Response
- Problems and Challenges

Stephen Johnson, Principal CBRNe Scientist, **Thales UK**

16.00 **Adsorbent Assisted Medical Counter-Measures Against CBRN Threats**
- Fallout Experiences- Chernobyl and beyond
- Developments in Adsorbent Counter-Measures
- Long Term Resilience

Professor Sergey Mikhalovsky, Chemical Scientist, **University of Brighton**

16.40 **CHAIR'S CLOSE AND END OF DAY ONE**

ABOUT DEFENCE IQ
Defence IQ is host to a series of global events and runs an online community of military and private sector professionals. We provide the platform which leading defence experts share their experience, knowledge and strategic thoughts. We are dedicated to providing military personnel and the private sector with strategic defence resources covering current defence issues. Join the community: http://www.defenceiq.com/join.cfm

T: +44 (0)20 7368 9300 F: +44 (0)20 7368 9301 E: enquire@defenceiq.com www.cbrnresilience.com

CONFERENCE AGENDA DAY TWO – 30th March 2011

08.30 **COFFEE & REGISTRATION**

09.00 **CHAIRMAN'S OPENING REMARKS**
Chris Abbott, Chairman of **The Emergency Planning Society Professional Working Group** / Managing Director, **Watership Associates**

09.10 **Developing the Police Service of Northern Ireland Capability Plan**
- PSNI and the All-Hazards Approach
- The Efficacy of Approaching CBRN, Drugs and Explosives Together
- The Challenges of the Approach

Chief Inspector Mark Roberts, Emergency Planning, **The Police Service of Northern Ireland**

09.50 **Overarching US CBRN Response, a State's Perspective**
- Existing CBRN Capabilities of the Active and Reserve Military Forces
- Expanding Capabilities of State National Guard Forces
- How these Forces Form the CBRN Enterprise of the US

Lieutenant Colonel Mark Riccardi, J3/Joint Director of Military Support, JFHQ-CO, **US Army**

10.30 **COFFEE & NETWORKING**

11.00 **CBRN Perspectives from the Republic of Ireland**
- Irish Policy & Doctrine in Responding to CBRN incidents
- Case Studies on CBRN Incidents & Lessons Learned
- Capabilities and Requirements

Peter Daly, National CBRN Lead / Chief Emergency Management Officer, **Health Service Executive, Republic of Ireland**

11.40 **Interactive Panel Session on Interoperability**
- What are the key issues relating to interoperability?
- Working culture or equipment issues?
- How can inter-agency interoperability be improved and developed?

Chris Abbott, Chairman of **The Emergency Planning Society Professional Working Group** / Managing Director, **Watership Associates**

12.20 **NETWORKING LUNCH**

13.30 **CBRN Planning - The Weakest Link**
- Threats and targets (brief analysis of CBRNE threats and soft/urban targets including hospitals)
- The weakest link into CBRN planning (indicating medical/hospital community worldwide – relevant results of ETHREAT Project (EU funded) addressing level of preparedness of front-line health professionals – current status in EU member states)
- 2004 Olympic Games: Medical CBRN defence – lessons identified (personal experience from deployment of the only hospital-based CBRN response unit deployed during the Games – formation, training, leadership, results)
- Suggestion for the future towards London 2012 (few key suggestion on how to overcome the problem of unwillingness of medical/nursing staff to be actively involved into CBRN operations)

Brigadier General (Ret'd) Ioannis Galatas, MD, MA(Terr), MC(Army), Medical CBRNE Planner, Senior Asymmetric Threats Analyst / ex. Commandant, 2004 Olympic Hospital, **CBRN Response Unit Athens, Greece**

14.10 **The Health Service Perspective**
- Health & Hospital Resilience & CBRN Response
- NHS Emergency Planning Issues
- Paediatric Healthcare Provision
- Emergency/Trauma Nursing

James Biser, Emergency Planning Officer, **University Hospitals Coventry & Warwickshire** and **Stewart Mason**, Emergency Planning & Resilience Manager, Birmingham Children's Hospital, **NHS Trust**

14.50 **EU CBRN Resilience Programme and Civil Protection**
- Overview of CBRN Action Plan
- Role in CBRN Incident Response and Improving Capability
- Future Role of EU CBRN Action

Yves Dussart, Principal Administrator, **European Commission**

15.30 **COFFEE & NETWORKING**

16.00 **European Committee for Standardisation Guidance Notes**
- Standards on Protecting the Victim and Potential Victim in Shelter in Place and Evacuation
- New protocols in self defence instead of reliance on emergency services
- Overwhelmed? Emergency Service Assistance During a Major Attack

Jeff Charlton, Founder, **British Damage Management Association**

16.40 **Dealing with the Public in the Aftermath of a Mass Casualty Incident**
- Dealing with the Public during Mass Casualty Incidents
- Effects on individuals and communities
- Effects on companies
- Long term implications

Rosie Murray MBE, SBCI, **Awareness Raising for Trauma**

16.40 **CHAIR'S CLOSE AND END OF DAY TWO**

SPONSORSHIP OPPORTUNITIES Three easy ways to get involved

1) **Thought Leadership:** [illegible]

2) **Branding:** [illegible]

3) **Focused Networking Events:** [illegible]

MEDIA PARTNERS

Defence Update [illegible] www.defense-update.com

ASDNews [illegible]

[illegible]

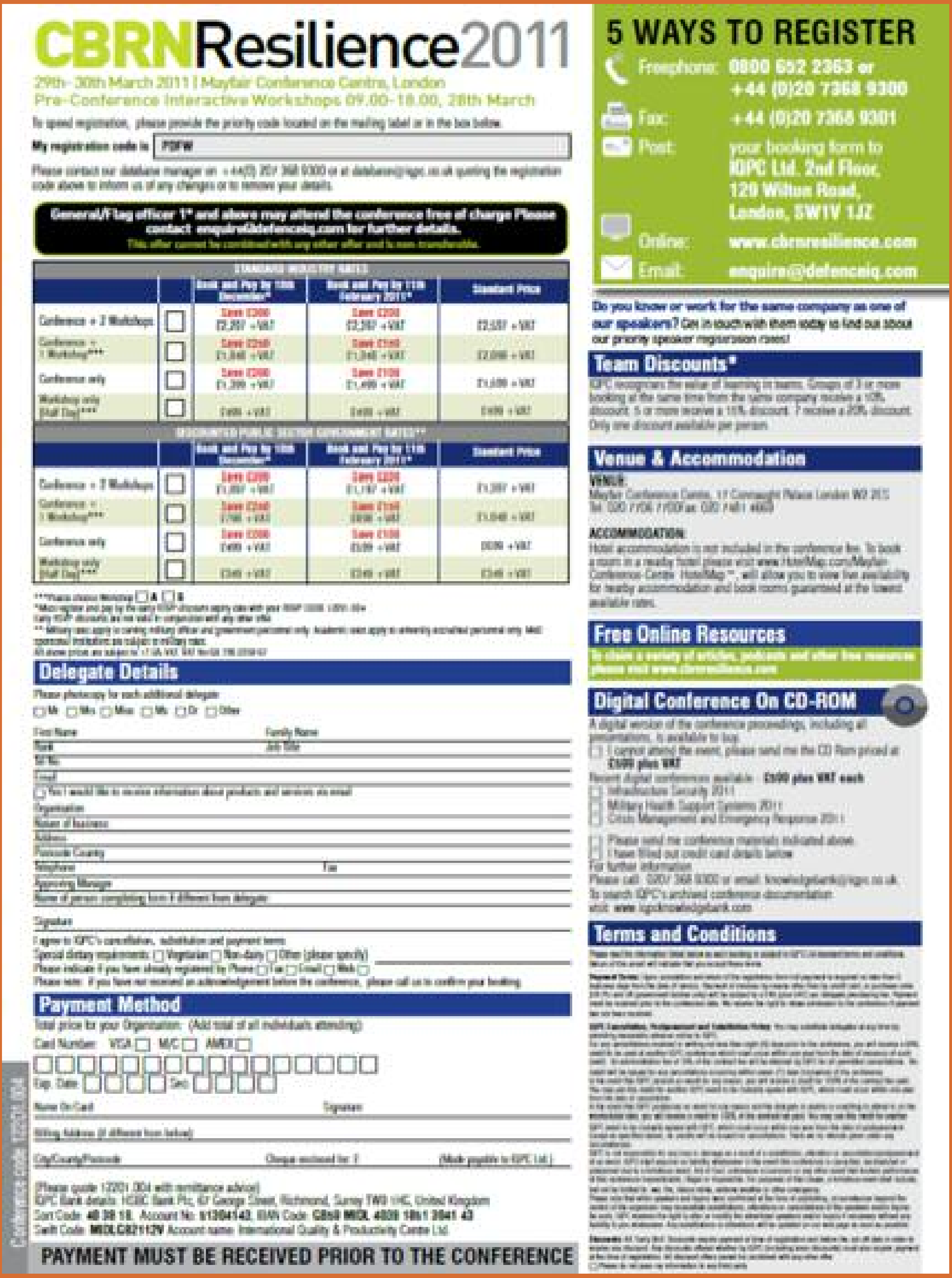
RAPCO [illegible]

FIRE & RESCUE [illegible]

[illegible]

T: +44 (0)20 7368 9300 F: +44 (0)20 7368 9301 E: enquire@defenceiq.com

www.cbrnresilience.com



CBRNResilience2011

29th- 30th March 2011 | Mayfair Conference Centre, London
Pre-Conference Interactive Workshops 09.00-18.00, 28th March

To speed registration, please provide the priority code located on the mailing label or in the box below.

My registration code is PDFW

Please contact our database manager on +44(0) 207 368 9300 or at database@iqpc.co.uk quoting the registration code above to inform us of any changes or to remove your details.

General/Flag officer 1* and above may attend the conference free of charge Please contact enquire@defenceiq.com for further details.
This offer cannot be combined with any other offer and is non-transferable.

STANDARD INDUSTRY RATES				
		Book and Pay by 10th December*	Book and Pay by 11th February 2011*	Standard Price
Conference + 2 Workshops	□	Save £300 £2,297 + VAT	Save £200 £2,397 + VAT	£2,597 + VAT
Conference + 1 Workshop***	□	Save £250 £1,848 + VAT	Save £150 £1,948 + VAT	£2,098 + VAT
Conference only	□	Save £300 £1,399 + VAT	Save £100 £1,499 + VAT	£1,599 + VAT
Workshop only (Half Day)***	□	£499 + VAT	£499 + VAT	£499 + VAT

DISCOUNTED PUBLIC SECTOR GOVERNMENT RATES**				
		Book and Pay by 10th December*	Book and Pay by 11th February 2011*	Standard Price
Conference + 2 Workshops	□	Save £200 £1,097 + VAT	Save £100 £1,197 + VAT	£1,297 + VAT
Conference + 1 Workshop***	□	Save £250 £798 + VAT	Save £150 £898 + VAT	£1,048 + VAT
Conference only	□	Save £200 £499 + VAT	Save £100 £599 + VAT	£699 + VAT
Workshop only (Half Day)***	□	£349 + VAT	£349 + VAT	£349 + VAT

***Please choose Workshop □ A □ B
*Must register and pay by the early [illegible] discount expiry date [illegible]
Early [illegible] discounts are not valid in conjunction with any other offer.
** Military rates apply to serving military officer and government personnel only. Academic rates apply to university accredited personnel only. [illegible]
All above prices are subject to [illegible] UK VAT. VAT No [illegible]

Delegate Details

Please photocopy for each additional delegate
□ Mr □ Mrs □ Miss □ Ms □ Dr □ Other

First Name Family Name
Rank Job Title
Tel No.
Email
□ Yes I would like to receive information about products and services via email
Organisation
Nature of business
Address
Postcode County
Telephone Fax
Approving Manager
Name of person completing form if different from delegate:

Signature
I agree to IQPC's cancellation, substitution and payment terms
Special dietary requirements: □ Vegetarian □ Non-dairy □ Other (please specify)
Please indicate if you have already registered by Phone □ Fax □ Email □ Web □
Please note: if you have not received an acknowledgement before the conference, please call us to confirm your booking.

Payment Method

Total price for your Organisation: (Add total of all individuals attending):
Card Number: VISA □ M/C □ AMEX □
□□□□□□□□□□□□□□□□
Exp. Date □□□□ Sec □□□□
Name On Card Signature
Billing Address (if different from below)
City/County/Postcode Cheque enclosed for: £ (Made payable to IQPC Ltd.)

(Please quote 12201.004 with remittance advice)
IQPC Bank details: HSBC Bank Plc, 67 George Street, Richmond, Surrey TW9 1HG, United Kingdom
Sort Code: **40 38 18**, Account No: **51304143**, IBAN Code: **GB59 MIDL 4038 1851 3041 43**
Swift Code: **MIDLGB2112V** Account name: International Quality & Productivity Centre Ltd.

Conference code: 12201.004

PAYMENT MUST BE RECEIVED PRIOR TO THE CONFERENCE

5 WAYS TO REGISTER

☎ Freephone: **0800 652 2363 or +44 (0)20 7368 9300**
Fax: **+44 (0)20 7368 9301**
Post: your booking form to
**IQPC Ltd. 2nd Floor,
120 Wilton Road,
London, SW1V 1JZ**
Online: **www.cbrnresilience.com**
Email: **enquire@defenceiq.com**

Do you know or work for the same company as one of our speakers? Get in touch with them today to find out about our priority speaker registration rates!

Team Discounts*

IQPC recognises the value of learning in teams. Groups of 3 or more booking at the same time from the same company receive a 10% discount. 5 or more receive a 15% discount. 7 receive a 20% discount. Only one discount available per person.

Venue & Accommodation

VENUE:
Mayfair Conference Centre, 17 Connaught Place London W2 2ES
Tel: 020 7706 7700Fax: 020 7401 4669

ACCOMMODATION:
Hotel accommodation is not included in the conference fee. To book a room in a nearby hotel please visit www.HotelMap.com/Mayfair-Conference-Centre. HotelMap™, will allow you to view live availability for nearby accommodation and book rooms guaranteed at the lowest available rates.

Free Online Resources

To claim a variety of articles, podcasts and other free resources please visit www.cbrnresilience.com

Digital Conference On CD-ROM

A digital version of the conference proceedings, including all presentations, is available to buy.
□ I cannot attend the event, please send me the CD Rom priced at **£600 plus VAT**
Recent digital conferences available - **£600 plus VAT each**
□ Infrastructure Security 2011
□ Military Health Support Systems 2011
□ Crisis Management and Emergency Response 2011

□ Please send me conference materials indicated above.
□ I have filled out credit card details below
For further information
Please call: 020 7368 9300 or email: knowledgebank@iqpc.co.uk
To search IQPC's archived conference documentation visit: www.iqpcknowledgebank.com

Terms and Conditions

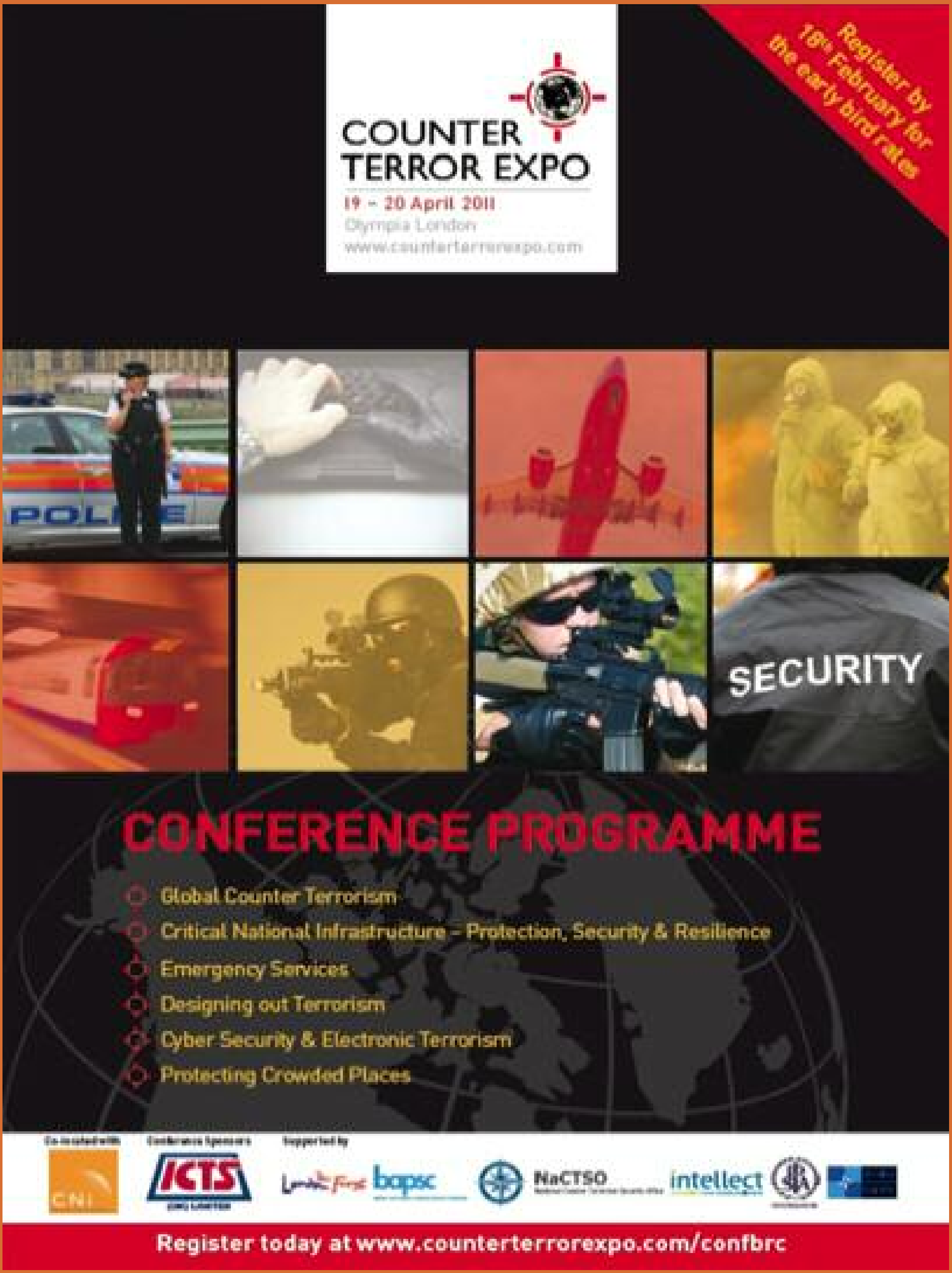
[illegible]

Payment Terms: [illegible]

IQPC Cancellation, Postponement and Substitution Policy: [illegible]

Discounts: [illegible]

□ [illegible]



Counter Terror Expo delivers both focus and clarity to the complex and multifaceted task of protecting people and assets from those with the intent to do harm.

This critically acclaimed event provides a vital forum for debate and plays a key role at the epicentre of the development of future global counter-terrorism strategy.

Counter Terror Expo's operationally critical and highly respected centrepiece conference event has a well deserved reputation for its delivery of insight, analysis and perspective on the range of threats faced.

This event gathers over 100 internationally recognised speakers in the field of counter-terrorism together, to debate the issues faced, define the operational strategies and help to shape future policy within the secure conclave of conference.

Counter Terror Expo's centrepiece conference is a multi-stream event featuring a mix of 1 & 2 day conferences and will cover 6 main areas, details of the themes and an explanation of each are shown below and overleaf, the detailed programmes and speaker details can be found throughout the brochure.

GLOBAL COUNTER TERRORISM
2 Day Conference – 19th and 20th April

A full decade on from the horror of 9/11, what lessons have been learned, has the United States of America counter-terrorism strategy educated or hindered, could the intervening European experience and response offer valuable lessons, what has been the impact on global business and human rights and where do we go from here?

Threats to national wellbeing remain potent given porous border controls, the threat within continues to be a matter of grave concern and States appear devoid of anything other than a military response.

- Is there another way and what are the pros and cons?
- Can an alternative strategy be accomplished and at what cost?
- Is this the way forward and will it bear fruit in respect to large-scale events such as the 2012 Olympic Games?

CRITICAL NATIONAL INFRASTRUCTURE – PROTECTION, SECURITY & RESILIENCE
2 Day Conference – 19th and 20th April

We take for granted the ability to switch a light on, get running water from a tap or be able to pick the phone up and make a call. These and other vital services form the backbone to the fabric of our lives and could so easily be lost for periods of time through issues ranging from climate change to natural disaster and acts of terrorism.

- How do you mitigate against such a diverse range of threats?
- What are the challenges and costs involved in doing so?
- How do you effectively manage the response to possibly unpredictable events?
- What is the economic implication from the loss for however short a time to a part of the Critical National Infrastructure?

EMERGENCY SERVICES
1 Day Conference – 19th April

Blue light services are the first responders to incidents of domestic and international terrorism.

Their role demands that the highest levels of coordination and interoperability exist between the individual services tasked with a first response. Achieving this in an operationally dynamic and demanding environment requires that meticulous planning is undertaken to ensure effective event mitigation strategies are delivered on the ground.

- What are the threats faced by blue light services engaged in a first response?
- What could be the impact if blue light first responders themselves are targeted?
- How do you deliver successful triage and evacuation of mass casualties in a potentially dangerous live environment?

The emergency services conference addresses these and very many other complex questions facing those who first respond to incidents of domestic and international terrorism.

DESIGNING OUT TERRORISM
1 Day Conference – 19th April

Recent history has shown that infrastructure, as well as assets and people, is just as much a target for those with intent to do harm. Building in appropriate protection, building out the fortress mentality and ensuring that space is usable, remain the priority.

- How do you accomplish that in the airport terminal, a shopping centre or within the corporate headquarters compound?
- What advice is available to you?
- How do you build requirements into the master plan?

Resilience is paramount in the face of modern day threats and this conference delivers best practice solutions based upon real world experience.

CYBER SECURITY & ELECTRONIC TERRORISM
1 Day Conference – 20th April

The cyber threat is a potent and growing issue for governments worldwide and, in a very real sense, represents a partially unseen but increasingly evident problem that must be dealt with urgently.

Stuxnet, a complex virus released into the wild within the past few months, was apparently designed to target Iranian computer installations supporting the nuclear programme in that country. Other computer viruses have been released into the wild by State actors in the recent past.

Recently, the United Kingdom stepped up its funding to fight cyber terrorism and crime, but only in terms of government and military assets.

The private sector critical national infrastructure providers are left on their own, but are required to deliver a response to these emerging threats, what does the future hold in the fight against this new wave of terrorism?

PROTECTING CROWDED PLACES
1 Day Conference – 20th April

NaCTSO
National Counter Terrorism Security Office

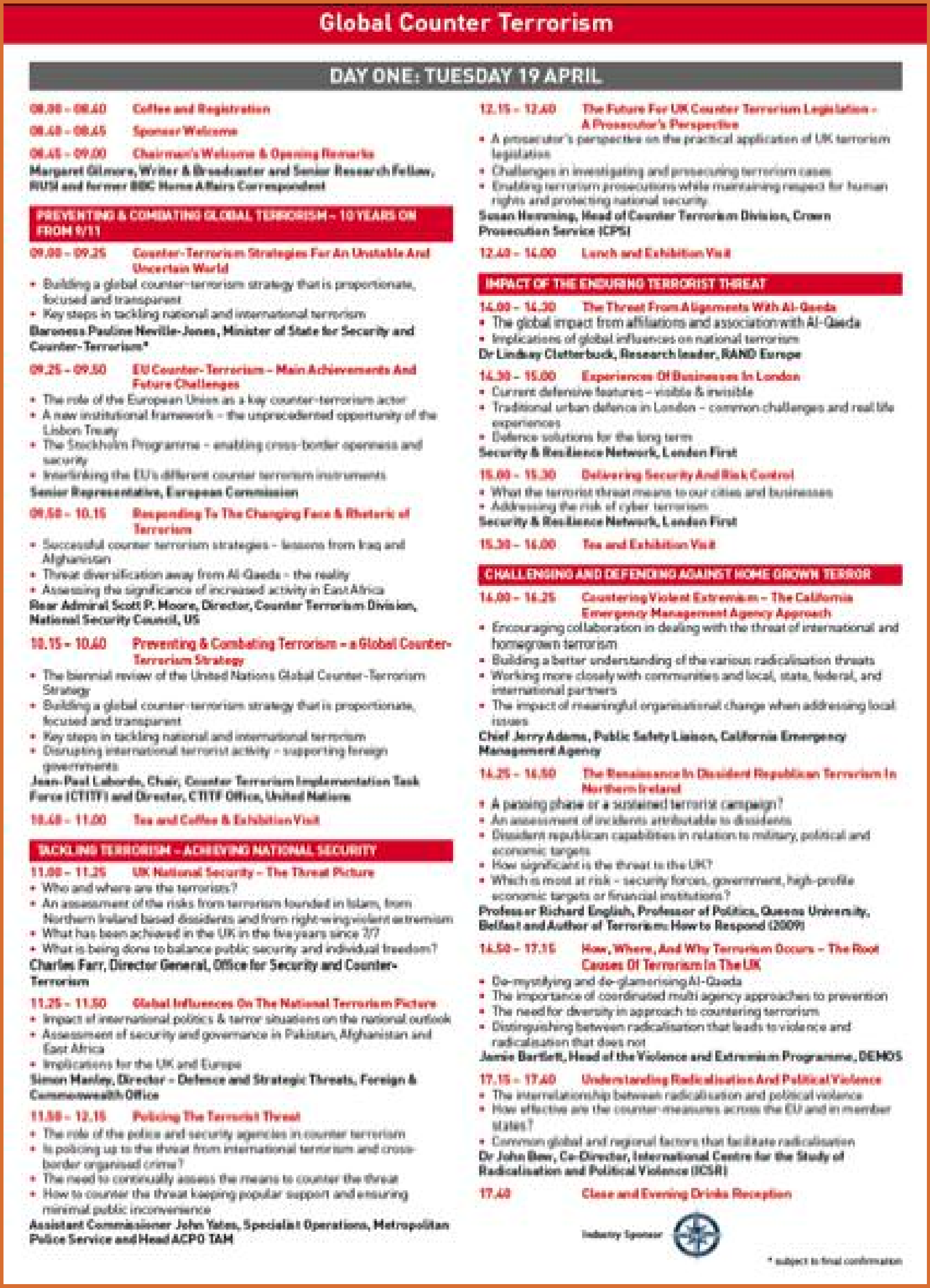
Although crowded public places have long been considered at risk from terrorist attack, the issue was publicly driven home by a recent warning from the US State Department.

Based upon intelligence received, the State Department warned that US citizens may be at risk in various locations across Europe where people congregate en-mass.

The governments of multiple other nations followed up with their own warnings to citizens who might be travelling in the alleged areas and locations of concern.

Crowded spaces are amongst the most difficult to secure, demand appropriate surveillance, as well as vigilance on the part of those tasked with the delivery of public facing security.

Each conference pass can be purchased on the basis of a 1 or 2 day pass for a particular stream, for those requiring access to multiple streams it is possible to buy multiple passes. Register today at www.counterterrorexpo.com/confbrc



Global Counter Terrorism

DAY ONE: TUESDAY 19 APRIL

08.00 – 08.40 Coffee and Registration

08.40 – 08.45 Sponsor Welcome

08.45 – 09.00 Chairman's Welcome & Opening Remarks

Margaret Gilmore, Writer & Broadcaster and Senior Research Fellow, RUSI and former BBC Home Affairs Correspondent

PREVENTING & COMBATING GLOBAL TERRORISM – 10 YEARS ON FROM 9/11

09.00 – 09.25 Counter-Terrorism Strategies For An Unstable And Uncertain World

- Building a global counter-terrorism strategy that is proportionate, focused and transparent
- Key steps in tackling national and international terrorism

Baroness Pauline Neville-Jones, Minister of State for Security and Counter-Terrorism*

09.25 – 09.50 EU Counter-Terrorism – Main Achievements And Future Challenges

- The role of the European Union as a key counter-terrorism actor
- A new institutional framework – the unprecedented opportunity of the Lisbon Treaty
- The Stockholm Programme – enabling cross-border openness and security
- Interlinking the EU's different counter terrorism instruments

Senior Representative, European Commission

09.50 – 10.15 Responding To The Changing Face & Rhetoric of Terrorism

- Successful counter terrorism strategies – lessons from Iraq and Afghanistan
- Threat diversification away from Al-Qaeda – the reality
- Assessing the significance of increased activity in East Africa

Rear Admiral Scott P. Moore, Director, Counter Terrorism Division, National Security Council, US

10.15 – 10.40 Preventing & Combating Terrorism – a Global Counter-Terrorism Strategy

- The biennial review of the United Nations Global Counter-Terrorism Strategy
- Building a global counter-terrorism strategy that is proportionate, focused and transparent
- Key steps in tackling national and international terrorism
- Disrupting international terrorist activity – supporting foreign governments

Jean-Paul Laborde, Chair, Counter Terrorism Implementation Task Force (CTITF) and Director, CTITF Office, United Nations

10.40 – 11.00 Tea and Coffee & Exhibition Visit

TACKLING TERRORISM – ACHIEVING NATIONAL SECURITY

11.00 – 11.25 UK National Security – The Threat Picture

- Who and where are the terrorists?
- An assessment of the risks from terrorism founded in Islam, from Northern Ireland based dissidents and from right-wing violent extremism
- What has been achieved in the UK in the five years since 7/7
- What is being done to balance public security and individual freedom?

Charles Farr, Director General, Office for Security and Counter-Terrorism

11.25 – 11.50 Global Influences On The National Terrorism Picture

- Impact of international politics & terror situations on the national outlook
- Assessment of security and governance in Pakistan, Afghanistan and East Africa
- Implications for the UK and Europe

Simon Manley, Director – Defence and Strategic Threats, Foreign & Commonwealth Office

11.50 – 12.15 Policing The Terrorist Threat

- The role of the police and security agencies in counter terrorism
- Is policing up to the threat from international terrorism and cross-border organised crime?
- The need to continually assess the means to counter the threat
- How to counter the threat keeping popular support and ensuring minimal public inconvenience

Assistant Commissioner John Yates, Specialist Operations, Metropolitan Police Service and Head ACPO TAM

12.15 – 12.40 The Future For UK Counter Terrorism Legislation – A Prosecutor's Perspective

- A prosecutor's perspective on the practical application of UK terrorism legislation
- Challenges in investigating and prosecuting terrorism cases
- Enabling terrorism prosecutions while maintaining respect for human rights and protecting national security

Susan Hemming, Head of Counter Terrorism Division, Crown Prosecution Service (CPS)

12.40 – 14.00 Lunch and Exhibition Visit

IMPACT OF THE ENDURING TERRORIST THREAT

14.00 – 14.30 The Threat From Alignments With Al-Qaeda

- The global impact from affiliations and association with Al-Qaeda
- Implications of global influences on national terrorism

Dr Lindsay Clutterbuck, Research leader, RAND Europe

14.30 – 15.00 Experiences Of Businesses In London

- Current defensive features – visible & invisible
- Traditional urban defence in London – common challenges and real life experiences
- Defence solutions for the long term

Security & Resilience Network, London First

15.00 – 15.30 Delivering Security And Risk Control

- What the terrorist threat means to our cities and businesses
- Addressing the risk of cyber terrorism

Security & Resilience Network, London First

15.30 – 16.00 Tea and Exhibition Visit

CHALLENGING AND DEFENDING AGAINST HOME GROWN TERROR

16.00 – 16.25 Countering Violent Extremism – The California Emergency Management Agency Approach

- Encouraging collaboration in dealing with the threat of international and homegrown terrorism
- Building a better understanding of the various radicalisation threats
- Working more closely with communities and local, state, federal, and international partners
- The impact of meaningful organisational change when addressing local issues

Chief Jerry Adams, Public Safety Liaison, California Emergency Management Agency

16.25 – 16.50 The Renaissance In Dissident Republican Terrorism In Northern Ireland

- A passing phase or a sustained terrorist campaign?
- An assessment of incidents attributable to dissidents
- Dissident republican capabilities in relation to military, political and economic targets
- How significant is the threat to the UK?
- Which is most at risk – security forces, government, high-profile economic targets or financial institutions?

Professor Richard English, Professor of Politics, Queens University, Belfast and Author of Terrorism: How to Respond (2009)

16.50 – 17.15 How, Where, And Why Terrorism Occurs – The Root Causes Of Terrorism In The UK

- De-mystifying and de-glamorising Al-Qaeda
- The importance of coordinated multi agency approaches to prevention
- The need for diversity in approach to countering terrorism
- Distinguishing between radicalisation that leads to violence and radicalisation that does not

Jamie Bartlett, Head of the Violence and Extremism Programme, DEMOS

17.15 – 17.40 Understanding Radicalisation And Political Violence

- The interrelationship between radicalisation and political violence
- How effective are the counter-measures across the EU and in member states?
- Common global and regional factors that facilitate radicalisation

Dr John Bew, Co-Director, International Centre for the Study of Radicalisation and Political Violence (ICSR)

17.40 Close and Evening Drinks Reception

Industry Sponsor

* subject to final confirmation

Global Counter Terrorism

DAY TWO: WEDNESDAY 20 APRIL

08.00 – 08.45 Coffee and Registration

08.45 – 09.00 Chairman Opening Remarks

Dr Dave Sloggett, Centre for Defence Studies, Department of War Studies, King's College London

ACHIEVING HOMELAND SECURITY IN THE FACE OF THE TERRORIST THREAT

09.00 – 09.25 Safeguarding Citizens And Countering Terrorism

- Counter terrorism's track record on safeguarding citizens – are the world's citizens safer now than 10 years ago?
- The PREVENT review and changes to counter terrorism legislation – the impact on homeland security
- Ensuring privacy and proportionality – assessing the balance between regulation and civil liberties

Lord Carlile of Berriew Q.C.

09.25 – 09.50 US Homeland Defence – A Decade On From 9/11

- An assessment of domestic safeguards a decade after 9/11 – is terrorism still the top problem?
- Combating home-grown terrorism and the threat from radical Jihadist networks in the decade ahead
- Ensuring homeland security – how big the risk from international terrorist activity?

Admiral James A. Winnefeld, Jr., Commander of the North American Aerospace Defense Command and United States Northern Command*

09.50 – 10.15 Could 7/7 Have Been Prevented?

- Failing to connect the dots - the missed opportunities
- Assessing the impact since 7/7 of new counter terrorism laws
- Ensuring improved prevention through cultural changes and improvements in inter-agency communication

Margaret Gilmore, Writer & Broadcaster and Senior Research Fellow – RUSI and former BBC Home Affairs Correspondent

10.15 – 10.40 Cyber Terrorism In Unguarded Corridors

- Cyber terrorism vs cyber crime – how the threat varies
- Use of cyber attacks by criminals, terrorists and small non-state groups
- Cyberspace and the Internet as a vector for terrorism – providing an asymmetric advantage for Jihadists?
- Key vulnerabilities for sovereign states from cyber terrorism
- Strategies for securing the UK in cyberspace

Dr Paul Killworth, Head of Cyber Strategy, Government Communication Headquarters (GCHQ)

10.40 – 11.00 Tea and Coffee & Exhibition Visit

CHALLENGING TERRORISM IN THE INFORMATION AGE

11.00 – 11.20 Cell Phone Hacking – The Terrorist's Latest Playground

- Cell phones as an information target & insecurities of current 3G and future 4G technologies
- The latest techniques employed by terrorists to intercept cell phone traffic
- Appropriate and effective counter measures

Nigel Stanley, Practice Leader – Security, Bloor Research

11.20 – 12.00 Securing Cyberspace In An Era Of Global Connectivity

- Cyber terrorism and cyber warfare – an assessment of the global threat
- How global connectivity facilitates economic espionage, money laundering, cyber fraud, intellectual property theft and security breaches
- Protecting electronic landscapes – lessons, challenges and opportunities
- The need for a rigorous approach to the security challenges of cyber space

Edward P Gibson, CISSP, Director, PricewaterhouseCoopers Global, former FBI Agent – US Embassy London and former Chief cyber Security Advisor, Microsoft (UK) Ltd

TERRORISM AND LARGE SCALE EVENTS

12.00 – 12.20 The Security Legacy Of The 2012 Olympic And Paralympic Games

- How games security will impact the UK population
- Security features and lessons for other large scale events
- Collaborative working: Government, public sector and private industry

Olympic Security Directorate, Home Office

12.20 – 12.40 Terrorism Threats at the Olympics – Forecasts for London 2012 and Sochi 2014

- Network analysis of various violent groups including an assessment of both capability and intent
- Preparedness of security forces
- Detailed locational mapping of likely target sets
- Potential threat of military conflict between Russia and Georgia

Simon Sole, Chief Executive Officer, Exclusive Analysis

12.40 – 14.00 Lunch and Exhibition Visit

THE FIGHT TO PREVENT RADICALISATION

14.00 – 14.30 Project Samossa – Foiling A Violent Terrorism Attack

- Assessment of domestic terrorist groups operating in Canada
- Implications from international and home-grown radicalization
- A review of Project Samossa

Chief Superintendent Serge Therriault, Royal Canadian Mounted Police

14.30 – 15.00 How Big Is The Threat Of Home Grown Terror?

- Are radical Islamists trying to exploit Islamophobia?
- How significant is the threat from UK residents training to fight in the insurgency in Yemen and Somalia?
- What is the likelihood of a lone terrorist attack in the UK?
- How significant is the threat from domestic extremism?

Dr. Brooke Rogers, Lecturer in Risk and Terror, King's Centre for Risk Management (KCRM), King's College London

ADDRESSING EXISTING & EMERGING THREATS

15.00 – 15.30 Tackling Trans-Border Crime

- Assessing the growth in trans-border crime
- Impact of social and economic integration between member states
- Streamlining trans-border cooperation – the role of the European Investigation Order (EIO)

Troels Oerting, Deputy Director, Europol (The European Police Office)

15.30 – 16.00 The Future Of CBRNE Related Terrorism

- Enhancing European CBRN terrorism countermeasures
- Assessing current challenges – why multi-agency cooperation is essential
- Capabilities to meet the threat and risks associated with the Olympics and beyond

Superintendent Andy Deegan , Deputy Head, UK Police National CBRN Centre

16.00 – 16.30 Al-Qaeda and the Power of Prophecy

- A review of Al-Qaeda, its franchises and the fundamentalist Islamist movement
- Operational trends and key activities
- Future intent, likely targets and implications for the West

Justin Crump, CEO, Sibylline

16.30 Close

Critical National Infrastructure – Protection, Security & Resilience

DAY ONE: TUESDAY 19 APRIL

08.40 – 08.45 Coffee and Registration

08.45 – 09.00 Chairman's Welcome & Opening Remarks

Steve Cummings, Deloitte and Former Director CPNI

CRITICAL INFRASTRUCTURE PROTECTION

09.00 – 09.20 Critical Infrastructure Protection – An Integral Part Of National Security

- Protecting against the impact of terrorism, natural disasters, or industrial hazards
- The impact of local, national and transnational causes
- Interdependencies between CNI Sectors
- The importance of contingency planning in a changing climate of political and economic risk

Centre for the Protection of National Infrastructure (CPNI)

09.20 – 09.40 Corporate Resilience & The Role Of The Private Sector In Securing Critical Infrastructure

- What are the high consequence risks facing the UK?
- The UK approach to corporate resilience
- Providing effective and coordinated crisis management in response to disruptive challenges
- Ensuring the private sector takes the protection of CNI more seriously

Stuart Sterling, Assistant Director – Corporate Resilience, Civil Contingencies Secretariat, Cabinet Office

09.40 – 10.00 Dealing With Failures Of Critical Infrastructures And Services

- Understanding the sources of failure
- Key actions to mitigate against wide-scale disaster
- Present and future protection solutions
- Impact of spending cuts on vital infrastructure maintenance and rebuilding

Cate Pye, Director Defence & Security Practice, Ernst & Young LLP

10.00 – 10.30 Round Table

- Are UK's CNI safeguards robust enough to withstand the latest attack scenarios?
- What are the consequences of government cut-backs?

10.30 – 11.00 Tea and Coffee & Exhibition Visit

PROTECTING AGAINST & RESISTING CYBER ATTACK

11.00 – 11.20 Understanding The Cyber Dimension

- Assessing the probability of disruptive cyber activity
- Potential effect on critical national infrastructure
- Key strategies for protecting against cyber attack – role of law enforcement and security agencies

Senior Representative, Alcatel-Lucent

11.20 – 11.40 Resilience In Converged Networks

- The criticality of converged networks in the UK communications infrastructure
- How Government and the regulator support resilience
- Delivering an effective emergency measures in the event of disaster

Dr Nigel P Brown, Director of Resilient Telecommunications Strategy, Civil Contingencies Secretariat, Cabinet Office

11.40 – 12.00 Vulnerabilities Of Critical Information And Control Infrastructures

- Assessing critical dependencies of energy, finance and transport infrastructures on ICT infrastructure
- Vulnerabilities of crucial infrastructures to remote hijacking and unauthorized control
- Implications for governments and nations and mitigation strategies

David Lacey, UK Director of Research, ISSA UK

12.00 – 12.30 Round Table

- What role for Governments in securing the networks of the future?
- Can we take action against rogue nation states ignoring global regulations?

12.30 – 14.00 Lunch and Exhibition Visit

SECURING CRITICAL INFRASTUCTURE

14.00 – 14.20 Securing Critical Infrastructure From Disruptive Technologies

- What is the impact on the threat landscape from disruptive technologies
- Understanding the threat & what can owners and operators do to mitigate the risks
- How valid is the threat to control systems from targeted cyber attack

Dr Paul Kearney, Security Futures Practice, BT Innovate

14.20 – 14.40 Ensuring The Security And Resilience Of Critical Assets And Networks

- Need for a dynamic and evolving approach to threat assessment
- Strategies for reducing disruption to critical infrastructure and essential services
- Understanding interdependencies between critical infrastructure sectors

Professor Jim Norton, Independent Director and Policy Adviser

14.40 – 15.00 Supply Chain & Infrastructure Security

- Key elements in supply chains and why they are important
- Procuring, building and maintaining a secure and risk free supply chain
- Potential impact from outsourcing
- The need for comprehensive emergency preparedness and response capabilities

Dr Helen Peck, Senior Lecturer, Commercial and Supply Chain Risk, Department of Management and Security, Cranfield University

15.00 – 15.30 Round Table

- Are terrorist attacks and insurgency the key threats?
- Key strategies for protecting process control systems

15.30 – 16.00 Tea and Coffee & Exhibition Visit

MITIGATING AGAINST SEVERE WEATHER & NATURAL HAZARD SITUATIONS

16.00 – 16.20 Adapting To The Impacts Of Climate Change

- The impacts of climate change for the UK's vital infrastructure
- How owners and operators might adapt in the future
- Is an overhaul of vital infrastructure including roads, water supplies and the power grid required?
- Using green infrastructure to mitigate and adapt to climate change impacts

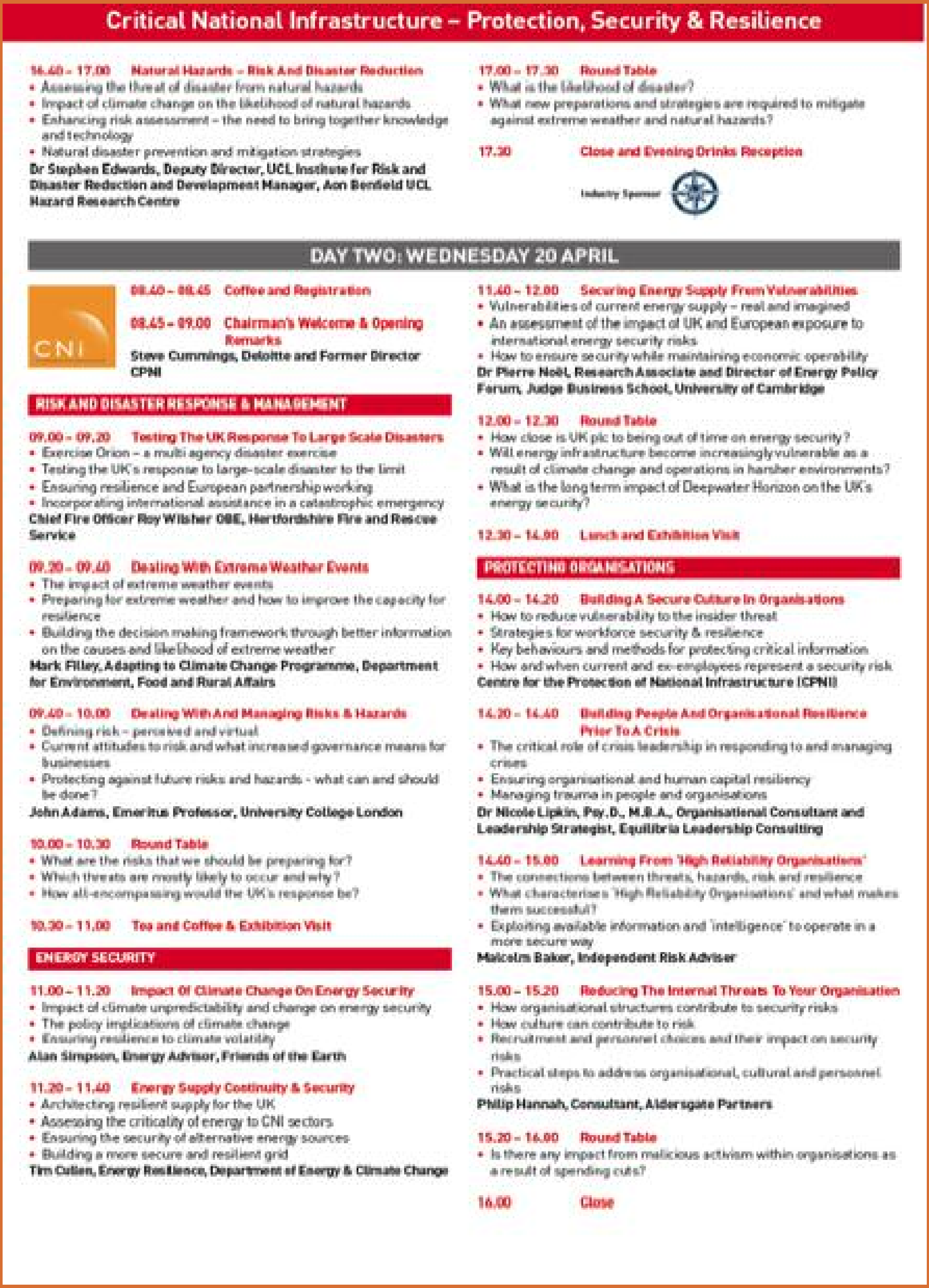
Lord John Krebs, Chair of the Adaptation Sub-Committee, Committee on Climate Change (CCC)

16.20 – 16.40 Weathering The Storm – Dealing With Adverse Winter Weather In The UK

- Further lessons on how the country can improve resilience to extreme winter weather
- Need for partnership working and for resilience in the supply chain
- Coordination of policies and plans across administrative borders
- Clear information to the public and businesses on expected levels of service in the event of severe winter weather

Councillor Peter Box, Leader of Wakefield Council, Chair of the Yorkshire and Humber Assembly and Member of the Government's Northern Way Steering Group

Day 1 programme continued over page...



Critical National Infrastructure – Protection, Security & Resilience

16.40 – 17.00 Natural Hazards – Risk And Disaster Reduction

- Assessing the threat of disaster from natural hazards
- Impact of climate change on the likelihood of natural hazards
- Enhancing risk assessment – the need to bring together knowledge and technology
- Natural disaster prevention and mitigation strategies

Dr Stephen Edwards, Deputy Director, UCL Institute for Risk and Disaster Reduction and Development Manager, Aon Benfield UCL Hazard Research Centre

17.00 – 17.30 Round Table

- What is the likelihood of disaster?
- What new preparations and strategies are required to mitigate against extreme weather and natural hazards?

17.30 Close and Evening Drinks Reception

Industry Sponsor

DAY TWO: WEDNESDAY 20 APRIL

08.40 – 08.45 Coffee and Registration

08.45 – 09.00 Chairman's Welcome & Opening Remarks

Steve Cummings, Deloitte and Former Director CPNI

RISK AND DISASTER RESPONSE & MANAGEMENT

09.00 – 09.20 Testing The UK Response To Large Scale Disasters

- Exercise Orion – a multi agency disaster exercise
- Testing the UK's response to large-scale disaster to the limit
- Ensuring resilience and European partnership working
- Incorporating international assistance in a catastrophic emergency

Chief Fire Officer Roy Wilsher OBE, Hertfordshire Fire and Rescue Service

09.20 – 09.40 Dealing With Extreme Weather Events

- The impact of extreme weather events
- Preparing for extreme weather and how to improve the capacity for resilience
- Building the decision making framework through better information on the causes and likelihood of extreme weather

Mark Filley, Adapting to Climate Change Programme, Department for Environment, Food and Rural Affairs

09.40 – 10.00 Dealing With And Managing Risks & Hazards

- Defining risk – perceived and virtual
- Current attitudes to risk and what increased governance means for businesses
- Protecting against future risks and hazards - what can and should be done?

John Adams, Emeritus Professor, University College London

10.00 – 10.30 Round Table

- What are the risks that we should be preparing for?
- Which threats are mostly likely to occur and why?
- How all-encompassing would the UK's response be?

10.30 – 11.00 Tea and Coffee & Exhibition Visit

ENERGY SECURITY

11.00 – 11.20 Impact Of Climate Change On Energy Security

- Impact of climate unpredictability and change on energy security
- The policy implications of climate change
- Ensuring resilience to climate volatility

Alan Simpson, Energy Advisor, Friends of the Earth

11.20 – 11.40 Energy Supply Continuity & Security

- Architecting resilient supply for the UK
- Assessing the criticality of energy to CNI sectors
- Ensuring the security of alternative energy sources
- Building a more secure and resilient grid

Tim Cullen, Energy Resilience, Department of Energy & Climate Change

11.40 – 12.00 Securing Energy Supply From Vulnerabilities

- Vulnerabilities of current energy supply – real and imagined
- An assessment of the impact of UK and European exposure to international energy security risks
- How to ensure security while maintaining economic operability

Dr Pierre Noël, Research Associate and Director of Energy Policy Forum, Judge Business School, University of Cambridge

12.00 – 12.30 Round Table

- How close is UK plc to being out of time on energy security?
- Will energy infrastructure become increasingly vulnerable as a result of climate change and operations in harsher environments?
- What is the long term impact of Deepwater Horizon on the UK's energy security?

12.30 – 14.00 Lunch and Exhibition Visit

PROTECTING ORGANISATIONS

14.00 – 14.20 Building A Secure Culture In Organisations

- How to reduce vulnerability to the insider threat
- Strategies for workforce security & resilience
- Key behaviours and methods for protecting critical information
- How and when current and ex-employees represent a security risk

Centre for the Protection of National Infrastructure (CPNI)

14.20 – 14.40 Building People And Organisational Resilience Prior To A Crisis

- The critical role of crisis leadership in responding to and managing crises
- Ensuring organisational and human capital resiliency
- Managing trauma in people and organisations

Dr Nicole Lipkin, Psy.D., M.B.A., Organisational Consultant and Leadership Strategist, Equilibria Leadership Consulting

14.40 – 15.00 Learning From 'High Reliability Organisations'

- The connections between threats, hazards, risk and resilience
- What characterises 'High Reliability Organisations' and what makes them successful?
- Exploiting available information and 'intelligence' to operate in a more secure way

Malcolm Baker, Independent Risk Adviser

15.00 – 15.20 Reducing The Internal Threats To Your Organisation

- How organisational structures contribute to security risks
- How culture can contribute to risk
- Recruitment and personnel choices and their impact on security risks
- Practical steps to address organisational, cultural and personnel risks

Philip Hannah, Consultant, Aldersgate Partners

15.20 – 16.00 Round Table

- Is there any impact from malicious activism within organisations as a result of spending cuts?

16.00 Close

Emergency Services

TUESDAY 19 APRIL

08.40 – 08.45 Coffee and Registration

08.45 – 09.00 Chairman's Welcome & Opening Remarks

David Buckenham, Director – Paladin Crisis Management Ltd, Senior Consultant – Resilience Centre Cranfield University and Deputy Secretary, Institute of Civil Protection & Emergency Management

THE IMPACT OF TERRORISM ON THE EMERGENCY SERVICES

09.00 – 09.30 The Impact Of Terrorism On Policing & Security

- Dealing with the threat from domestic and international terrorism
- The relationship between the police and security services
- Impact of global issues on local counter terror policing

Keith Weston QPM MA, Senior Research Fellow in Counter Terrorism, Security Studies Institute, Department of Management and Security, Cranfield University

09.30 – 10.00 Emergency Response In Large-Scale Disasters

- The role of the Fire Brigade & co-operation with other agencies
- UK capabilities in disaster response and management
- Planning for 2012 and the future

Deputy Assistant Commissioner Bernie Higgins, Head of Special Operations Group, London Fire Brigade

10.00 – 10.30 Understanding & Responding To The Threat of Terrorism

- Assessing the threat from international terrorism
- The role of blue light services – the cornerstone of the UK response
- The importance of multi agency collaboration in defending against & responding to terrorism

Dr Dave Sloggett, Centre for Defence Studies, Department of War Studies, King's College London

10.30 – 11.00 Tea and Coffee & Exhibition Visit

EMERGENCY RESPONSE – CAPABILITY & INTEROPERABILITY

11.00 – 11.30 Strategic (Gold) Command Interoperability At A Major Terrorist Incident

- Assessing the role of prevention and pre-event detection in counter terrorism
- The link between outcomes and the potential number of casualties to the strategic response of Emergency – lessons from Mumbai
- The complexities of achieving interoperability at major incidents and what happens when First Responders are targeted.
- The interoperability complexities facing Emergency First Responders today
- The trust relationships at Gold command level required to effectively deal with a complex major terrorist incident

Andy Beale, Deputy Chief Fire Officer, Nottinghamshire Fire & Rescue

11.30 – 12.00 First Responder Communications & Interoperability – 2011 and 2012

- Supporting an all hazards, all agencies approach to communications
- Exploiting the benefits of a single platform for all emergency responder communications
- The key role of communication in securing the 2012 Olympic and Paralympic Games

Rob Walley, Chairman, Multi-Agency Airwave User Group (MAAUG)

12.00 – 12.30 Hospital CBRN Response In A Megapolis Environment

- CBRN threats and targets
- A medical perspective: Tokyo's subway sarin and the Goiânia Incident
- The medical & nursing community – the weak link in CBRN planning?
- 2004 Olympic Games Medical CBRN Defence Planning – personal experience
- The way ahead – towards London 2012

Colonel Galatas Ioannis MD, MC, Head, Department of Asymmetric Threats, Intelligence Analysis Branch, Joint Military Intelligence Division, Hellenic National Defence General Staff, Greece

12.30 – 14.00 Lunch and Exhibition Visit

RESPONDING TO THE THREAT – MULTI AGENCY RESPONSE

14.00 – 14.30 Multi-Agency Counter Terror Operations

- Managing the safe decontamination of detainees under restraint
- Ensuring a continual evidence chain during multi-agency CT operations

Tony Shryane, CBRNE Manager, Emergency Preparedness Team, North West Ambulance Service NHS Trust

14.30 – 15.00 Joint Operations At Bomb Making Factories

- Assessing the threat from the amateur bomb and firework manufacturing
- The roles and limits of Police, Fire & EOD when dealing with the threat
- The challenges in terms of operational response and legislation

Chris Case, Group Manager, Merseyside Fire & Rescue and Vice President of the Institute of Explosives Engineers

15.00 – 15.30 Tactical Emergency Medical Response

- The potential for serious injury and illness
- Preplanning the NHS response
- Joint Police & Ambulance Service training
- Benefits and future developments

Professor Andy Newton MCPara, Consultant Paramedic & Clinical Director, South East Coast Ambulance Service NHS Trust & Visiting Professor of Paramedic Practice, University of Surrey

15.30 – 16.00 Tea and Coffee & Exhibition Visit

RESPONDING TO MASS CASUALTY EVENTS

16.00 – 16.30 Ambulance Hazardous Area Response Team (HART) – A Fundamental Part In The National Resilience Infrastructure

- How HART came about and progress with implementation
- Working with other agencies to train and prepare for deliberate mass casualty events
- The contribution to the national infrastructure in the face of terrorist attacks
- CBRN and USAR capabilities – examples of work to date

Russ Mansford, Strategic Ambulance Advisor, Emergency Preparedness Division, Department of Health

16.30 – 17.00 Responding To Chemical And Biological Deliberate Release

- The ORCHIDS project – building a network of expertise
- How to optimise methods for dealing with a range of contaminants
- Best practice for existing mass casualty decontamination facilities

Dr Richard Amlôt, ORCHIDS Technical Leader, Centre for Emergency Preparedness and Response, Health Protection Agency

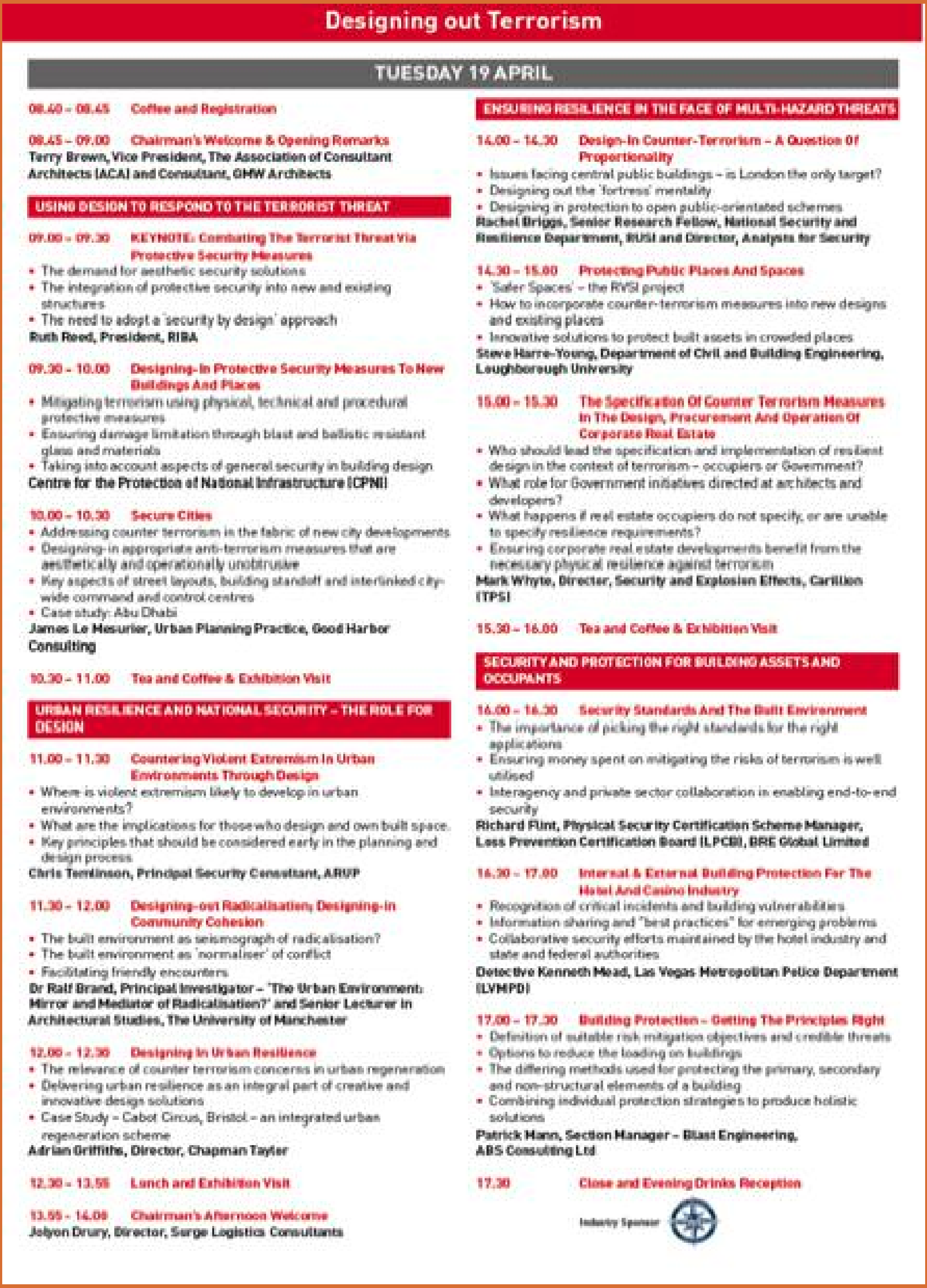
17.00 – 17.30 Planning For Mass Casualty Triage

- Responding to events with a large number of injured patients
- How to train organisations and systems for conducting mass casualty triage
- Organisation and system allocation during a mass casualty incident

Jim Sideras RN, MSN, MIFireE, CFO, CMO, Division Chief, Sioux Falls Fire Rescue

17.30 Close and Evening Drinks Reception

Industry Sponsor



Designing out Terrorism

TUESDAY 19 APRIL

08.40 – 08.45 Coffee and Registration

08.45 – 09.00 Chairman's Welcome & Opening Remarks
Terry Brown, Vice President, The Association of Consultant Architects (ACA) and Consultant, GMW Architects

USING DESIGN TO RESPOND TO THE TERRORIST THREAT

09.00 – 09.30 KEYNOTE: Combating The Terrorist Threat Via Protective Security Measures

- The demand for aesthetic security solutions
- The integration of protective security into new and existing structures
- The need to adopt a 'security by design' approach

Ruth Reed, President, RIBA

09.30 – 10.00 Designing-In Protective Security Measures To New Buildings And Places

- Mitigating terrorism using physical, technical and procedural protective measures
- Ensuring damage limitation through blast and ballistic resistant glass and materials
- Taking into account aspects of general security in building design

Centre for the Protection of National Infrastructure (CPNI)

10.00 – 10.30 Secure Cities

- Addressing counter terrorism in the fabric of new city developments
- Designing-in appropriate anti-terrorism measures that are aesthetically and operationally unobtrusive
- Key aspects of street layouts, building standoff and interlinked city-wide command and control centres
- Case study: Abu Dhabi

James Le Mesurier, Urban Planning Practice, Good Harbor Consulting

10.30 – 11.00 Tea and Coffee & Exhibition Visit

URBAN RESILIENCE AND NATIONAL SECURITY – THE ROLE FOR DESIGN

11.00 – 11.30 Countering Violent Extremism In Urban Environments Through Design

- Where is violent extremism likely to develop in urban environments?
- What are the implications for those who design and own built space.
- Key principles that should be considered early in the planning and design process

Chris Tomlinson, Principal Security Consultant, ARUP

11.30 – 12.00 Designing-out Radicalisation; Designing-in Community Cohesion

- The built environment as seismograph of radicalisation?
- The built environment as 'normaliser' of conflict
- Facilitating friendly encounters

Dr Ralf Brand, Principal Investigator – 'The Urban Environment: Mirror and Mediator of Radicalisation?' and Senior Lecturer in Architectural Studies, The University of Manchester

12.00 – 12.30 Designing In Urban Resilience

- The relevance of counter terrorism concerns in urban regeneration
- Delivering urban resilience as an integral part of creative and innovative design solutions
- Case Study – Cabot Circus, Bristol – an integrated urban regeneration scheme

Adrian Griffiths, Director, Chapman Taylor

12.30 – 13.55 Lunch and Exhibition Visit

13.55 – 14.00 Chairman's Afternoon Welcome
Jolyon Drury, Director, Surge Logistics Consultants

ENSURING RESILIENCE IN THE FACE OF MULTI-HAZARD THREATS

14.00 – 14.30 Design-In Counter-Terrorism – A Question Of Proportionality

- Issues facing central public buildings – is London the only target?
- Designing out the 'fortress' mentality
- Designing in protection to open public-orientated schemes

Rachel Briggs, Senior Research Fellow, National Security and Resilience Department, RUSI and Director, Analysis for Security

14.30 – 15.00 Protecting Public Places And Spaces

- 'Safer Spaces' – the RVSI project
- How to incorporate counter-terrorism measures into new designs and existing places
- Innovative solutions to protect built assets in crowded places

Steve Harre-Young, Department of Civil and Building Engineering, Loughborough University

15.00 – 15.30 The Specification Of Counter Terrorism Measures In The Design, Procurement And Operation Of Corporate Real Estate

- Who should lead the specification and implementation of resilient design in the context of terrorism – occupiers or Government?
- What role for Government initiatives directed at architects and developers?
- What happens if real estate occupiers do not specify, or are unable to specify resilience requirements?
- Ensuring corporate real estate developments benefit from the necessary physical resilience against terrorism

Mark Whyte, Director, Security and Explosion Effects, Carillion (TPS)

15.30 – 16.00 Tea and Coffee & Exhibition Visit

SECURITY AND PROTECTION FOR BUILDING ASSETS AND OCCUPANTS

16.00 – 16.30 Security Standards And The Built Environment

- The importance of picking the right standards for the right applications
- Ensuring money spent on mitigating the risks of terrorism is well utilised
- Interagency and private sector collaboration in enabling end-to-end security

Richard Flint, Physical Security Certification Scheme Manager, Loss Prevention Certification Board (LPCB), BRE Global Limited

16.30 – 17.00 Internal & External Building Protection For The Hotel And Casino Industry

- Recognition of critical incidents and building vulnerabilities
- Information sharing and "best practices" for emerging problems
- Collaborative security efforts maintained by the hotel industry and state and federal authorities

Detective Kenneth Mead, Las Vegas Metropolitan Police Department (LVMPD)

17.00 – 17.30 Building Protection – Getting The Principles Right

- Definition of suitable risk mitigation objectives and credible threats
- Options to reduce the loading on buildings
- The differing methods used for protecting the primary, secondary and non-structural elements of a building
- Combining individual protection strategies to produce holistic solutions

Patrick Mann, Section Manager – Blast Engineering, ABS Consulting Ltd

17.30 Close and Evening Drinks Reception

Industry Sponsor

Cyber Security & Electronic Terrorism

WEDNESDAY 20 APRIL

08.40 – 08.45 Coffee and Registration

08.45 – 09.00 Chairman's Welcome & Opening Remarks
Intellect

TERRORISM IN THE DIGITAL AGE

09.00 – 09.30 Delivering the Cyber Security Strategy
- Building capacity to fight cyber crime and electronic terrorism
- Strengthening key government, critical national infrastructure and defence computer systems against cyber attack

Air Commodore Graham Wright CBE, Deputy Director, Office of Cyber Security, Cabinet Office

09.30 – 10.00 Terrorism And New Media
- The relationship between terrorism and new media
- The exploitation of new media to promote terrorism & political violence
- The relationship between media presence and terrorist activity
- The use of smartphones and social media in the Mumbai attacks – by those hiding from the violence and those causing it

Dr Ben O'Loughlin, Co-Director, New Political Communication Unit, Royal Holloway, University of London

10.00 – 10.30 Monitoring Cyber Space For Dangerous, Criminal Or Fraudulent Activity
- The impact of increasing activity in the cyber world – what it means for businesses and government agencies
- The need for monitoring – examining the current state of the art
- How much should we know about the cyber activities of employees, customers and of those seeking to cause loss or damage?

Richard Nethercott, Global Managing Director of Security, Logica

10.30 – 11.00 Tea and Coffee & Exhibition Visit

THREAT AWARENESS

11.00 – 11.40 The Contemporary Terrorist And The Internet
- The role of the Internet – how anonymity, ease of access, lack of regulation and the fast flow of information is exploited
- Assessing the content of terrorist websites – the prevalence of psychological warfare and propaganda
- The extent of online fundraising, recruitment, propaganda dissemination and supply procurement

Dr Maura Conway, School of Law and Government, Dublin City University

11.40 – 12.30 Mobile & Smartphone Vulnerabilities
- Getting access to mobile devices – the focus of criminal activity
- Accessing data stored on mobile devices – connection methods that can be vulnerable to attack
- Countering 'phreaking', 'blue-snarfing' & 'blue jacking'

John Bayliss, Director, Communications Risk Management (CRM)

12.30 – 14.00 Lunch and Exhibition Visit

SECURING INFORMATION TECHNOLOGY & MANAGING ASYMMETRIC THREATS

14.00 – 14.50 Securing Cyberspace In An Era Of Global Connectivity
- Cyber terrorism and cyber warfare – an assessment of the global threat
- How global connectivity facilitates economic espionage, money laundering, cyber fraud, intellectual property theft and security breaches
- The need for a rigorous approach to the security challenges of cyber space

Edward P Gibson, CISSP, Director PricewaterhouseCoopers Global, former FBI Agent – US Embassy London and former Chief cyber Security Advisor, Microsoft (UK) Ltd

14.50 – 15.15 Securing Communications
- Countering threats to information technology infrastructure from increasing threat sophistication
- Countermeasures for the defence of Communication and Information Systems (CIS)
- Strategies for protecting electronic landscapes

Nader Henein, Security Advisory, BlackBerry Security Group, Research In Motion

15.15 – 15.40 Asymmetric Warfare In The Information Age
- Conceptual challenges of information warfare
- Countering the threat of economic and psychological terrorism in asymmetric warfare

Dr Fred Mpala, University of East London

EXPLOITING TECHNOLOGY TO DEFEAT TERRORISM

15.40 – 16.05 Exploiting New Technology & Innovation For Detecting Terrorist Activities
- New tools for tackling terrorism
- Using analytics as an emerging science in detecting terrorist activities
- New visual & text analytics techniques for assessing surveillance data

Dr Eric Atwell, Senior Lecturer, School of Computing, Leeds University

16.05 – 16.30 Implementing National Lawful Interception Platforms For Intelligence And Counter Terrorism
- How national interception platforms are deployed and implemented
- Insights into the difficulties and obstacles when deploying unified intelligence systems
- The key interception technologies that support both normal policing and counter terrorism requirements

Oisin Fouere, Special Projects Advisor, Analysys Mason Limited

16.30 Close

Protecting Crowded Places

WEDNESDAY 20 APRIL

NaCTSO
National Counter Terrorism Security Office

08.40 – 08.45 Coffee and Registration

08.45 – 09.00 Chairman's Welcome & Opening Remarks

Professor Chris Kemp, Executive Dean – Faculty of Enterprise & Innovation and Head of Education, The International Centre for Crowd Management and Security Studies, Bucks New University

COUNTER TERRORISM IN CROWDED PLACES

09.00 – 09.45 UK Counter Terrorism Strategy For Crowded Places

- Assessing the public acceptability of current counter terrorism measures
- Impact of surveillance and territorial control measures in reducing the risk of terrorist attack in cities
- Review of counter terrorism issues for crowded places

DCI Chris Phillips GCGI, FSyI, Head National Counter Terrorism Security Office (NaCTSO)

09.45 – 10.30 Current And Future Threats To Crowded Places

- Assessment of existing and potential terrorist threats to crowded places
- How vulnerable are 'soft' targets such sports grounds, shopping centres and entertainment facilities
- Learning from terrorist behaviour and intent to reduce the risk of terrorist attacks

Mark Joyce, Director Security Intelligence, Stirling Assynt and Americas Fellow, RUSI

10.30 – 11.00 Tea and Coffee & Exhibition Visit

PROTECTING CROWDED SPACES AND PUBLIC BUILDINGS

11.00 – 11.30 Vulnerability Self Assessment

- Reducing the vulnerability of crowded places sites – small to medium enterprises as terrorist targets
- Determining vulnerability to terrorist attack – assistance for owners and operators of crowded places

Lee Doddridge, National Counter Terrorism Security Office (NaCTSO)

11.30 – 12.00 Identification And Disruption Of Terrorist Hostile Reconnaissance

- Key elements in terrorist pre-attack planning and hostile reconnaissance
- How to identify and counter pre-attack planning
- Effecting prevention, disruption and detection of hostile reconnaissance

Centre for the Protection of National Infrastructure (CPNI)

12.00 – 12.30 Protecting Hospitals – The Ultimate Crowded Place

- Potential impact of a terrorist attack and the health sector response
- Update on Project Argus – Health
- How good security arrangements can aid the management and response to an incident
- Responding to incidents – potential scenarios and plans to mitigate against the effects

Christopher John, Policy Lead: Counter Terrorism and Security Preparedness, NHS Counter Fraud and Security Management Service

12.30 – 14.00 Lunch and Exhibition Visit

PROTECTING RETAIL, ENTERTAINMENT & SPORTING VENUES

14.00 – 14.25 Retail Protective Security

- Addressing counter terrorism in the retail environment
- Assessing the threats, vulnerabilities and possible impact
- Lessons from the deployment of protective security in a major retail environment

John Frost, Head of Business Continuity, Marks & Spencer

14.25 – 14.50 Shopping Centres As A Terrorist Target

- The relevance of counter terrorism concerns in retail and shopping centre design
- The need for resilience and protective security against traditional and unconventional threats
- Designing in cost-effective security measures to shopping centre locations with limited protective security
- Ongoing European trends

Derek Barker, Managing Director, Haskoll Architects and Designers

14.50 – 15.15 Designing In And Maintaining Resilience And Protection For Stadia And Arenas

- Key strategies to reduce the risk of a terrorist attack
- Ensuring continual good practice – enhancing the protective security measures
- Linking security strategy and operational security services

Richard Lyall, Facility Services Director, AEG (Europe) – The 02

15.15 – 15.40 The Role Of Police Counter Terrorism Security Coordinators At Large Events

- The core role of Police Security Coordinators and the police security philosophy
- Managing police/public partnerships to deliver safe events
- Balancing risk appetite amongst stakeholders

Chief Inspector Paul Seery, Counter Terrorism Security Coordinator, SO20 Protective Security Command, Metropolitan Police Service

PROTECTING TRANSPORT SYSTEMS

15.40 – 16.05 Securing Airports – A Focus On Terminal Protection

- Impact of the terrorist threat on airports as crowded places
- Addressing vulnerabilities and reducing terrorist opportunities at airports
- Integrating physical security and technology solutions to enhance terminal security

Centre for the Protection of National Infrastructure (CPNI)

16.05 – 16.30 Protecting Crowded Places In The Rail System

- Implications for transport and crowded places policing from high levels of threat from extremism
- Practical security advice to prevent an attack
- Mitigating the immediate effects and on-going consequences of a terrorist attack

Inspector Chris Bunyan, Senior Counter Terrorism Security Adviser (CTSA), British Transport Police

16.30 Close

CYBER DEFENCE

Analysing Global Cyber Threats

16 - 17 May 2011, Istanbul, Turkey

16th to 17th May 2011, Marriott Istanbul, Istanbul, Turkey

Keeping cyber space secure is an increasingly complex challenge. We face threats not only to ourselves as individuals; but to businesses, governments and national security. Cyber Defence 2011 will be held for the first time in Istanbul and will explore the explosive issue of cyber security the world over. Bringing together an extensive list of cyber security professionals from across Europe, the US and Asia – Cyber Defence 2011 will deliver a packed 2 days of presentations, followed by a full day interactive workshop. This event offers you the chance to hear from a diverse speaker faculty representing an array of military, civil and commercial organisations – don't miss the opportunity to meet them and discuss the latest developments in Cyber Defence. *View event website*

19. MEDIZINISCHE A-SCHUTZ-TAGUNG

19th Nuclear Medical Defence Conference

16th to 18th May 2011, Munich, Germany

The Bundeswehr Institute of Radiobiology affiliated to the University of Ulm will be holding the 19th Nuclear Medical Defence Conference from Monday, 16th to Wednesday 18th of May 2011. For the first time the conference will be presented in a new «Update» format. New research findings and insights in the fields of medical radiation protection, radiobiology and radiation medicine will be the key topics. Special attendance is attached to the fact that these aspects will be presented in a comprehensive form for a broader audience thus facilitating the idea of continuous education.

Prof. Dr. Viktor Meineke, Colonel (MC)
Bundeswehr Institute of Radiobiology
affiliated to the University of Ulm

Neuherbergstrasse 11
D-80937 Muenchen
Germany
Tel: +49-(0)89-3168-2251
Fax:+49-(0)-89-3168-2255
Email: viktor.meineke@uni-ulm.de
Web : **http://www.nmd-conference.org/**

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 6850-15-157-8946**
Decontaminant product for persons.

PERSONNEL DECONTAMINATION

BX 30 (powder)

Code 240256
Training version of BX 24

CBRN TRAINING

BX 40 (liquid)

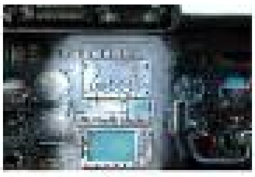
Code 240257 - **NATO Standard Number 6850-15-157-8946**
Decontaminant product for CBRN decontamination of aircraft, helicopters, etc.

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

FD 404

CRISTANINI CBRN
DECONTAMINATION SYSTEMS

A5009
CONFORM TO THE QUALITY SYSTEM STANDARD AQAP 2110
and ISO 9001:2008

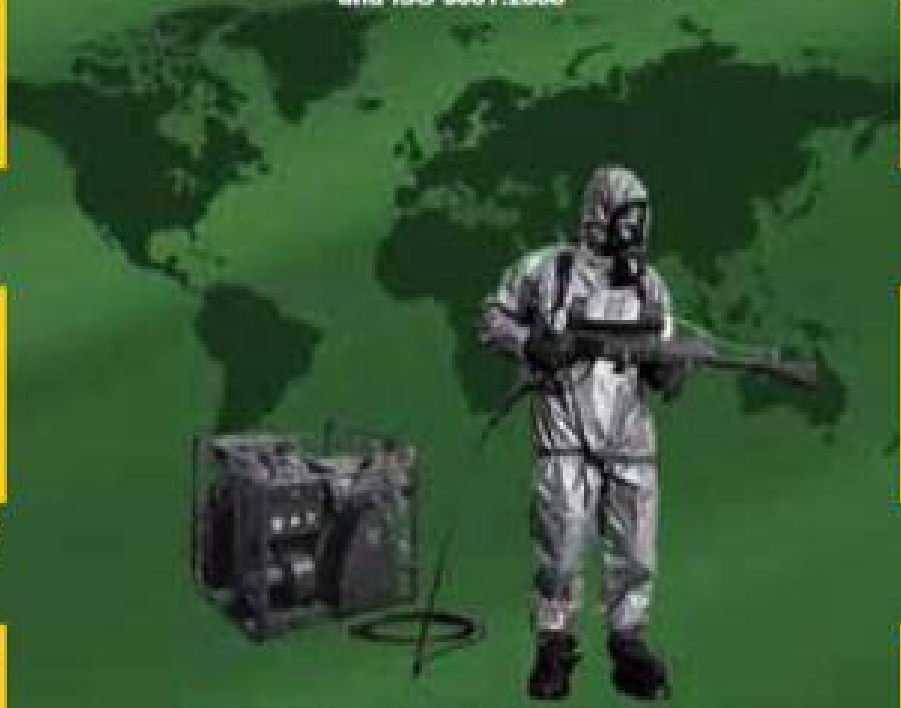
DEPLOYABLE CBRN ANALYTICAL LABORATORY (STANAG 4632)

DEPLOYABLE BIO LABORATORY CLASS III BIO SECURITY LEVEL

RI/CBRN TRAILER FOR CBRN DECONTAMINATION AND DETOXIFICATION

TSDM-TACTICAL STEAM DECON MODULE

SX34 CBRN DECONTAMINATION OF SENSITIVE EQUIPMENT AND SURFACES



ONLY ONE PERSON
ONLY ONE MACHINE
ONLY ONE PRODUCT

DOMAS LARGE SCALE DECONTAMINATION SYSTEM HIGHLY DEPLOYABLE

DOMAS LARGE SCALE DECONTAMINATION SYSTEM DUAL OPERATORS

MOBILE SYSTEM FOR AIRCRAFT DECONTAMINATION

SANIJET C 1126 HR CBRN DUAL OPERATOR DECONTAMINATION AND DETOXIFICATION GROUP

CBRN PRODUCTION LINE

1972

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