Volume 40, 2011

CBRNE
Newsletter
Terrorism

Editor's Corner
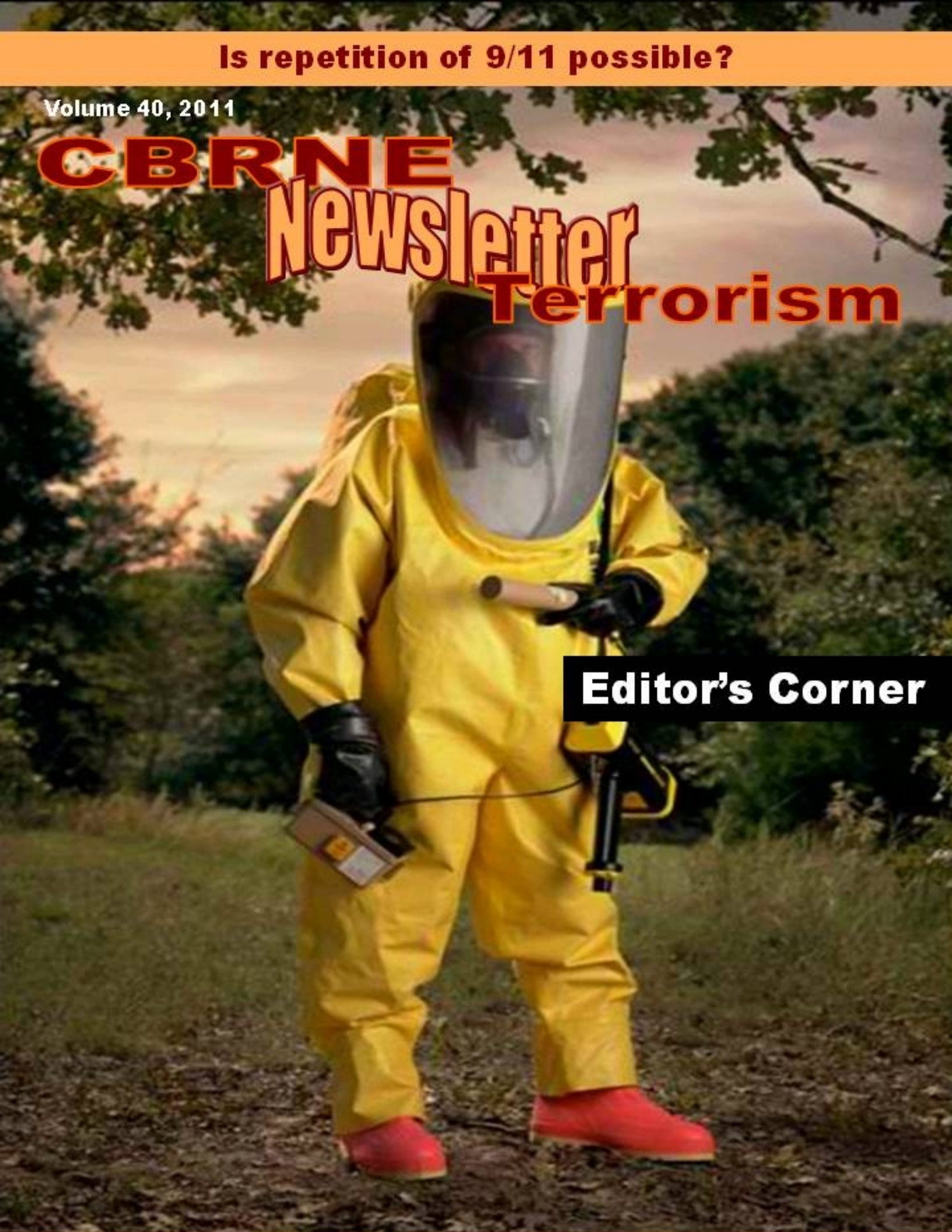
Editor
BG (ret) Ioannis Galatas MD, MA, MC
Consultant in Allergy & Clinical Immunology
Medical CBRN Planner
Senior Terrorism/WMD Analyst
CBRN Scientific Coordinator @ RIEAS
VC Greek Intelligence Studies Association (GISA)
Athens, **Greece**

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
EMDM Alumni Association Treasurer
Council member of the EuSEM DM section
Padua, **Italy**

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

CBRNE-Terrorism Newsletter is published quarterly and distributed free of charge. All full page advertisements in Winter 2011 issue are free of charge; they are just another way to provide information on useful products of interest to First Responders. ► **Starting 2012,** Newsletter will go bimonthly.

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

Full page (A4)	€500 €250
Half page	€400
Inside front cover	€400 €750
Back cover	
Double pages (A4X2)	

Free capability profile will be provided to all advertisers in the same issue (length: 400 words + 1 picture + 1 logo in .jpg format). 20% reduction for annual ad inclusion.

PUBLISHER
Mendor Editions S.A.
3 Selinountos Street
14231 Nea Ionia
Athens, Greece
Tel: +30 210 2723094/-5
Fax: +30 210 2723698

Contact e-mail:
Valia Kalantzi
info@mendor.gr

Explosive News

Anti-magnet: to protect ships' hulls from mines

Source: http://www.homelandsecuritynewswire.com/anti-magnet-protect-ships-hulls-mines

Researchers at the Universitat Autònoma de Barcelona have created a new type of magnetic cloak which shields objects from magnetic fields – at the same time that it
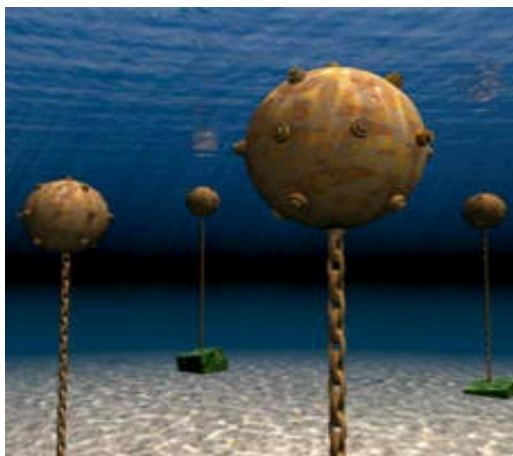
prevents any internal magnetic fields from leaking out.

Fox News reports that this "antimagnet" could be used to protect a ship's hulls from mines that detonate when a magnetic field is detected, or allow patients with pacemakers or cochlear implants to use medical equipment.

The researchers admit, though, that the discovery could also be used by criminals to evade security systems in airports and shops. "It is conceivable that they could be used for reducing the magnetic signature of forbidden objects, with the consequent threat to security," Sanchez told Fox News. "For these reasons, the research could be taken into account by security officials in order to design safer detection systems and protocols."

The researchers' study was published 23 September in the New Journal of Physics. The researchers presented their research at the Superconductivity Centennial Conference held 18-23 September the Hague. The conference was held to mark 100 years of superconductivity.
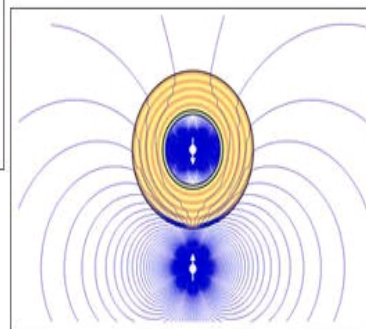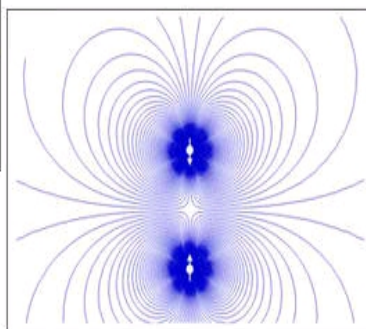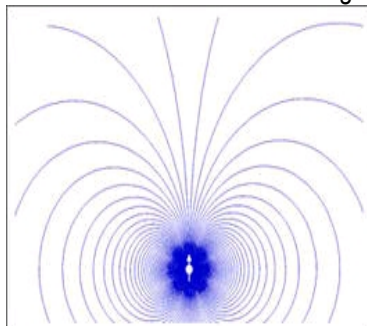
The magnetic cloak calls a truce on warring magnetic fields. On the left, the magnetic field of a lone cylinder-shaped magnet. In the middle, a second magnet, pointing the opposite way, disrupts its field. On the right, the second magnet's field is hidden in the cloak, which also allows the first magnet's field to extend as if the second weren't there at all. Credit: (illustration) J. Prat-Camps; A. Sanchez, C. Navau, D.-X. Chen/Autonomous U. of Barcelona

Researchers develop IED detecting laser

Source: http://www.bbc.co.uk/news/technology-14973447

Improvised explosive devices (IEDs) have proven to be the deadliest threat to allied troops fighting in Afghanistan and Iraq, but
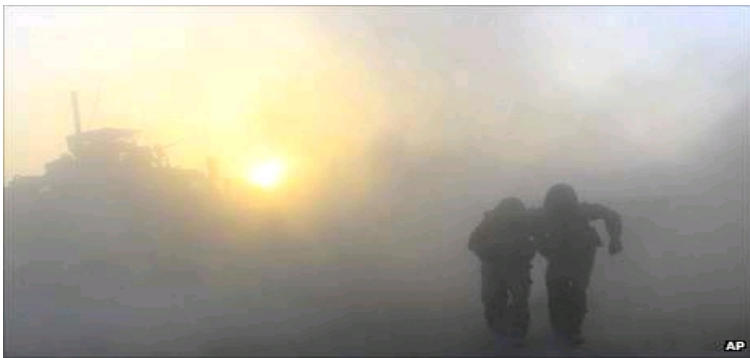
researchers have developed a laser beam that could help neutralize these dangerous weapons.

A team from Michigan State University has created a laser beam that can "sense" where bombs are by making molecules vibrate. The researchers say that each molecule vibrates with a unique frequency, so when the laser hits an IED it could determine if it is an explosive based on its frequency.

Dr. Marcos Dantus, the lead developer of the laser detector, explained that detecting IEDs has proven to be particularly challenging due to the chemical compounds present in the environment that mask the bomb's molecular makeup.

"Having molecular structure sensitivity is critical for identifying explosives and avoiding unnecessary evacuation of buildings and closing roads due to false alarms," he said.

With the laser, troops can use it to analyze the chemical composition of an object from a safe distance. The beam combines short pulses that "kick" the molecules to make them vibrate with longer pulses.

"The laser and the method we've developed were originally intended for microscopes, but we were able to adapt and broaden its use to demonstrate its effectiveness for standoff detection of explosives," Dr. Dantus said.

The team's research remains highly confidential, and when pressed for details, Dantus said, "All we are saying is that it could detect explosives from a stand-off distance."

A true dog of war: Hero RAF dog Buster bow wows out after serving FIVE tours of duty

Source: http://www.dailymail.co.uk/news/article-2045431/War-hero-RAF-dog-Buster-bow-wows-serving-FIVE-tours-duty.html

Air Dog 'Buster' is enjoying a quieter life with RAF Police Sergeant Michael 'Will' Barrow (pictured) in Lincolnshire after braving bombs and bullets over five operational tours of duty

An RAF dog who braved bombs and bullets over five operational tours of duty is retiring a military hero.

Air Dog Buster, a nine-year-old English springer spaniel, has earned a row of campaign medals for his service in in Bosnia, Iraq and Afghanistan.

The arms and explosives sniffer dog now lives with his handler RAF Police Sergeant Michael 'Will' Barrow, 45, and his wife, Tracy, in Cranwell, Lincolnshire.

© Corporal Scott Robertson

But though he will now take a step back from frontline duties, the heroic dog has not turned his back on military life - he is set to become the RAF Police mascot.

In Afghanistan's deadly Helmand

province, Buster saved his countless lives by sniffing out explosive vests - leading to the arrests of two suicide bombers.

He joined his comrades repeatedly on foot patrols through the poppy fields hunting

Taliban insurgents and tracking down booby trap bombs left behind for British and American troops.

Sergeant Barrow told the Daily Express how, even in the face of enemy attacks, Buster's unflappable composure held solid.

Decorated: Buster, a nine-year-old English springer spaniel, has earned a row of campaign medals for his service in in Bosnia, Iraq and Afghanistan

'Each time [we were attacked], Buster waited calmly for the action to cease, then carried on his search for improvised explosive devices, and keeping patrols safe,' he said.

Now Buster will spend the rest of his days with the Barrows and their two dogs - another springer spaniel and a German shepherd.

But, like many military men, adapting to life away from the warzone has not proved easy.

'We had to teach Buster to play with the other dogs,' said Sergeant Barrow.

'When he was a working dog he only got toys when he made a find. And when he came home he

collected up all the dogs' toys and became very

protective of them.'

Hero: During action Buster would wait calmly for the action to cease, then carried on his search for improvised explosive devices, and keeping patrols safe. Seven year old Josh Barrie-Marklow gives the spaniel a welcome home hug

Paper-based wireless sensor detects explosive devices

Source: http://www.homelandsecuritynewswire.com/paper-based-wireless-sensor-detects-explosive-devices

Researchers at the Georgia Institute of Technology have developed a prototype wireless sensor capable of detecting trace amounts of a key ingredient found in many explosives. The device, which employs carbon nanotubes and is printed on paper or paper-like material using standard inkjet technology, could be deployed in large numbers to alert authorities to the presence of explosives, such as improvised explosive devices (IEDs).

"This prototype represents a significant step toward producing an integrated wireless system for explosives detection," said Krishna Naishadham, a principal research scientist who is leading the work at the Georgia Tech Research Institute (GTRI). "It incorporates a sensor and a communications device in a small, low-cost package that could operate almost anywhere."

A Georgia Tech release quotes Naishadham to say that other types of hazardous gas sensors are based on expensive semiconductor fabrication and gas chromatography, and they consume more power, require human intervention, and typically do not operate at ambient temperatures. Furthermore, those sensors have not been integrated with communication devices such as antennas.

The wireless component for communicating the sensor information — a resonant lightweight antenna — was printed on photographic paper using inkjet techniques devised by Professor Manos Tentzeris of Georgia Tech's School of Electrical and Computer Engineering. Tentzeris is collaborating with Naishadham on development of the sensing device.

The release reports that the sensing component, based on functionalized carbon nanotubes (CNTs), has been fabricated and tested for detection sensitivity by Xiaojuan (Judy) Song, a GTRI research scientist. The device relies on carbon-nanotube materials optimized by Song.

A presentation on this sensing technology was given in July at the IEEE Antennas and Propagation Symposium (IEEE APS) in Spokane, Washington, by Hoseon Lee, a Ph.D. student in the School of Electrical and Computer Engineering co-advised by Tentzeris and Naishadham. The paper received the Honorable Mention Award in the Best Student Paper competition at the symposium.

This is not the first inkjet-printed ammonia sensor that has been integrated with an antenna on paper, said Tentzeris. His group produced a similar integrated sensor last year in collaboration with the research group of C.P. Wong, who is Regents professor and Smithgall Institute Endowed Chair in the School of Materials Science and Engineering at Georgia Tech.

Tentzeris explained that the key to printing components, circuits and antennas lies in novel "inks" that contain silver nanoparticles in an emulsion that can be deposited by the printer at low temperatures — around 100 degrees Celsius. A process called sonication helps to achieve optimal ink viscosity and homogeneity, enabling uniform material deposition and permitting maximum operating effectiveness for paper-based components.

"Ink-jet printing is low-cost and convenient compared to other technologies such as wet etching," Tentzeris said. "Using the proper inks, a printer can be used almost anywhere to produce custom circuits and components, replacing traditional clean-room approaches."

Low-cost materials — such as heavy photographic paper or plastics like polyethylene terephthalate — can be made water resistant to ensure greater reliability, he added. Inkjet component printing can also use flexible organic materials, such as liquid crystal polymer (LCP), which are known for their robustness and weather resistance. The resulting components are similar in size to
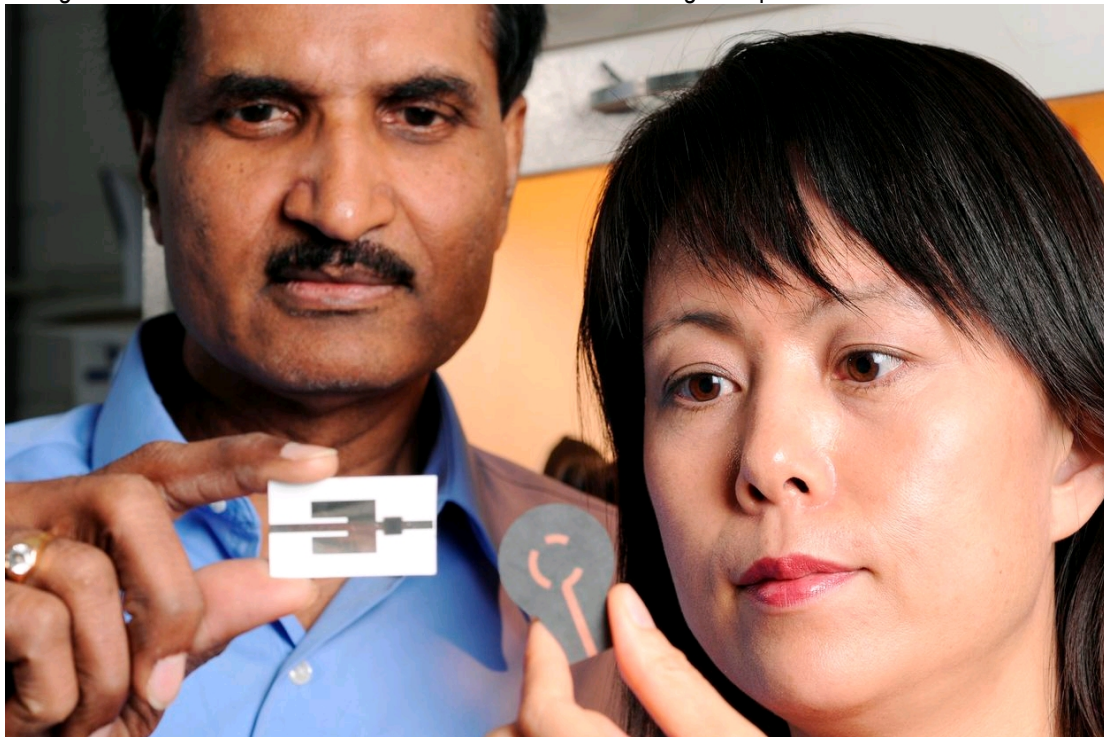
"The fundamental difference is that this newest CNT sensor possesses dramatically improved sensitivity to miniscule ammonia concentrations," Tentzeris said. "That should enable the first practical applications to detect trace amounts of hazardous gases in challenging operational environments using inkjet-printed devices."

conventional components but can conform and adhere to almost any surface.

Naishadham explained that the same inkjet techniques used to produce RF components, circuits and antennas can also be used to deposit the functionalized carbon nanotubes used for sensing. These nanoscale

cylindrical structures — about one-billionth of a meter in diameter, or 1/50,000th the width of a human hair — are functionalized by coating them with a conductive polymer that attracts ammonia, a major ingredient found in many IEDs.

Sonication of the functionalized carbon nanotubes produces a uniform water-based ink that can be printed side-by-side with RF components and antennas to produce a compact wireless sensor node.

"The optimized carbon nanotubes are applied as a sensing film, with specific functionalization designed for a particular gas or analyte," Song said. "The GTRI sensor detects trace amounts of ammonia usually found near explosive devices, and it can also be designed to detect similar gases in household, healthcare and industrial environments at very low concentration levels."

The sensor has been designed to detect ammonia in trace amounts — as low as five parts per million, Naishadham said.

The resulting integrated sensing package can potentially detect the presence of trace explosive materials at a distance, without endangering human lives. This approach, called standoff detection, involves the use of RF technology to identify explosive materials at a relatively safe distance. The GTRI team has designed the device to send an alert to nearby personnel when it detects ammonia.

The wireless sensor nodes require relatively low power, which could come from a number of technologies including thin-film batteries, solar cells or power-scavenging and energy-harvesting techniques. In collaboration with Tentzeris's and Wong's groups, GTRI is investigating ways to make the sensor operate passively, without any power consumption.

"We are focusing on providing standoff detection for those engaged in military or humanitarian missions and other hazardous situations," Naishadham said. "We believe that it will be possible, and cost-effective, to deploy large numbers of these detectors on vehicles or robots throughout a military engagement zone."

Mother of 9-year-old Iraqi suicide bomber arrested

Source:http://www.thenational.ae/news/worldwide/middle-east/mother-of-9-year-old-iraqi-suicide-bomber-arrested

Iraqi security forces have arrested a woman whose boyfriend convinced her to send her little boy on a suicide mission and then failed to stop the attack after she had a change of heart, police said.

Sunni widow Suad al-Obaidi, 47, was arrested on Friday along with her allegedly Al-Qaeda boyfriend, after attacks on anti-Qaeda Sahwa (Awakening) militia in Diyala province a day earlier, a Diyala police officer told AFP. She was arrested in Diyala province, while the boyfriend, Hamid Alwan, 53, was detained in

Baghdad.

According to the officer, Alwan convinced Obaidi to send nine-year-old Murtada Latif Kadhem to bomb a Shiite mosque in Khales, north of Baghdad, several years ago. Alwan "took her son with her ... by car to the Shiite mosque but, on the way there, she started to cry about her son," the officer said. "He put her out of the car, and took the son, who was wearing an explosive belt, to the mosque," where "he blew himself up."

Security officials said the December 29, 2006 attack killed at least nine people, including the imam of the mosque, and wounded at least eight.

A few months later, Alwan tried to convince Suad to send her 18-year-old son Kadhem Latif

Kadhem on a suicide attack, but he fled to the home of his married sister, Hanna.

Diyala province, north of Baghdad, was the scene of bloody sectarian fighting that left thousands dead. "After the attacks against the Sahwa (Awakening) last Thursday, we received information about terrorists groups and wanted people in some areas in Diyala," said the officer. "We arrested a group of terrorists and through the investigation we reached Hamid and arrested him in Baghdad Friday."

On Thursday, a suicide bomber and a car bomb targeted Sahwa militiamen near Baquba, north of Baghdad, killing five people and wounding 26, an army officer and a doctor said.

U.S. Officials Reveal Al-Qaeda Breakthrough in "Super Explosives"
Source: http://kabulpress.org/my/spip.php?article86605

Several years ago an official with the State Department's Bureau of Diplomatic Security disclosed to this author that al-Qaeda scientists had achieved a stunning breakthrough in non-nuclear explosives. At that time al-Qaeda

air and flipped it over along a Kabul highway killing all 13 military and civilian occupants.

The story begins at the Bureau of Diplomatic Security's training facility at Summit Point, West Virginia. This author, who was serving in the State Department at the time, was selected for an anti-terrorist training program run by security officials Brian Duffy and Martin Burk. On March 26, 2008, this author was given an unclassified briefing by one of the Bureau's senior ordinance experts. That official disclosed the al-Qaeda breakthrough. He described State Department officials as being fearful of the consequences of this new class of explosives. He went on to reveal that government

experts were reportedly on the verge of developing a new class of "super explosives." A more accurate description would be to refer to them as "sustained detonation" or "uncurved brisance" explosives. On October 29, 2011, those explosives may have made their debut when one of NATO's supposedly "bomb-proof" Rhino armored buses was hit by a suicide car bomb which threw the massive Rhino into the

experts were stunned because they did not know that sustained detonation or uncurved brisance explosives were even possible. True to form the Bureau and the State Department have concealed this information from the American public and more importantly from U.S. troops who would have to face these explosives. It is not clear if the information was ever disclosed to Congress. The

resulting lack of public discussion means that the U.S. military is unprepared to deal with these new weapons; weapons which expose American personnel to new and heightened risks.

Chemical explosives, i.e., those which detonate rather than simply burn, obtain most of their destructive power due to a supersonic shock wave formed by the detonation impulse. The higher the velocity of the impulse the greater its shattering power. That is generally referred to as the "brisance" of the explosive. The name originated from the French verb "briser" meaning to break or shatter. The velocity can be depicted as a curve in which the impulse climbs, peaks and then falls. According to Diplomatic Security officials, the **al-Qaeda's explosives rise and peak but do not immediately fall.** Instead the peak can be maintained for a very short period. As a result there is no curve as with conventional

cryogenics, including liquid oxygen (LOX). There was a report that the terrorist group Jemaah Islamiyah used crude thermobaric explosives in its 2002, Bali bombings. This new threat prompted writer David Eshel in 2006, to coin the term "thermobaric terrorism."

In the aftermath of the October 29, 2011, Kabul attack, U.S. and NATO officials released a misleading analysis of the attack. They stated that 700 kilograms of explosives were used. That comment was misleading because they could not possibly know the amount of explosives. The blast effects of 700 kilograms of ammonium nitrate, TNT and RDX explosives are considerably different. All that these officials could possibly say about the Kabul explosives is that the blast effects are consistent with that produced by 700 kilograms of a conventional explosive. The fact is that the same explosive effect could have been produced by perhaps 200 kilograms of a super

explosives. This would magnify their destructive power considerably.

There is reportedly substantial research on-going in this area. The Pentagon had been the leader in new explosives due to its pioneering work in thermobaric explosives, which use fuel/air mixtures combined with powdered aluminum to achieve a longer duration blast. Other theoretical super explosive research has focused on using metallic hydrogen and

explosive. If so, the Kabul attack may signal the ominous beginning of a new terrorist campaign wherein small quantities of super explosives might be used to bring down commercial airliners, destroy public buildings and attack infrastructure targets in the West. **Support for the premise that a super explosive may have been used in the Kabul attack can be seen in the following facts:**

1. 700 kilograms is a massive weight for an average civilian passenger vehicle to covertly transport, which makes the U.S./NATO claims suspect;
2. This was clearly intended to be a demonstration of something new as the terrorists chose the most bomb-proof vehicle in the U.S./NATO

weapons of mass destruction) and it may now be fueling the Afghan War.

If these explosives exist and if their use is being concealed by the Pentagon and NATO, then billions of dollars in U.S. taxpayer funds spent on MRAPs (mine resistant vehicles) may have been wasted. With each new terrorist weapon, a counter needs to be devised and fielded as quickly as possible. The concern is
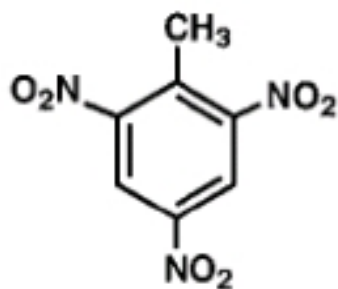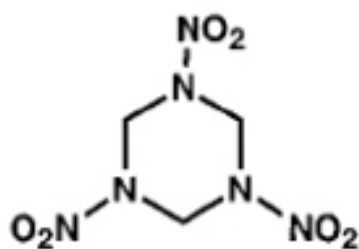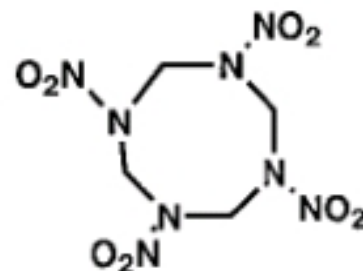
TNT   **RDX**   **HMX**
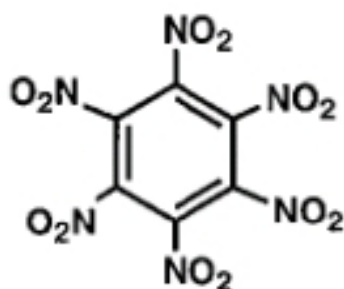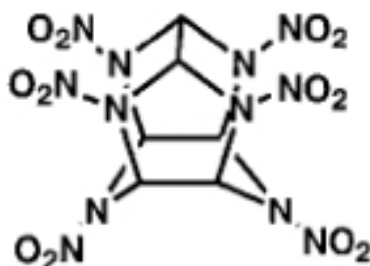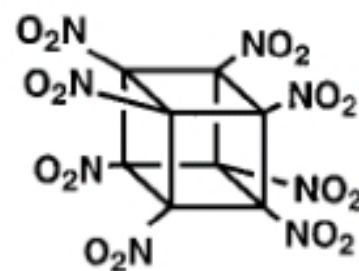
HNB   **CL-20**   **ONC**

inventory as their target;
3. We know from the State Department that terrorist groups have had these super explosives for at least several years; and finally,
4. U.S. officials cannot be relied on to publicly acknowledge the existence of these new al-Qaeda weapons or their use. They would likely view the truth as destabilizing because the increased risks to American forces might undermine the already dwindling support in the U.S. for the Afghan war. Deception fueled the Vietnam War (with the fabricated Tonkin Gulf incidents), the Iraq War (with Saddam Hussein's fabricated

that excessive secrecy may have delayed research into new equipment, armor and vehicles to counter this emerging threat. The consequences may be that more Americans troops will die needlessly, just as they did as a result of previous delays in fielding upgraded body armor, armored HUMVEES and the original MRAPs; and no Administration officials, Generals or Admirals will ever be held accountable.

The American way of war perhaps can be summed up in two rules:
"Rule 1: the truth gets concealed, inept officials prosper and soldiers die, and
 Rule 2: no one seems to be able
to change Rule 1."

New Gunshot Detection Capability Expands the Role of Mini-UAVs in Force Protection

Source:http://defense-update.com/20111031_new-gunshot-detection-capability-expands-the-role-of-mini-uavs-in-force-protection.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+DefenseUpdate+%28Defense+Update%29

Detecting gunshots has always challenged the

Microflown Acoustic Sensor for UAVs

military and law enforcement agencies. Two principal approaches are used – detecting the acoustic signature of the gunshot and spotting the visible signature of the event. A new approach combining a new approach to acoustic detection, developed by the Dutch company Microflown Avisa has now matured and is introduced for use on unmanned aerial vehicles.

Microflown Avisa is displaying two applications of its gunshot detector at ISDEF 2011, an artillery fire locator capable of detecting artillery and mortars firing events at ranges of 30km and a new airborne gunshot detection system, that can be mounted on a mini UAV and offer detection ranges up to seven kilometers.
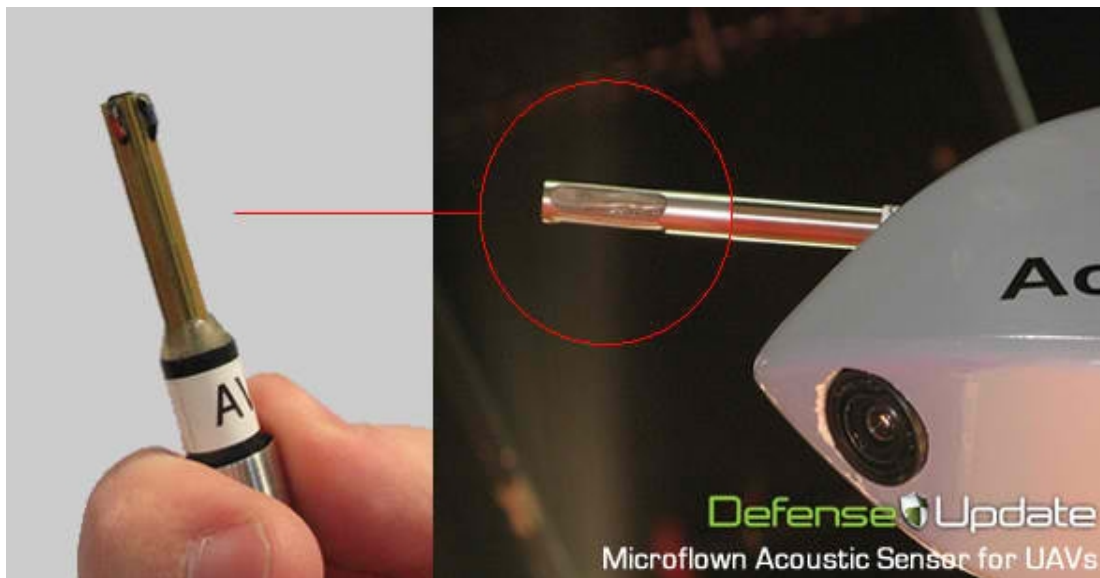
The proprietary Miniature Electro-Mechanical System (MEMS) vector sensor developed by Microflown measures temperature differences in the cross-section of two extremely sensitive heated wires, to determine acoustic particle velocity. Assembling three orthogonally placed sensors in one single point, a very compact acoustic vector sensor is produced. The integrated processor computes these parameters to provide bearing, and elevation at the firing source, at angular accuracy of 0.25-2 degrees. Further algorithms and additional

acoustic vector sensor allows distance to be measured (by triangulation).

Microflown Avisa displayed here an acoustic sensor for UAVS, enabling micro drones to detect gunshots from seven kilometers. Photo: Tamir Eshel, Defense Update.

Actual performance depends on weather and humidity conditions, but the sensor can operate effectively even under 100% humidity as well as extreme high or low temperatures. The sensors can detect and report multiple sources of fire simultaneously, even in complex acoustic situations such as urban environments or on noisy platforms such as UAVs.

The company is now offering UAV acoustic sensors to equip miniature UAVs. At ISDEF Microflown highlights the sensor integrated on a Aerovironment Raven, offering effective situational awareness for small units operating the miniature drone. According to John Bremner, business development manager at Microflown, the sensor weighing about 200 grams can be best integrated in the mini UAVs employing pusher propellers, as it offers a clean environment for the system. The sensor can also be integrated on aerostats, typically

operated on force protection missions.

Response to Homemade Explosives

By August Vernon
Source:http://www.fireengineering.com/articles/print/volume-164/issue-11/features/response-to-home made-explosives-.html

Improvised explosive device (IED) and homemade explosive (HME) attacks can consist of anything from homemade pipe bombs to sophisticated military ordnance; however, emergency service agencies are more likely to encounter IEDs/HMEs than military weapons in their day-to-day responses. Terrorists around the globe prefer explosives for several reasons, as the recent explosives incidents in Norway, Pakistan, Iraq, and Afghanistan have shown. The Federal Bureau of Investigation's annual report on terrorism shows that explosive incidents constitute the majority of domestic terrorism attacks in the United States. Public safety agencies at all levels (local, regional, state, military, and federal) must learn to work together to deter IED attacks in their jurisdictions and to safely respond if an attack occurs. Understanding some basic information, such as indicators and tactics, may help first responders prevent the initial attack and protect themselves and the

public from secondary attacks.

This article provides some easy-to-follow procedures and guidelines to assist responders and incident commanders in their planning and training efforts. The information presented in this article should not replace common sense and experience. It is impossible to plan for every situation that may occur. New intelligence, "best practices," lesson learned, and training become available on an ongoing basis. Update these plans on a regular basis.

Home-made/improvised explosive materials
Improvised explosive materials are typically made by combining an oxidizer with a fuel. Many of these materials are fairly simple to make, requiring very little technical expertise or specialized equipment. Instructions on how to make them are provided on the Internet and in written resources such as The Anarchist Cookbook. However, recipes for homemade explosives are often inaccurate and dangerous to follow. Even accurate recipes are extremely dangerous, and the explosive materials created are often highly unstable.

(1) IEDs can be found in several different sizes, kinds, and types. (Photos by author.)

More than one would-be explosives maker has been killed or injured attempting to make these materials. These clandestine locations can be a fire and explosive hazard when discovered.

Recipes for making nitroglycerin, mercury fulminate, blasting gelatin, dynamite, TNT, tetryl, picric acid, black powder, and smokeless powder are readily available. Picric acid, nitrogen trichloride, and nitrogen tri-iodide are not marketed as commercial explosives, but they are used in laboratories and in other industrial uses. They are potentially very unstable and could be

used for criminal purposes. The attacker in the Oslo, Norway, car bombing was reported to have used a 2,100-pound device using fertilizer that was built at the bomber's farm.

Peroxide-based explosives

Peroxide-based explosives such as triacetonetriperoxide (TATP), hexamethylene triperoxide diamine (HMTD), and methyl ethyl ketone peroxide (MEKP) are growing concerns and threats. TATP has been frequently used by Middle Eastern terrorists to produce devices for suicide bombers' belts, and it has been used in several recent terrorist attacks globally, including the 2005 London mass transit suicide bombings. Peroxide-based explosives can be made by mixing concentrated hydrogen peroxide (an oxidizer) with a fuel, such as acetone or ethanol, along with a strong acid. Different recipes vary the fuel and concentration of peroxide to create a range of explosives. Both TATP and HMTD are very dangerous to make and handle because they are very unstable. Both can be made in illicit laboratories located almost anywhere since highly specialized equipment is not needed for the manufacturing process. TATP is typically found in crystal form while HMTD is usually a powder; however, peroxide explosives can be in liquid form as well.

HME Information Sources

Information on the construction and deployment of HMEs is readily available to the public. Many of the different methods of

explosives attacks are described in detail in the al-Qaeda and Jihad training manuals and videos.

(2) Some of the reference materials that may be found in a clandestine explosives lab.

Several specialty publishers produce books that show how to build devices using improvised materials and commercial products. Military field manuals have also been used as sources of information and can be purchased at yard sales and online. All these sources of information are also easily found on the Internet and are readily available to anyone with an interest.

Explosives Labs

Some explosive labs do not need to heat or cook any of their materials and, therefore, may lack the glassware, tubing, Bunsen burners, chemical bottles, and other paraphernalia traditionally associated with the term laboratory. However, a lab established to make explosive chemical mixtures might look more like a traditional industrial or university chemistry lab, and labs used to make TATP, HMTD, or other peroxide-based explosives might look much like a meth or drug lab.

They can be mistaken for clandestine drug labs because of the presence of household chemicals. Some improvised explosive materials can also be mistaken for narcotics. These labs can be discovered anywhere, since they do not require a lot of equipment or resources. Recipes are very easy to find on the Internet and in anarchist literature, terrorist materials, and other sources. Common explosives materials such as black powder, gunpowder, or smokeless powder can be easily incorporated into an IED. Some improvised explosive materials such as TATP and HMTD require a clandestine production lab to create. The materials needed to produce these two dangerous explosives can be found in hardware and drug stores. The basic ingredients are a fuel and an oxidizer.

Use caution. Peroxide-based explosives are extremely sensitive to heat, shock, and friction. Some indicators of a possible explosives lab can include the following:

- Refrigerator/coolers/ice baths.
- Glassware and laboratory equipment.
- Blenders.
- Blasting caps/batteries/fuses/switches.
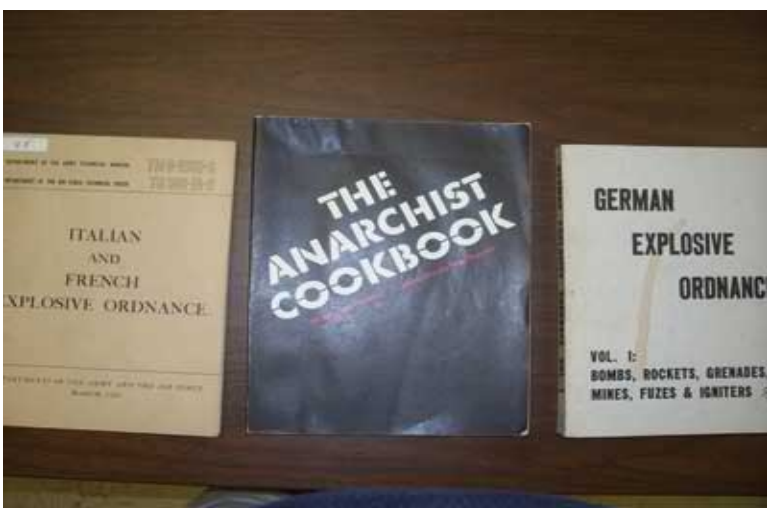
- Pipes/end caps/storage containers.
- Shrapnel-type materials.
- Strong acidic odors.
- Hot plates.
- Some of the common ingredients that may be found in a TATP/HMTD lab include the following:
- Acetones.
- Hydrogen peroxide.
- Strong or weak acids.

Once the materials are produced, they can be incorporated into a variety of IEDs. If a material is being transported using a cooling method (such as ice in a cooler), treat it with caution, as this is a favorite method of transporting raw materials. All types of clandestine labs are dangerous. Responders should be able to safely identify them and take the appropriate safety measures. If mishandled, the materials in an explosives lab can pose a significant danger.

Other clues to the presence of an explosives lab might include literature on how to make bombs, significant quantities of fireworks, hundreds of matchbooks or flares, ammunition like shotgun shells, black powder, smokeless powder, blasting caps, commercial explosives, incendiary materials, or other chemicals on the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) explosive materials list. Finding these items in conjunction with components that can be used to make IEDs (pipes, activation devices, propane containers, and the like) would give even more evidence of an explosives lab. Also, electronic components such as wires, circuit boards, batteries, cellular phones, and other items can point toward the possible design of an IED.

Responders must use extreme caution inside any type of clandestine laboratory. Do not attempt to approach, move, handle, or disarm a confirmed or suspected IED or HME. This is a job for specially trained and equipped personnel.

IED identification

Responders must also be able to recognize a possible explosives material, an IED, or a booby trap. An IED can be discovered during a terrorist or criminal explosives incident response or when conducting routine public safety investigative or response activities. IEDs can be designed to be concealed or look like ordinary items. Be very cautious of any items that arouse your curiosity, and remember that the exterior inspection of a suspected device does not ensure its safety. Be especially wary of the following:

- Unusual devices or containers with electronic components such as wires, circuit boards, cellular phones, antennas, and other items attached or exposed.
- Devices containing quantities of fuses, fireworks, match heads, black powder, smokeless powder, incendiary materials, and other unusual materials or liquids.
- Materials attached to an item such as nails, bolts, drill bits, marbles, and so on that could be used for shrapnel.
- Ordnance such as blasting caps, detcord, military explosives, commercial explosives, grenades, and the like.
- Any combination of the above described items!

On-scene activities

A first responder who comes across a suspicious material/item during routine activities or tactical operations should immediately inform all personnel and leave the area. Do not use your radio, cell phone, or mobile computer terminal until you are a safe distance (at least 300 feet minimum) from the material or item, depending on location and terrain.

(3) IEDs may consist of some type of electronic materials, circuit boards, wires, cell phones, and timers.

If you find yourself next to a possible suspicious materials/item, take these steps:

- Call out to other response personnel to stop moving.
- Stop and look around for any other devices or suspicious items.
- DO not touch or move anything.
- DO not operate light, power, or electrical switches.
- Keep other responders from coming over to look or take photos.
- Do not approach or handle the suspected device/materials once they have been identified as a risk.
- Move out of the area the same way you entered by retracing your steps.
- Conduct personnel accountability reports outside the danger area.
- Isolate and secure the area.
- Establish zones of control (Hot, Warm, and Cold).
- Shield yourself, other responders, and the public.
- Call and wait for the local or state bomb squad/hazardous device unit.
- Notify other proper authorities, depending on the jurisdiction and situation.

The best and most effective defense is to be aware of your surroundings. Based on your threat, if you think the object does not belong in your area, consider it suspicious.

Scene management

Immediately implement the incident command system and unified command for these events. The response to an IED, an HME, an anti-personnel device, or a booby trap is very similar to that for a hazardous materials response. Use your "zones of control" to assist in your response efforts: Hot zone (where the device is located), Warm zone (where the perimeter will be established), and Cold zone (secured location of unified command post and staging). Notify all appropriate agencies (fire, emergency medical services, law enforcement, bomb squad, emergency management office, and hospitals) as soon as possible if there is a report of an incident or a possible threat. Resist the temptation to look at or take pictures of a confirmed or suspected IED.

Secondary devices

If explosives devices or materials are discovered during a response or an illicit lab operation, be prepared for the presence of a secondary device or threats. Be aware of your surroundings, and search the critical areas such as the locations of the command post and staging area. In the Middle East and Far East, there have been multiple incidents in which secondary devices were left for first responders. In the United States, there have been several cases of secondary devices having been planted.

Planning and training

Preparation is the key to mitigating an IED incident; that includes having a clear idea of your actions before the incident occurs. This should at least include an awareness of the hazards associated with IEDs and the proper steps for the responders to take on the discovery of an item or response to an incident. If there is a local bomb squad or a hazardous devices unit in your area, ask it to help you train and plan. Most bomb technicians will be glad to provide your agency with training on their procedures and equipment, since they will require your support during an incident.

Responders should understand their roles and responsibilities in supporting bomb squads during these incidents and how to safely treat an injured bomb tech and remove the bomb tech's suit and equipment in case of injury. An excellent training resource is the Incident Response to Terrorist Bombings course in Soccoro, New Mexico, funded through the U.S. Department of Homeland Security. This course provides information regarding planning for and responding to IED and terrorist events. Students will witness live explosive events ranging from a small pipe bomb to a large car bomb. Students will be able to provide awareness-level training for their agencies.

August Vernon is the operations officer for the Forsyth County (NC) Office of Emergency Management. He returned to his position at emergency management in 2005 after a year in Iraq as a security contractor. He has been employed in this field for more than 10 years, has served in the fire service and as a fire service instructor, and also has served in the U.S. Army as a CBRN (chemical, biological, radiological and nuclear) operations specialist. Vernon has given more than 140 multiagency

presentations over the past 11 years and instructs in incident command, mass violence, crisis management, emergency management, and terrorism planning response. He is a member of the IFSTA WMD/Terrorism Committee. Since 2004, he has been a technical reviewer for Emergency Film Group. Vernon provides critical incident and crisis management planning and training at the local, regional, state, and federal levels. He is the author of the First Responders Critical Incident Guide (Red Hat Publishing).

Researchers develop printable explosive detectors

Source:http://www.homelandsecuritynewswire.com/srdetect20111107-researchers-develop-printable-explosive-detectors

Researchers at the Georgia Institute of Technology are developing a low-cost explosives detector that can be printed on an inkjet printer.

The explosive detector uses a wireless sensor to detect trace amounts of ammonia, a key
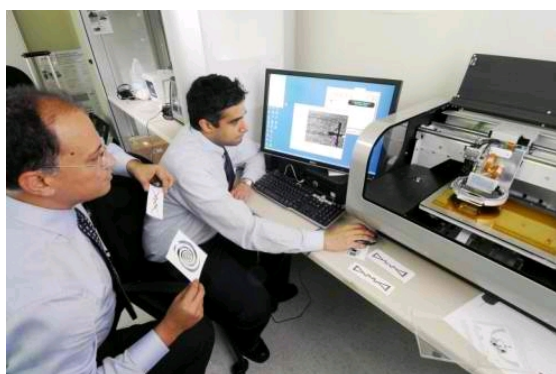
chemical used in improvised explosive devices (IEDs), the deadliest killer of U.S. troops in Iraq and Afghanistan.

The detector has the potential to be deployed cheaply and broadly in warzones as the sensor and its antennae can be printed on paper-like material from an inkjet printer. In addition, the device has low power requirements allowing it to operate for several days when attached to long lasting, thin-film batteries.

The military hopes to eventually scatter large amounts of these sensors downrange to help thwart the threat of IEDs. "IEDs are a very pressing problem. A lot of military personnel and civilians are losing their lives," said Krishna Naishadham, the principal research scientist, who is leading the team of Georgia Tech researchers. "The sensors being used are expensive or require special training. We had the idea of producing something low-cost, so you could spread these in the field."

The integrated sensors are capable of detecting trace elements of explosive materials from as far as sixty-five feet away. In addition, the sensors can be used to check shipping containers for explosives as well as at airports
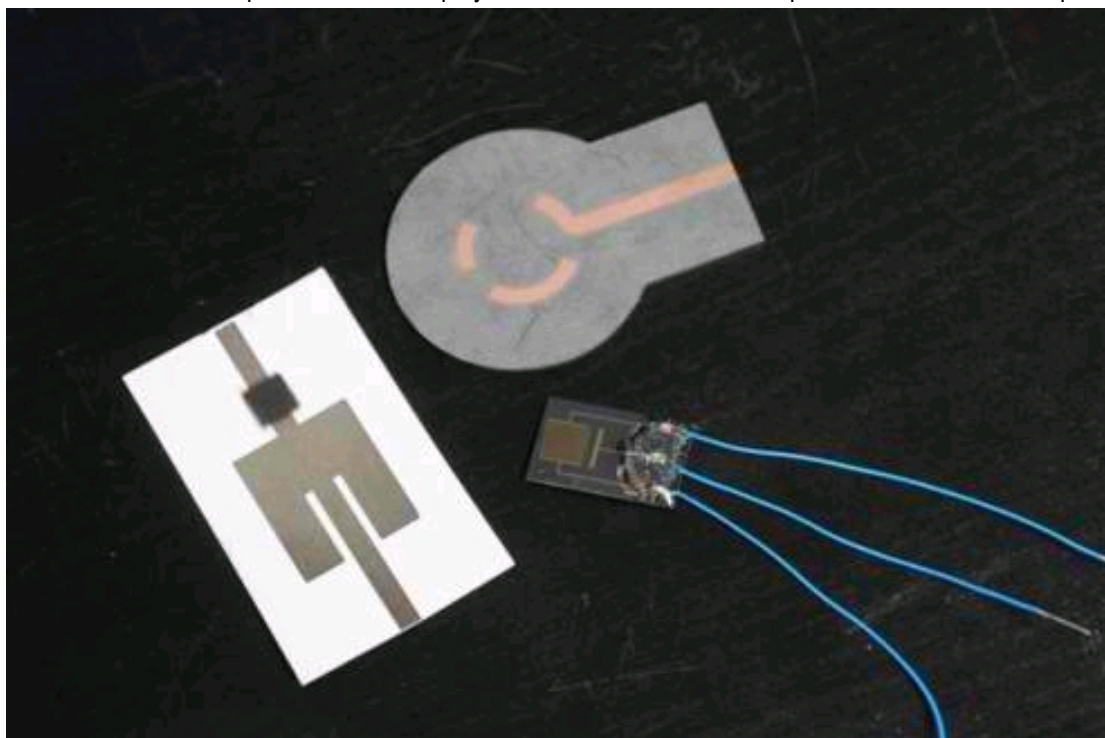
and border security checkpoints.

Currently, the sensors still have a few kinks that need to ironed out before they can be deployed. For instance, detecting ammonia alone would yield far too many false-positives as the chemical is found in many other sources like runoff from fertilizer. "Two important things need to be done before this technology is made ready for field applications," Naishadham said. "You want to maximize the sensitivity while filtering responses to remove naturally occurring gases."

Researchers also hope to improve the sensors to detect other gases so they can be deployed in a variety of settings like in hospitals to detect biological or environmental contamination.

As of now, the sensors still require specialized ink-jet printers that can create a specific pattern on photographic paper, so they are only practical in a laboratory setting.

Naishadham believes full-scale production of sensors is still roughly two to three years away. "It's low-cost, but not low-manufacturing yet," he said.

New detector can identify homemade explosives in under a minute

Source:http://www.homelandsecuritynewswire.com/srdetect20111107-new-detector-can-identify-home made-explosives-in-under-a-minute

A new technique could help investigators identify the type of explosive used in an attack in less than sixty seconds. The new technology is designed to aid security personnel in detecting homemade explosives, which are more difficult to detect.

"Homemade bombs are much harder to detect," explained Michael Breadmore, associate professor of chemistry at the University of Tasmania.

According to Breadmore, homemade explosives contain inorganic molecules like nitrates and chlorates that are not volatile. In the detection process it takes time and skill to separate these ions from a sample. But using capillary electrophoresisAustralian researchers at the University of Tasmania have developed a new method to quickly and accurately detect inorganic explosives.

An investigator can take a sample, either by swabbing a briefcase handle or from debris after an explosion, and turn it into a solution that is then injected into a capillary filled with a flowing electrolyte solution under the influence of a strong, applied electric field.

Depending on their electrical charge and size, the sample's ions move through the capillary at different speeds and based on this knowledge an investigator can identify the ions based on their charge and the time it took them to move through the capillary.

Bruce McCord, a forensic scientist at Florida International University, said the new system is novel in its potential for portability as well as its "definite advantage in terms of speed."

Researchers are currently working on way to design a user-friendly interface and hope to finish the system by mid-2012.

Smart phones enhanced with nanotube hazmat detectors bring a new dimension to preparedness

Source:http://www.gsnmagazine.com/node/24920?c=disaster_preparedness_emergency_response
By Chris Needs

What if your cell phone could detect toxic airborne substances like carbon monoxide, chlorine or even chemical warfare agents?

The public would have a new level of personal protection against a range of fairly common airborne chemical-based toxins, as well as against terrorist attacks involving WMDs. And when sensor data is harnessed in an environmental sensing network for first responders and other organizations, it will be

the dawn of a new era for disaster preparedness.

While this may sound like science fiction, it has become a reality today, and it is known as **Cell-All**. The U.S. Department of Homeland Security's Science and Technology directorate and a cadre of technology and disaster preparedness partners recently demonstrated the Cell-All capability at a Los Angeles Fire

Department training facility. The technology is based on new nanotube sensors developed by NASA and Synkera Technologies and is engineered to work within the small space and power consumption requirements of a cell phone.

operates incident monitoring centers for government and corporate clients. NC4 analysts are trained to quickly assess the incident, correlate it with other real-time information and contact first responders or other organizations -- all within minutes of initial

Qualcomm technology captures the sensor data, scrubs it of any personal information associated with the owner of the cell phone, and uses a series of algorithms to characterize the confidence, severity, location and other aspects of the incident. The validated incident

detection.

The benefits of this technology for emergency and disaster preparedness are evident on numerous levels. An individual could be notified immediately if there were abnormal concentrations of a toxic chemical in close
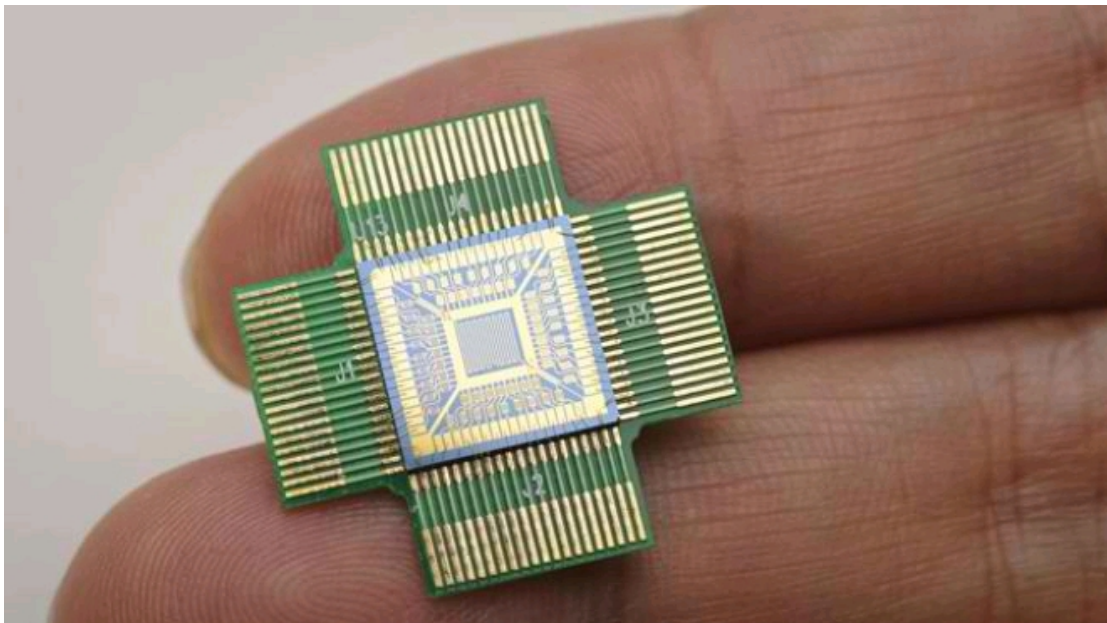
data is then transmitted to analysts at NC4, a technology and services company that

proximity. The sounding of an alarm brings instant situational

awareness to the owner of the smart phone, so that he or she can take action and get to safety. If the individual opted into the environmental sensing network, hazmat teams and first responders would be notified automatically, helping to alleviate the strain on the increasingly overburdened 9-1-1 system. Sensor-enabled smart phones could become part of standard-issue personal protective equipment for these first responders, better preparing them to assess life-and-death situations without carrying special, cumbersome equipment.

Private industry could use the technology to reduce the risk of workplace accidents, especially in more dangerous sectors, such as the chemical industry. For places that attract large gatherings of people, such as hotels, malls or stadiums, security staff could more quickly engage personnel to pro-actively organize evacuations.

Furthermore, state and federal emergency management and national security preparedness would be enhanced with real-time data on toxic events involving the public. While the benefits of Cell-All technology are numerous, so are its applications.

It is important to emphasize that alerts generated by the Cell-All network are not just raw sensor data processed and pushed out by sophisticated computers. Experienced NC4 analysts perform the critical human-in-the-loop function of identifying false positives, assessing the characteristics of the incident, and correlating it with other information. Analysts evaluate the geographical context -- where is the incident happening and is it located near a soft target or sensitive facility? Is one sensor being triggered in a private residence, or are many sensors being activated in a mall or sports stadium? Does the event correlate in proximity, subject or in any other way with one of the other 900 real-time incidents being monitored by NC4 each week (like a suspicious package or other hazmat incident)?

By evaluating this kind of information, and correlating it with other open source information, such as roadway closures from a state DOT, or wind speed and direction from the NWS, or restricted information from law enforcement and emergency response channels, NC4 transforms basic incident information into vetted, value-added and actionable intelligence that consumers in the public and private sectors can trust.

If any sizable proportion of the 300 million cell phones in the U.S. were enabled with this technology, it would also bring a powerful tool to the nation's anti-terrorism efforts, with minimal investment. The ability to crowd-source the data provided by these sensors could help identify coordinated terrorist attacks more quickly.

In 2008, Lashkar-e-Taiba coordinated 10 simultaneous shootings and bombings in Mumbai, and we are all too familiar with Al Qaeda's coordinated attacks using airplanes on 9/11. The effects of a coordinated chemical attack like the 1995 release of sarin gas in the Tokyo subway system could be mitigated by Cell-All. The early identification of the toxin combined with other sensor and GPS data could help authorities stop the right subway traffic, to disable airflow systems that disperse the toxin, and to engage EMS and hazmat crews as early as possible.

Professionals in national security, corporate security, crisis response and emergency preparedness fields know that real preparedness is both multi-dimensional and overlapping. The Cell-All program evokes both by involving the individual, first responders, private enterprise, and local, state, and federal governments. Mobile devices are a tool for change, and we now have technology to leverage the power of the masses and the cell phones they carry to improve both personal safety and public readiness.

Chris Needs oversees the NC4 Risk Center solution for tactical and strategic situational awareness.

Liquid restrictions to be lifted at Australian airports in 2013
Source: http://www.ausbt.com.au/liquid-restrictions-to-be-lifted-at-australian-airports-in-2013

Liquid, aerosol and gel restrictions for hand luggage of overseas travellers will be lifted from all Australian airports in 2013, but laptops and tablets will still need to be hauled out of your bag.

Sophisticated new security equipment being installed at international airports around

Australia and capable of detecting liquid explosives means the current 100ml restrictions -- introduced in 2006 after a plot to detonate liquid explosives on flights from the UK -- will no longer be necessary.

According to a Commonwealth Government statement issued by the Department of Infrastructure and Transport, passengers will once again be able to carry bottles of water, more sizeable cosmetics as well as wine,

spirits, perfume and other toiletries without fear of them being pulled from your luggage and tossed into a bin behind the security scanning stations.

But it's not all roses for the business travel brigade: laptops and tablets will still need to be removed from your carry-on bag and placed in a tray for individual scanning, a department spokesperson told Australian Business Traveller.

"The existing Australian arrangements for the screening of laptops and similar devices remain in place" the spokesperson said.

"We are aware of efforts by the United States

Transportation Security Administration to

enable certain laptops and similar devices to

remain in passengers' carry-on bags during screening. It is possible that at some point in the future, with appropriate equipment in place, laptops may not need to be removed for screening purposes."

The new airport scanning equipment -- comprising multi-view explosive detection x-ray machines and bottled liquid scanners -- has already been trialled at Sydney and Melbourne airport, with staff wearing distinctive purple

uniforms to highlight their presence and explain the process to passengers.

Multi-view x-ray machines can examine baggage at more than one angle, and have the ability to detect different liquids' densities. Explosives are measurably more dense than, say, water or juice.

Bottled liquid scanners have been in use on a limited basis in international airports, mainly for checking medically necessary liquids, which have been exempt from restrictions.
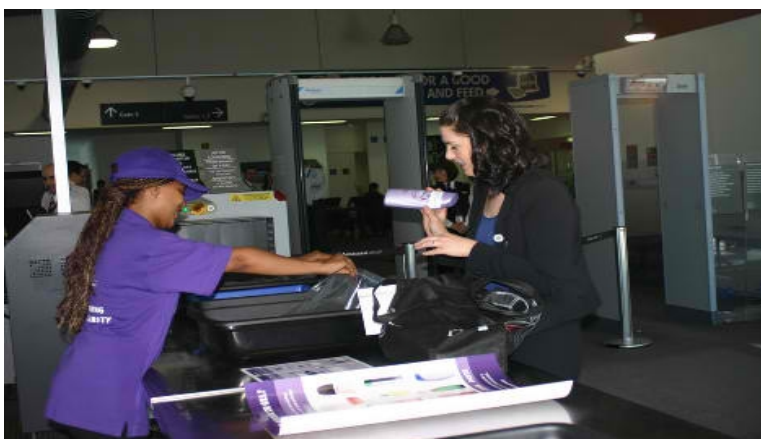
However, the new system will apply only for travellers flying out of Australia -- inbound passengers will still need to observe the 100ml limit.

The Government is hopeful of that changing, saying that trials of the new technology were conducted "in cooperation with authorities from both the US and Great Britain" and that "the Government continues to work within the international community to achieve further relaxations".

(Here's hoping those "relaxations" don't include the complimentary deep-tissue massage offered by the United States' TSA screeners...)

DNDO progressing on Helium-3 alternative

Source: http://www.homelandsecuritynewswire.com/srdetect20111121-dndo-progressing-on-helium3-alternative

DHS is one step closer in its quest to find an alternative to Helium-3, a key element used in radiation scanners that detect illegal nuclear or radiological materials.

DHS's Domestic Nuclear Detection Office (DNDO) recently announced that it had completed its final analysis on Helium-3 alternatives. Warrant Stern, the director of DNDO, said the analysis found some "promising" alternative radiation detection technologies that could eventually eliminate the need for Helium-3 based detectors.

Since 9/11 the demand for radiation detectors designed to prevent terrorists from executing an attack using a "dirty bomb" has increased dramatically, placing a strain on limited Helium-3 supplies.

The naturally-occurring element is primarily obtained from decommissioned nuclear weapons and heavy water reactors, but with the drawing down of the U.S. nuclear stockpile supply has not kept pace with demand. Helium-3 supplies have been further strained by increasing demand from other applications like medical imaging and diagnostics, cryogenics research, and oil and gas exploration.

To head off the impending Helium-3 shortage, DNDO has actively been exploring efficient, cost-effective strategies to find alternative radiation detection technology. In addition, DNDO has been working with manufacturers to develop ways to decrease the use of Helium-3 in existing detectors as well as ways to recycle the element.

According to Stern, DNDO currently has about fifteen different technologies under development that could eventually replace Helium-3.

Al-Qaeda 'lone wolf' was hours away from completing bombs for US attacks

Source: http://www.telegraph.co.uk/news/worldnews/al-qaeda/8905176/Al-Qaeda-lone-wolf-was-hours-away-from-completing-bombs-for-US-attacks.html

Jose Pimentel (photo) was seized by police (Nov, 21) after being filmed converting pipes into casings for bombs that could have killed dozens in New York and New Jersey, Mayor Michael Bloomberg claimed.

He was allegedly plotting to avenge the killing of Anwar al-Awlaki, the radical Islamist cleric, after reading an article in an al-Qaeda magazine titled "How to

make a bomb in the kitchen of your mom".

"The NYPD remains focused on preventing another terrorist attack," Mr Bloomberg told a late-night press conference. "This is just another case where our precautions paid off."

However, doubts were raised about the severity of the alleged plot, after it emerged the FBI declined to take on the case, having concluded Mr Pimentel had neither the "predisposition or the ability" to carry it out.

A 27-year-old US citizen born in the Dominican Republic, Mr Pimentel is a Muslim convert also known as Muhammad Yusuf. He has spent most of his life in New York and once allegedly considered changing his name to Osama Hussein, to honour his "heroes" Osama bin Laden and Saddam Hussein.

He lives with his mother, Carmen Sosa, who said yesterday they had drifted apart. "I don't know what's going on," she told reporters outside her home. "I didn't raise him that way. He changed."

He is alleged to have emailed Awlaki and wanted to train at his base in Yemen "before returning to New York to become a martyr", officials said.

Mr Pimintel allegedly planned to attack US soldiers returning from war zones, police cars and facilities in New York and New Jersey and US post offices.

He was under surveillance for two years and allegedly began plotting in August, but "jacked up his speed" after Awlaki's September death, Mr Kelly said.

He allegedly bought piping, Christmas lights and an alarm clock for his planned bombs from Home Depot and a 99-cent shop.

He also allegedly ran a website, which featured bomb-making instructions lifted from Inspire, al-Qaeda's English-language magazine.

Mr Bloomberg assured residents Mr Pimentel was "not part of a larger conspiracy" overseas. He "was a so-called lone wolf, motivated by his own resentment of the presence of American troops in Iraq and Afghanistan, as well as inspired by al Qaeda propaganda," he claimed.

But officials suggested yesterday that the alleged plot was in fact so minor that the FBI twice declined a request from the NYPD to get involved with the case.

Mr Pimentel was arrested on Sunday at the New York flat of a "police informant", with

"Once his bombing campaign began, Mr Pimentel said the public would know that there were mujahideen in the city to fight jihad here," claimed Ray Kelly, the New York police commissioner.

whom he had discussions over his alleged plot. He was filmed working on the alleged bombs at the flat by a surveillance camera.

According to a criminal complaint, Mr Pimentel told police that he was an hour away from completing his first bomb when they swooped. He appeared in a Manhattan court late on Sunday night, charged with possession of a bomb for terrorism and several other crimes. He was detained after being denied bail.

His lawyer, Joseph Zablocki, argued that the case against his client did not make sense. "As they admit, he has a very public online profile," said Mr Zablocki. "This is not the way you go about committing terrorist attacks."

Examining shoes for trace amounts of explosives – discreetly

Source:http://www.homelandsecuritynewswire.com/dr20111122-examining-shoes-for-trace-amounts-of-explosives-discreetly

NIST has been developing a prototype shoe sampling system that relies on aerodynamic sampling as the primary mechanism for liberating, transporting, and collecting explosive contamination.

As part of an ongoing effort with the Transportation Security Laboratory, the National Institute of Standards and Technology (NIST) has been developing a prototype shoe sampling system that relies on aerodynamic sampling as the primary mechanism for liberating, transporting, and collecting explosive contamination.

On 21st of November, NIST's Matthew Staymates presented a paper at the 64th Annual Meeting of the American Physical Society (APS) Division of Fluid Dynamics which focused on the fluid dynamics associated with the current prototype design.

An APS release reports that this design includes several air jets and air blades that are used to dislodge particles from target areas of a shoe. A large blower then draws air and liberated particles into a collection device at several hundred liters per second. Experiments that utilize optical particle counting techniques have shown that the applied shear forces from these jets are capable of liberating particles efficiently from shoe surfaces. Results from real-world contamination testing also support the effectiveness of air jet impingement in this prototype. Many examples of flow visualization will be shown.

Staymates also discussed the issues associated with air spillage, particle release efficiency, and particle transport.

— Read more in "Design and characterization of an aerodynamic shoe sampling system for screening trace explosive materials" (paper presented at the 64th Annual Meeting of the APS Division of Fluid Dynamics, Baltimore, Md., 21 November 2011)

Graphene foam detects explosives better than gas sensors

Source: http://www.homelandsecuritynewswire.com/dr20111129-graphene-foam-detects-explosives-better-than-gas-sensors

Researchers demonstrate that graphene foam can outperform leading commercial gas sensors in detecting potentially dangerous and explosive chemicals; the discovery opens the door for a new generation of gas sensors to be used by bomb squads, law enforcement officials, defense organizations, and in various industrial settings

A new study from Rensselaer Polytechnic Institute demonstrates how graphene foam can outperform leading commercial gas sensors in detecting potentially dangerous and explosive chemicals. The discovery opens the door for a new generation of gas sensors to be used by bomb squads, law enforcement officials, defense organizations, and in various industrial settings.

The new sensor successfully and repeatedly measured ammonia (NH_3) and nitrogen dioxide (NO_2) at concentrations as small as twenty parts-per-million. Made from

continuous graphene nanosheets that grow into a foam-like structure about the size of a postage stamp and thickness of felt, the sensor is flexible, rugged, and finally overcomes the shortcomings that have prevented nanostructure-based gas detectors from reaching the marketplace.

Results of the study were published today in the journal *Scientific Reports*, published by Nature Publishing Group.

"We are very excited about this new discovery, which we think could lead to new commercial gas sensors," said Rensselaer Engineering Professor Nikhil Koratkar, who co-led the study along with Professor Hui-Ming Cheng at the Shenyang National Laboratory for Materials Science at the Chinese Academy of Sciences. "So far, the sensors have shown to be significantly more sensitive at detecting ammonia and nitrogen dioxide at room temperature than the commercial gas detectors on the market today" (watch a short video of Koratkar talking about this research).
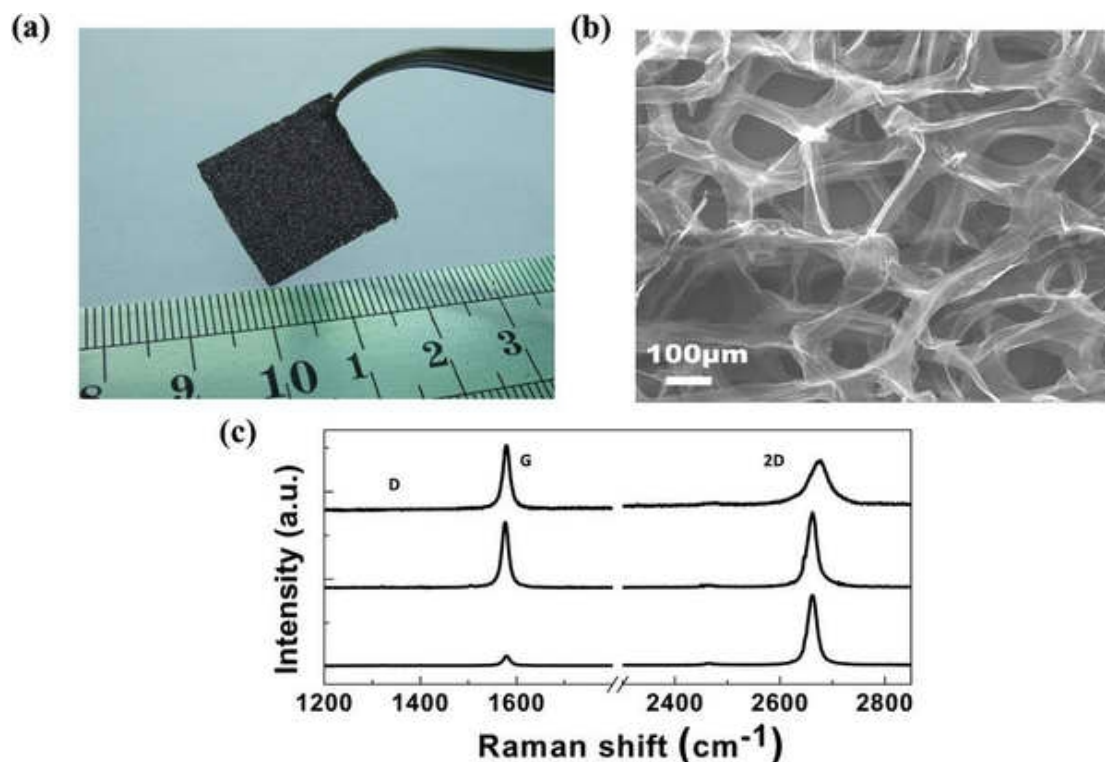
(a) Photograph and (b) scanning electron micrograph of the microporous GF structure showing a continuous network of 3D interconnected graphene sheets that comprise the walls of the foam-like structure. The robust and flexible GF strips can be easily handled and manipulated. Electrical contacts to the macro-scale GF can be established without the need for lithography. (c) Typical Raman spectra obtained at various locations on the GF indicating that the foam walls are comprised of mono to few-layer graphene.

Rensselaer Polytechnic Institute release reports that over the past decade researchers have shown that individual nanostructures are extremely sensitive to chemicals and different gases. To build and operate a device using an individual nanostructure for gas detection, however, has proven to be far too complex, expensive, and unreliable to be commercially viable, Koratkar said. Such an endeavor would involve creating and manipulating the position of the individual nanostructure, locating it using microscopy, using lithography to apply gold contacts, followed by other slow, costly steps. Embedded within a handheld device, such a single nanostructure can be easily damaged and rendered inoperable. Additionally, it can be challenging to "clean" the detected gas from the single nanostructure.

The new postage stamp-sized structure developed by Koratkar has all of the same attractive properties as an individual nanostructure, but is much easier to work with because of its large, macroscale size. Koratkar's collaborators at the Chinese Academy of Sciences grew graphene on a structure of nickel foam. After removing the nickel foam, what's left is a large, free-standing network of foam-like graphene. Essentially a single layer of the graphite found commonly in our pencils or the charcoal we burn on our barbeques, graphene is an atom-thick sheet of

carbon atoms arranged like a nanoscale chicken-wire fence. The walls of the foam-like graphene sensor are comprised of continuous graphene sheets without any physical breaks or interfaces between the sheets.

The release notes that Koartkar and his students developed the idea to use this graphene foam structure as a gas detector. As a result of exposing the graphene foam to air contaminated with trace amounts of ammonia or nitrogen dioxide, the researchers found that the gas particles stuck, or adsorbed, to the foam's surface. This change in surface chemistry has a distinct impact upon the electrical resistance of the graphene. Measuring this change in resistance is the mechanism by which the sensor can detect different gases.

Additionally, the graphene foam gas detector is very convenient to clean. By applying a ~100 milliampere current through the graphene structure, Koratkar's team was able to heat the graphene foam enough to unattach, or desorb, all of the adsorbed gas particles. This cleaning mechanism has no impact on the graphene foam's ability to detect gases, which means the detection process is fully reversible and a device based on this new technology would be low power — no need for external heaters to clean the foam — and reusable.

(a)

(b)

(c)
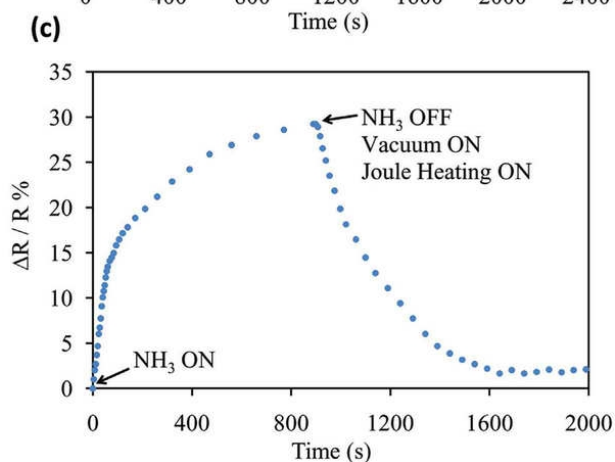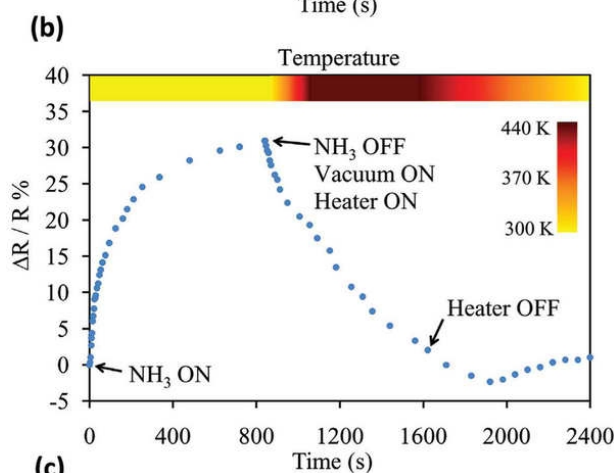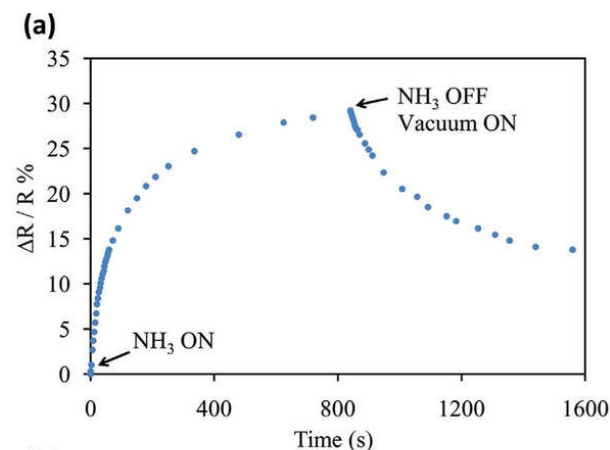
Change in the normalized resistance of the GF as a function of time during adsorption of ~1000 ppm of NH_3 and desorption using (a) room temperature degassing and (b) high temperature degassing. The color bar at the top of the graph in (b) shows the change in temperature as a function of time. (c) Corresponding adsorption and desorption response obtained by using Joule heating of the sample during the desorption step. The control current supplied to the GF to heat it to ~400 K is ~125 mA.

Koratkar chose ammonia as a test gas to demonstrate the proof-of-concept for this new detector. Ammonium nitrate is present in many explosives and is known to gradually decompose and release trace amounts of ammonia. As a result, ammonia detectors are often used to test for the presence of an explosive. A toxic gas, ammonia also is used in a variety of industrial and medical processes, for which detectors are necessary to monitor for leaks.

Results of the study show the new graphene foam structure detected ammonia at 1,000 parts-per-million in 5 to 10 minutes at room temperature and atmospheric pressure. The accompanying change in the graphene's electrical resistance was about 30 percent. This compared favorably to commercially available conducting polymer sensors, which undergo a 30 percent resistance change in 5 to 10 minutes when exposed to 10,000 parts-per-million of ammonia. In the same time frame and with the same change in resistance, the graphene foam detector was ten times as

sensitive. The graphene foam detector's sensitivity is effective down to 20 parts-per-million, much lower than the commercially available devices. Additionally, many of the commercially available devices require high power consumption since they provide adequate sensitivity only at high temperatures, whereas the graphene foam detector operates at room temperature.

Koratkar's team used nitrogen dioxide as the second test gas. Different explosives including nitrocellulose gradually degrade, and are known to produce nitrogen dioxide gas as a byproduct. As a result, nitrogen dioxide also is used as a marker when testing for explosives. Additionally, nitrogen dioxide is a common pollutant found in combustion and auto emissions. Many different environmental monitoring systems feature real-time nitrogen dioxide detection.

The new graphene foam sensor detected nitrogen dioxide at 100 parts-per-million by a 10 percent resistance change in 5 to 10 minutes at room temperature and atmospheric pressure. It showed to be ten times more sensitive than commercial conducting polymer sensors, which typically detect nitrogen dioxide at 1,000 part-per-million in the same time and with the same resistance chance at room temperature. Other nitrogen dioxide detectors available today require high power consumption and high temperatures to provide adequate sensitivity. The graphene foam sensor can detect nitrogen dioxide down to twenty parts-per-million at room temperature.
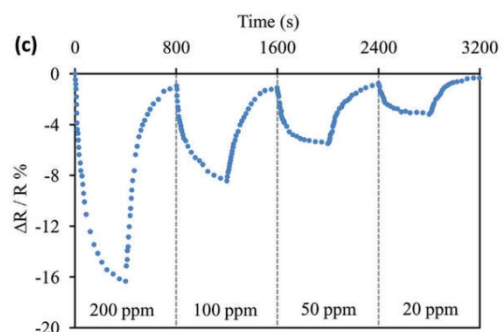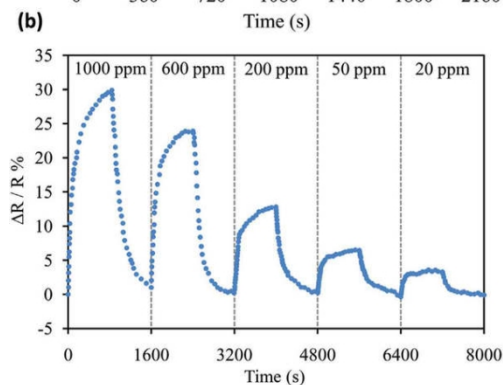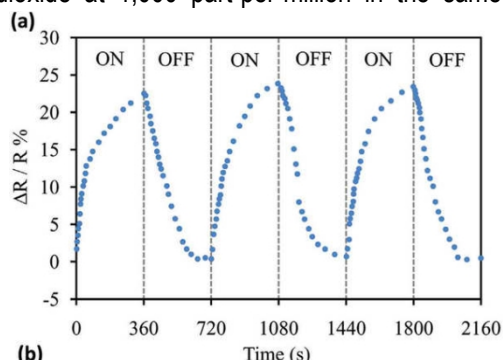
"We see this as the first practical nanostructure-based gas detector that's viable for commercialization," said Koratkar, a professor in the Department of Mechanical, Aerospace, and Nuclear Engineering at Rensselaer. "Our results show the graphene foam is able to detect ammonia and nitrogen dioxide at a concentration that is an order of magnitude lower than commercial gas detectors on the market today."

(a) Normalized change in electrical resistance of the GF as a function of time for detection of ~1000 ppm of NH_3 in three cycles. With Joule heating during the desorption step, the GF sensor exhibits a fully reversible response. (b) Normalized resistance change vs. time for different concentrations of NH_3 in air. The adsorption step is performed at room temperature, while Joule heating to ~400 K is used during desorption. (c) Corresponding normalized resistance change vs. time for different concentrations of NO_2 in air.

The graphene foam can be engineered to detect many different gases beyond ammonia and nitrogen dioxide, he said.

The release also notes that studies have shown the electrical conductivity of an individual nanotube, nanowire, or graphene sheet is acutely sensitive to gas adsorbtion. The small size of individual nanostructures, however, made it costly and challenging to develop into a device, plus the structures are delicate and often don't yield consistent results.

The new graphene foam gas sensor overcomes these challenges. It is easy to handle and manipulate because of its large, macroscale size. The sensor also is flexible, rugged, and robust enough to handle wear and tear inside of a device. Plus it is fully reversible, and the results it provides are consistent and repeatable. Most important, the graphene foam is highly sensitive, thanks to its 3-D, porous structure that allows gases to easily adsorb to its huge surface area. Despite its large size, the graphene foam structure essentially functions as a single nanostructure. There are no breaks in the graphene network, which means there are no interfaces to overcome, and

electrons flow freely with little resistance. This adds to the foam's sensitivity to gases.

"In a sense we have overcome the Achilles' heel of nanotechnology for chemical sensing," Koratkar said. "A single anostructure works great, but doesn't mean much when applied in a real device in the real world. When you try to scale it up to macroscale proportions, the interfaces defeats what you're trying to accomplish, as the nanostructure's properties are dominated by interfaces. Now we're able to scale up graphene in a way that the interfaces are not present. This allows us to take advantage of the intrinsic properties of the nanostructure, yet work with a macroscopic structure that gives us repeatability, reliability, and robustness, but shows similar sensitivity to gas adsorbtion as a single nanostructure."

This research was supported in part by the Advanced Energy Consortium (AEC), the National Science Foundation of China, and the Chinese Academy of Sciences.

— *Read more in Fazel Yavari et al., "High Sensitivity Gas Detection Using a Macroscopic Three-Dimensional Graphene Foam Network," Scientific Reports 1, article no. 166 (23 November 2011)*

Improvised Explosive Devices

Trends and Issues: October 2011 in Review

NATO"s Defence against Terrorism Centre of Excellence (DaT-CoE) reported 391 people were killed and 858 others injured globally from 309 IED, vehicle-borne IED, or suicide bomber attacks during October 2011. The casualties from these IED attacks make up 46.3% of the victims from all terrorist incidents, yet IED attacks[1] comprise 37.9% of global terrorism events reported during the month.

The fact that IEDs caused a proportionately greater share of casualties[2] than other methods[3] of terrorist attacks in October is not unusual. A review of data from the DaT-CoE monthly terrorism reports over the past year (figure 1) shows that while IED attacks comprise an average of 38.4% of reported global terrorism events, they are responsible for over 53% of the casualties from all terrorism events.

Figure 1

IED Attacks and Casualties as Percentage of all Terrorism Events
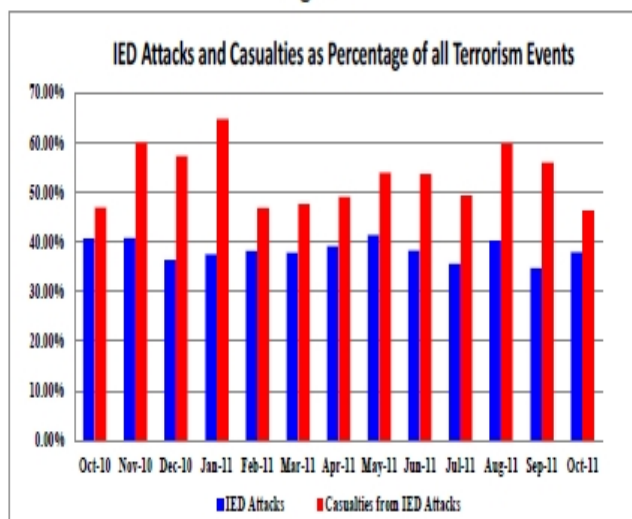
Source: Compiled from data extracted from DaT-CoE Oct 2010 – Oct 2011 monthly reports

[1] Include IED explosions, vehicle-borne IED attacks, and suicide attacks
[2] Casualties are defined as people killed or wounded
[3] The DaT-CoE include IED, armed attack, clash, indirect fire, execution, vehicle-borne IED, abduction, suicide attack, raid, arson, cyber and hoax among its categories of terrorism incidents

Despite the threat posed by traditional roadside bombs, the greater dangers are high-profile suicide and vehicle-borne IED (VBIED) attacks. A closer look at the data (figure 2)

indicates that vehicle-borne and suicide IED attacks constitute 17.4% of total IED events, but are responsible for nearly 45% of IED casualties.

Figure 2

	Total # IED attacks	Total # casualties from IED attacks	IED explosions	Casualties from IED explosions	# suicide attacks	# casualties from suicide attacks	# VBIED attacks	# casualties from VBIED attacks
Oct-10	406	1484	350	1096	18	260	38	128
Nov-10	405	2157	326	1247	25	582	54	328
Dec-10	338	2032	269	957	36	843	33	232
Jan-11	375	2354	318	975	23	886	34	493
Feb-11	375	1694	319	612	32	753	24	329
Mar-11	400	1782	347	969	22	531	31	282
Apr-11	442	2064	366	1429	36	424	40	211
May-11	471	2269	386	1200	31	545	54	524
Jun-11	447	2134	372	1290	32	521	43	323
Jul-11	439	1808	364	1102	28	262	47	444
Aug-11	424	2436	341	1273	37	735	46	428
Sep-11	319	2094	251	1025	33	651	35	418
Oct-11	309	1249	252	817	22	268	35	164

Suicide Attacks and Casualties as Percentage of All IED Attacks

Average 7.4% of all IED attacks
Average 28% of total IED casualties

■ Suicide Attacks as % of all IED atks   ■ Suicide Attacks casualties as % of total IED casualties

Vehicle-borne IED Attacks and Casualties as Percentage of All IED Attacks

Average 10% of all IED attacks
Average 16.6% of total IED casualties

■ VBIED attacks as % of all IED atks   ■ VBIED casualties as % of total IED casualties

Source: Data and charts compiled from DaT-CoE Oct 2010 – Oct 2011 monthly reports

Uni-Direction technology used in Karachi blasts
Source: http://www.dailytimes.com.pk/default.asp?page=2011\12\12\story_12-12-2011_pg7_1

The law enforcement agencies (LEAs) have expressed concern over the use of latest technology (Uni-Direction) in all four blasts

although all four blasts not create disastrous impact, yet the technology was used in these blasts to demonstrate the power. They said the

during Muharram. According to sources in investigation department, the Uni-Direction technology, which was brought from Afghanistan by some outlawed, could target the object at specific direction. They said

investigators were still unable to identify the targets of the militants through these blasts but they termed that technique as massacre. The sources said the investigators

were presently busy to identify the precautionary measures to avert the use of this technology in any other terrorist activity. They said the relevant department had also written a letter to Crisis Management Cell calling for help to overcome the issue. The sources said the group behind all those blasts had so far not identified, therefore, the LEAs were going to conduct search operation at massive scale, especially at Afghan settlements to grab the real culprits. For the purpose, the relevant authorities have given go-ahead signal to dig out the guilty party. They said the wave of that sort of blasts had engulfed the city on 9th Muharram when Lines Area came under target. This incident was initially declared as gas cylinder blast. This blast occurred soon after the procession passed the site.

The second was planted at a middle of the Kalapul within Defence police limits and exploded on Tuesday morning at around 11:00am. Both bomb exploded with big sounds, which were heard at a distance of about 4-6 kilometers. At least four passersby, Manzoor Hussain, Rasheed, Iftikhar and Kaneez Begum, were wounded when an explosion took place at Kalapul but the police officials concerned said that only one man was injured, who was shifted to the Jinnah Postgraduate Medical Centre for treatment.

The blast left a crater in the middle of the bridge and the explosion also partially damaged the bridge as safety wall alongside the bridge had collapsed. Similarly, in third blast, three Rangers personnel were targeted while two other were injured at Safora Goth on Dec 9. This wave of blasts is still unstoppable as fourth blast of this kind occurred near university, claiming a life and injuring three persons. Although there is no doubt that the LEAs are head-to-head to avert such happening in future, the action should be taken at earliest so as to save Karachi from another massacre, they maintained.

Cyber News

Second Cyber Hezbollah conference held in Tehran

Source: http://www.terrorism-info.org.il/malam_multimedia/English/eng_n/html/iran_e133.htm

Last weekend the second Cyber Hezbollah conference was held in Tehran. Cyber Hezbollah is an organization whose establishment was first reported several weeks ago. The conference was held on the occasion of the Holy Defense Week, marking the beginning of the Iran-Iraq War (September 1980), and was titled "Clicks of Resistance". Fars News Agency reported that the aim of the conference was to show appreciation for jihad and resistance activists operating in cyberspace as well as bloggers whose blogs are dedicated to jihad and sacrifice, and who attract considerable interest.

During the conference, Cyber Hezbollah member and spokesman Soheil Karimi read a statement emphasizing the need to spread the culture of sacrifice also in cyberspace (www.hizbullahcyber.com, September 22).

From www.hizbullahcyber.com

The main lecture of the conference was given by Dr. Hassan Abbasi, head of the Center for

Doctrinal Analysis for Security across Frontiers, affiliated with the Revolutionary Guards. Abbasi is considered one of the major theoreticians of the radical faction in the conservative camp and the Revolutionary Guards.

Abbasi warned about the close monitoring of Iranians' web traffic by Western intelligence services, particularly the American National Security Agency (NSA). Addressing students who use the internet, he said that even though they currently do not possess important information that can be of interest to foreign

intelligence services, they must exercise caution on the web, because someday they will have important and sensitive information that can be exposed by those who follow their online activity. He noted that the NSA is the organization that actually controls the world wide web.

Abbasi said that the major concern is that a considerable part of the information on young Iranian men and women and their activity is currently online. While this doesn't mean that the internet is to be avoided, one should surf the web wisely and remember that it is monitored by Iran's enemies, who wage a war against Muslim society and the religion of Islam. Iran's online presence, Abbasi said, is like an operation in enemy territory, and the principles of asymmetrical warfare should also be applied in cyberspace—that is, existing online tools should be used against the enemy. Abbasi added that the United States intends to carry out a massive September 11-like cyber attack on Iran. He warned that the United States is looking for excuses to instigate wars across the globe to rescue its declining economy. Accordingly, Cyber Hezbollah activists must act cautiously to foil the plots hatched by the enemies and not give them any pretext to take action against Iran. They must also act in the cultural sphere against American websites and spread the message of the Muslim world in cyberspace (Fars, September 23).

Ya Lesarat, a weekly affiliated with the radical conservative organization Ansar Hezbollah, reported the launch of Cyber Hezbollah in early September. According to the report, the organization was established in June 2011 as a spontaneous collaboration of pro-regime activists who worked against regime opponents in cyberspace during the 2009 riots. The organization held its first conference in August 2011. A memorandum released by Cyber Hezbollah after its establishment specified its goals and objectives, which include coordinating between pro-regime activists operating in

cyberspace, offering them courses and training, holding meetings aimed to acquaint the activists with cyber warfare tactics, and mobilizing the activists for various online activities (Ya Lesarat, September 1).

Meanwhile, Passive Resistance Organization chief Gholam-Reza Jalali discussed the efforts made by his organization to deal with cyber threats. Speaking at a press conference for Holy Defense Week, Jalali announced that cyberspace is one of the key focus areas of the Passive Resistance Organization in dealing with enemy threats.

Jalali specified the actions taken this past year to improve cyber preparation, including the establishment of a Cyber Defense Headquarters under the Armed Forces General Staff, which works together with the intelligence

and telecommunications ministries and the National Security Supreme Council, and the launch of an experimental cyber defense study program in Tehran's Imam Hossein University. In addition, he said that 500 cyber defense drills are expected to take place this year to identify and correct weak spots in the country's executive systems (IRNA, September 26).

Iran's English-language Press TV network recently reported that the first national cyber defense conference is scheduled to take place in Iran on January 25-26, 2012. Sa'id Ghazi Maghrebi, the scientific secretary of the conference, reported that the conference will provide a platform for cyber experts to present articles and give lectures on cyber defense (Press TV, September 15).

German police uses backdoor Trojan to monitor Skype calls

Source: http://www.zdnetasia.com/hackers-say-german-officials-used-backdoor-trojan-62302449.htm

A backdoor Trojan capable of monitoring online activity and recording Skype calls has been detected — and is allegedly being used by the German police force.

ZDnet reports that according to research by the Chaos Computer Club (CCC), the malware can siphon away intimate data, and also offers a remote control or backdoor functionality for uploading and executing arbitrary programs. It said functionality in the
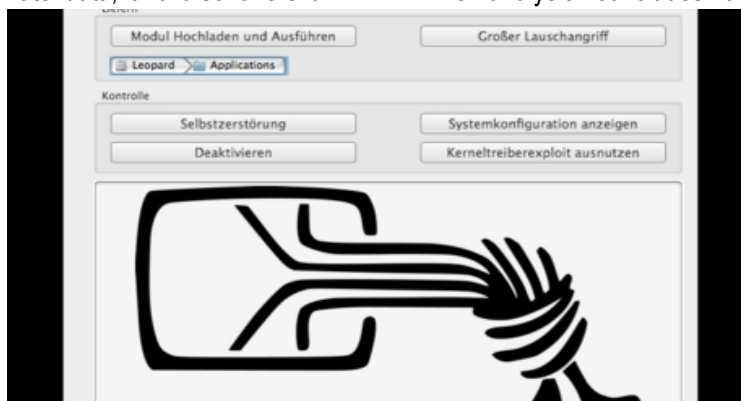
"Bundestrojaner light" ("federal Trojan"), concealed as "Quellen-TKÜ," goes much further than to just observe and intercept internet based telecommunication, and thus violates the terms set by the constitutional court.

German courts have permitted police to use Bundestrojaner to record Skype conversations if there is legal permission for a wiretap.

The report said: "The Trojan can, for example, receive uploads of arbitrary programs from the internet and execute them remotely. This means an upgrade path from Quellen-TKÜ to the full Bundestrojaner's functionality is built in right from the start.

"The analysis concludes that the Trojan's developers never even tried to put in technical safeguards in to make sure the malware can exclusively be used for wiretapping internet telephony, as set forth by the constitution court. On the contrary, the design included functionality to clandestinely add more components over the network right from the start, making it a bridge-head to further infiltrate the computer."

Computer Virus Hits U.S. Drone Fleet

Source: http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet/

A computer virus has infected the cockpits of America's Predator and Reaper drones, logging pilots' every keystroke as they remotely fly missions over Afghanistan and other warzones.

The virus, first detected nearly two weeks ago by the military's Host-Based Security System, has not prevented pilots at Creech Air Force Base in Nevada from flying their missions overseas. Nor have there been any confirmed incidents of classified information being lost or sent to an outside source. But the virus has resisted multiple efforts to remove it from Creech's computers, network security specialists say. And the infection underscores the ongoing security risks in what has become

the U.S. military's most important weapons system.

"We keep wiping it off, and it keeps coming back," says a source familiar with the network infection, one of three that told Danger Room about the virus. "We think it's benign. But we just don't know."

Military network security specialists aren't sure whether the virus and its so-called "keylogger" payload were introduced intentionally or by accident; it may be a common piece of malware that just happened to make its way into these sensitive networks. The specialists don't know exactly how far the virus has spread. But they're sure that the infection has hit both classified and unclassified machines at Creech. That raises the possibility, at least, that

secret data may have been captured by the keylogger, and then transmitted over the public internet to someone outside the military chain of command.

Drones have become America's tool of choice in both its conventional and shadow wars, allowing U.S. forces to attack targets and spy on its foes without risking American lives. Since President Obama assumed office, a fleet of approximately 30 CIA-directed drones have hit targets in Pakistan more than 230 times; all told, these drones have killed more than 2,000 suspected militants and civilians, according to the Washington Post. More than 150 additional Predator and Reaper drones, under U.S. Air Force control, watch over the fighting in Afghanistan and Iraq. American military drones struck 92 times in Libya between mid-April and late August. And late last month, an American drone killed top terrorist Anwar al-Awlaki — part of an escalating unmanned air assault in the Horn of Africa and southern Arabian Peninsula.

Photo courtesy of Bryan William Jones

But despite their widespread use, the drone systems are known to have security flaws. Many Reapers and Predators don't encrypt the video they transmit to American troops on the ground. In the summer of 2009, U.S. forces discovered "days and days and hours and hours" of the drone footage on the laptops of Iraqi insurgents. A $26 piece of software allowed the militants to capture the video.

The lion's share of U.S. drone missions are flown by Air Force pilots stationed at Creech, a tiny outpost in the barren Nevada desert, 20 miles north of a state prison and adjacent to a one-story casino. In a nondescript building, down a largely unmarked hallway, is a series of rooms, each with a rack of servers and a "ground

control station," or GCS. There, a drone pilot and a sensor operator sit in their flight suits in front of a series of screens. In the pilot's hand is the joystick, guiding the drone as it soars above Afghanistan, Iraq, or some other battlefield.

Some of the GCSs are classified secret, and used for conventional warzone surveillance duty. The GCSs handling more exotic operations are top secret. None of the remote cockpits are supposed to be connected to the public internet. Which means they are supposed to be largely immune to viruses and other network security threats.

But time and time again, the so-called "air gaps" between classified and public networks have been bridged, largely through the use of discs and removable drives. In late 2008, for example, the drives helped introduce the agent.btz worm to hundreds of thousands of Defense Department computers. The Pentagon is still disinfecting machines, three years later.

Use of the drives is now severely restricted throughout the military. But the base at Creech was one of the exceptions, until the virus hit. Predator and Reaper crews use removable hard drives to load map updates and transport mission videos from one computer to another. The virus is believed to have spread through these removable drives. Drone units at other Air Force bases worldwide have now been ordered to stop their use.

In the meantime, technicians at Creech are trying to get the virus off the GCS machines. It has not been easy. At first, they followed removal instructions posted on the website of the Kaspersky security firm. "But the virus kept coming back," a source familiar with the infection says. Eventually, the technicians had to use a software tool called BCWipe to completely erase the GCS' internal hard drives. "That meant rebuilding them from scratch" — a time-consuming effort.

The Air Force declined to comment directly on the virus. "We generally do not discuss specific vulnerabilities, threats, or responses to our computer networks, since that helps people looking to exploit or attack our systems to refine their approach," says Lt. Col. Tadd Sholtis, a spokesman for Air Combat Command, which oversees the drones and all other Air Force tactical aircraft. "We invest a lot in protecting and monitoring our systems to counter threats and ensure security, which includes a comprehensive response to viruses, worms, and other malware we discover."

However, insiders say that senior officers at Creech are being briefed daily on the virus. "It's getting a lot of attention," the source says. "But no one's panicking. Yet."

Midair Collision Between a C-130 and a UAV

Is it virus related?

Source: http://defensetech.org/2011/08/17/midair-collision-between-a-c-130-and-a-uav/

Well, it finally happened. Something some pilots operating in Iraq and Afghanistan have told me they worry about more than enemy surface-to-air fire; a midair collision with a UAV. A small RQ-7 Shadow UAV apparently collided with what looks like it might be an Air Force Special Operations Command MC-130 in the skies over Afghanistan. The collision apparently ruptured the wing fuel tank and may have done damage to the spar and wing box. Still, this could have been much worse. Good

job to the pilots for bringing the Herk home safely.

It will be interesting to see how this changes protocols for operating UAVs in congested airspace. Maybe this was a fluke incident that no amount of UAV sense and avoid technology could have stopped or maybe the collision is a prime example of why this technology must be implemented ASAP.

New report highlights Zeus Trojan's enhancement

Source: http://www.homelandsecuritynewswire.com/new-report-highlights-zeus-trojans-enhancement

New report highlights enhancements of the notorious Zeus Trojan; the enhancements help Zeus undermine tacking and detection aimed at thwarting Zeus

TrustDefender Labs, the research arm of online security and Web fraud detection company TrustDefender, – has released a new in-depth report covering recent variants of the world's most successful Trojan that focuses solely on making it harder to be tracked by the good guys.

The Zeus Trojan is one of the most successful Trojans of our times, which can mainly be attributed to the innovation, flexibility, separation of core Trojan and the Man-In-The-Browser configuration (webinjects) plus its stealthy operation that enables the creators to easily distribute the 'Zeus Trojan as a service' (SaaS) to many, many fraudsters.

TrustDefender notes that when the source code of the Zeus Trojan was leaked to the public in April this year, it was clear that it would have some serious implication for the security industry. Within a matter of weeks, three new variants of the Zeus Trojan have been found in the wild based on this leaked source code. All new variants have implemented improved antivirus evasion capabilities and the ability to make sure security researchers and automated security tools cannot easily compile a list of targeted brands (such as financial institutions, payment processors, government agencies or any online retailer).

Andreas Baumhof, CEO of TrustDefender comments that "Currently there are dedicated services offerings available that constantly decrypt known Zeus configuration files to determine which brands are affected and how they are affected. These services try to give financial institutions an early warning that they are being targeted. The disturbing fact is that with the proliferation of many new and different variants of the Zeus Trojan plus new innovative methods of encrypting the configuration file, this method of decryption cannot be done automatically anymore — thus giving the criminals a head start and more time to perpetrate the crime."

Baumhof proceeds: "We need to change the paradigm from 'reactive to proactive'. We cannot rely on the fact that we protect against just the things we know; we need to change our thinking to protect the good things we have. The TrustDefender Intelligence Suite is built exactly on this paradigm. For example our clientless Man-In-The-Browser protection in TDzero works by intelligently fingerprinting the website, whereby we know how the genuine website really looks like versus the site the customer or end user is looking at. We don't need to know a configuration file to protect a brand. This is true protection that is instant, proactive and without delay."

The recent variants show that the creators of the various malware are constantly improving their work and it is only going to be a question of time before current security countermeasures simply don't work anymore.

Stuxnet Clone 'Duqu' Possibly Preparing Power Plant Attacks
By Matt Liebowitz
Source:http://www.foxnews.com/scitech/2011/10/18/stuxnet-clone-found-possibly-preparing-power-plant-attacks/#ixzz1bFlcsjws

Security researchers have detected a new Trojan, scarily similar to the infamous Stuxnet worm, which could disrupt computers controlling power plants, oil refineries and other critical infrastructure networks.

The Trojan, dubbed "Duqu" by the security firm Symantec, appears, based on its code, to have been written by the same authors as the Stuxnet worm, which last July was used to cripple an Iranian nuclear-fuel processing plant. "Stuxnet source code is not out there," wrote F-Secure cybersecurity expert Mikko Hyppönen on his firm's blog. "Only the original authors have it. So, this new backdoor was created by the same party that created Stuxnet."

The original Stuxnet was specifically designed to compromise an industrial control system by manipulating the supervisory control and data acquisition (SCADA) software on which these facilities rely on for automation. Duqu may have its sights set on the same target, but it approaches from a different angle.

"Duqu shares a great deal of code with Stuxnet; however, the payload is completely different," researchers for the security firm Symantec wrote on its Security Response blog.

Iranian technicians work at the Bushehr nuclear power plant, outside the southern city of Bushehr, Iran.
(AP Photo/ IIPA, Ebrahim Norouzi)

Instead of directly targeting the SCADA system, Duqu gathers "intelligence data and assets from entities, such as industrial control system manufacturers, in order to more easily conduct a future attack against another third party. The attackers are looking for information such as design documents that could help them mount a future attack on an industrial control facility."

"Duqu is essentially the precursor to a future Stuxnet-like attack," the researchers added.

Symantec said whoever is behind Duqu rigged the Trojan to install another information-stealing program on targeted computers that could record users' keystrokes and system information and transmit them, and other harvested data, to a command-and-control (C&C) server. The C&C server is still operational, Symantec said.

McAfee, another prominent security firm, has a different analysis of Duqu. Two of its researchers wrote on McAfee's blog that Duqu is actually highly sophisticated spyware designed to steal digital certificates, which are encrypted "keys" that websites use to verify their identities. (Stolen certificates, apparently purloined by a lone Iranian hacker, have become a big issue recently.)

Neither Symantec, McAfee nor F-Secure would speculate about who's behind Duqu, but the onventional wisdom on Stuxnet is that it was created by the intelligence services of the U.S. and Israel to knock out a uranium-refinement plant in Iran.

This new entry into the Stuxnet family comes just after the Department of Homeland Security (DHS) issued a bulletin warning that the notorious hacking group Anonymous may soon start looking to bring down or disrupt industrial control facilities. Posted yesterday (Oct. 18) to publicintelligence.net, the unclassified bulletin assesses Anonymous' ability to compromise SCADA systems that run power plants, chemical plants, oil refineries and other industrial facilities.

Government officials did not blame Anonymous for any such hacks, and the bulletin says that based on available information, Anonymous has "a limited ability to conduct attacks" on industrial control systems.

The group's agenda could change, however. The DHS document cites several recent actions, including Anonymous' cyberattack on the websites and servers of biotech seed company Monsanto, as proof that Anonymous could "develop capabilities to gain access and trespass on control system networks very

quickly."

The 10 Worst Computer Viruses in History

Source: http://www.securitynewsdaily.com/10-worst-computer-viruses-history-0966/

Stoned

Before there was the World Wide Web, the first computer viruses spread via floppy disks. One of the earliest was the 1987 boot-sector virus Stoned, which taunted infected users with the on-screen message, "Your computer is now stoned."

Several variants of the virus were written by copycats, ushering in the practice of hackers updating existing virus code to create more infections.

Jerusalem

Toward the end of 1987, the Jerusalem virus began spreading. The virus was much more destructive than the Stoned virus, infecting both .exe and .com files (different kinds of applications).

Because it launched only on every Friday the 13th, Jerusalem's spread was more slow-moving than Stoned's, but Jerusalem destroyed tens of thousands of users' programs along the way.

The Morris Worm

November 1988 saw what is widely regarded as the first worm — a self-contained program that spreads without human intervention — to infect public networks. At the time, it was estimated to have infected about 10 percent of all computers connected to the nascent Internet.

Its creator, Cornell University graduate student Robert Tappan Morris, whose father was a famous computer scientist, became the first person convicted under the Computer Fraud and Abuse Act.

The Concept Virus

The '90s saw the development of a raft of new bugs, including so-called polymorphic viruses that could change their appearance with each new infection, making it difficult for anti-virus software to detect their presence.

In 1995, the Concept virus broke new ground by being the first to infect Microsoft Word documents. Unaware users sharing documents via email helped make it one of the fastest spreading viruses of its time.

Melissa

Before the decade was out, one of the worst viruses of all-time appeared. Reputed to be named for a Florida stripper, Melissa showed up in mid-1999 and was one of the first viruses designed to spread from computer to computer without relying on action on the user's part.

For every PC it infected via email, it attempted to infect another 50 using the victim's Microsoft Outlook address book. The subsequent volume of Internet traffic forced companies such as Intel and Microsoft to temporarily shut down their own mail servers.

The Love Bug

Social engineering — tricking a person to open a file or reveal information — came into its own in May 2000 with the ILOVEYOU virus.

Like Melissa, it also used email and appeared to come from someone known to the recipient. But in reality, the attached script deleted multimedia and personal files, changed the Internet Explorer start page and unleashed a torrent of junk mail.

The Love Bug is still considered to be one of the most destructive viruses ever. It infected more than 50 million computers in just nine days, and caused several military sites to shut down their networks until the virus could be purged.

The Anna Kournikova Virus

You didn't have to be a tennis fan in February 2001 to fall victim to this virus. Inaugurating what has since become a commonplace tactic, the Kournikova virus enticed email recipients to open an attached picture of the statuesque tennis star.

There was in fact no image behind the message — just an obsessed young programmer from the Netherlands, who

quickly turned himself in to authorities.

Code Red

In 2001, anti-virus researchers were frustrated by a new worm dubbed Code Red, after the hyper-caffeinated flavor of Mountain Dew soda its finders were drinking when they discovered it.

Code Red attacked Microsoft servers and during the summer of 2001 infected more than 350,000 computers. It proved tricky to eradicate because it was able to re-infect cleaned systems, causing overload and denial-of-service problems for sites around the world.

Nimda

Using a tripartite attack, Nimda ("admin" spelled backwards) was not only a virus (an alteration to a benign program or file) but also a worm and a Trojan horse (a standalone program that pretends to be benign).

Nimda's variety of attack methods enabled it to spread faster than any previous malware, spanning the globe in less than an hour. (It appeared on Sept. 18, 2001, leading to media speculation of an Al Qaeda connection.) Although estimates vary, it is reported to have caused billions of dollars worth of damage.

Netsky and Sasser

By 2004, virus writers were rapidly exploiting and building on each other's code, so much so that they were beginning to interfere with one another. So the Netsky and Sasser worms took the extraordinary step of attempting to clean out other worms on a victim's PC before installing themselves. Sasser drew attention because it knocked out the satellite communications system for the French news agency Agence France-Presse and caused problems with Delta Air Lines systems, causing some flight cancellations. Eventually, both viruses were traced to a teenage computer science student in Germany.

New Stuxnet-like virus hits Europe
Source: http://www.homelandsecuritynewswire.com/new-stuxnet-virus-hits-europe

The dreaded Stuxnet worm, which was the first instance of a computer virus creating physical damage, may have spawned a dangerous new piece of malware.

Researchers at Symantec believe they have discovered a new computer virus that uses many of the same techniques in European computers.

According to Liam O Murchu, a Symantec researcher who has extensively analyzed Stuxnet, parts of the new code, which has been named "Duqu," are nearly identical to Stuxnet and appears to have been written by the same authors behind it or programmers with direct access to Stuxnet's source code.

Like Stuxnet, Duqu disguises itself as legitimate code to avoid detection. In addition the malware hides itself in a computer's memory rather than on the hard drive to avoid being detected by anti-virus software, a sophisticated technique beyond other types of malware.

Duqu does not self-replicate to infect other computers and does not contain a destructive payload to damage hardware like Stuxnet, instead researchers believe it is a precursor to a Stuxnet-like attack, gathering intelligence on industrial control systems for a targeted attack later.
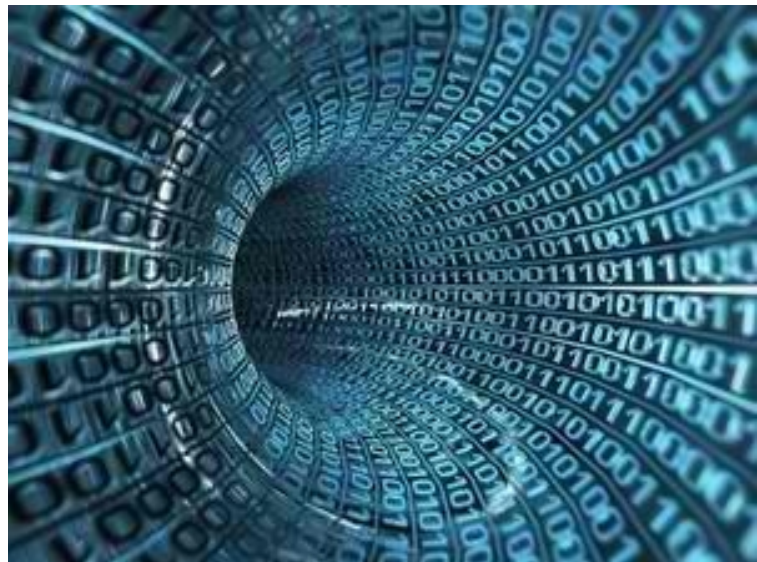
"When we talked about Stuxnet before, we expected there was another component of Stuxnet we didn't see that was gathering information about how a plant was laid out," O Murchu said.

"But we had never seen a component like that [in Stuxnet]. This may be that component."

Based on the dates some of the code was compiled, researchers believe Duqu may have been in place as early as December 2010, about five months after the discovery of Stuxnet.

"The real surprising thing for us is that these guys are still operating," O Murchu said. "We thought these guys would be gone after all the publicity around Stuxnet. That's clearly not the case. They've clearly been operating over the last year. It's quite likely that the information they are gathering is going to be used for a new attack. We were just utterly shocked when we found this."

Duqu is designed to operate for thirty-six days before automatically removing itself from an infected system.

So far the majority of Duqu infections have not been grouped in any geographical region, whereas Stuxnet was primarily found in Iran. O Murchu believes that a pattern could emerge if new infections are discovered.

As of now, researchers still do not know how Duqu has been infecting systems.

"There's an installer component [to Duqu] we haven't seen," O Murchu said. "We don't know if the installer is self-replicating. That's a piece of the jigsaw that we're missing right now."

With Stuxnet, which is largely believed to have been created by the U.S. and Israeli military, computers were infected with a USB stick loaded with the virus that exploited a zero-day vulnerability that allowed it to spread across systems.

Stuxnet-clones easily created

Source: http://www.homelandsecuritynewswire.com/stuxnet-clones-easily-created

Initial reports regarding Stuxnet suggested that the code was developed by elite computer

experts with the help of state support and highly secretive military intelligence, but security experts working in a laboratory setting have been able to recreate key elements of the worm in a short time frame with limited resources.

With the release of the Stuxnet worm, the first piece of malicious code to cause physical damage, a whole new frontier of cyberattacks has been opened and imitators have been able to create Stuxnet-like clones with alarming ease.

The worm specifically targeted specialized software called supervisory control and data acquisition systems (SCADA) that controlled core processes at Iran's Bushehr nuclear facility and forced centrifuges there to spin out of control.

Initial reports regarding Stuxnet suggested that the code was developed by elite computer experts with the help of state support and highly secretive military intelligence, but security experts working in a laboratory setting have been able to recreate key elements of the worm in a short time frame with limited resources.

For instance, in just two months and with $20,000 in equipment, Dillon Beresford, an independent cybersecurity researcher at NSS Labs, was able to find more than a dozen vulnerabilities in the same type of electronic controllers exploited by Stuxnet in Iran. With the vulnerabilities that he found, Beresford was able to remotely commandeer an industrial control system's devices and reprogram them.

"What all this is saying is you don't have to be a nation-state to do this stuff. That's very scary," said Joe Weiss, an industrial control system expert. "There's a perception barrier, and I think Dillon crashed that barrier."

Meanwhile, Ralph Langner, a German control system security consultant and an expert on Stuxnet, developed a Stuxnet copycat in just four lines of code. Langner calls the code a "time bomb" and describes it as the most basic imitation attack that a malicious actor could create.

"As low-level as these results may be, they will spread through the hacker community and will attract others who continue digging," he said.

In another test, Mocana Corp., a cybersecurity firm was hired by a power utility in southern California to test the controllers used in its substations. In one day, Mocana was able to find multiple vulnerabilities that would allow hackers to control any piece of equipment connected to the controllers.

"We've never looked at a device like this before, and we were able to find this in the first day," said Kurt Stammberger, Mocana's vice president. "These were big, major problems, and problems frankly that have been known about for at least a year and a half, but the utility had no clue."

According to Siemens AG, one of the world's largest manufacturers of industrial control systems and the maker of the system hit by Stuxnet, security vulnerabilities primarily affect older industrial control systems, but even those are heavily protected with passwords and other security measures that critical infrastructure should have in place.

In addition, the company said that it had patched vulnerabilities in its software and that it was working with DHS Computer Emergency Response Team (CERT) to defend against future threats.

Siemens is not the only company with vulnerabilities in its control systems, security gaps appear to be an industry-wide problem, as the system tested by Mocana was not manufactured by Siemens.

Fixing these security gaps could prove to be a significant challenge to industry as control systems are designed to be in place for decades, making replacing or updating them a difficult task. In addition as more research is published, the more likely attacks become. Finally, to secure older units, critical infrastructure operators would likely be forced to install new equipment, a decision strongly avoided by companies as they would be forced to shut down their operations.

"The situation is not at all as bad as it was five to six years ago, but there's much that remains to be done," said Ulf Lindqvist, an expert on industrial control systems with SRI International. "We need to be as innovative and organized on the good-guy side as the bad guys can be."

U.S. fears science fiction-style sabotage in new wave of cyber attacks

Source:http://www.dailymail.co.uk/news/article-2052709/U-S-fears-science-fiction-style-sabotage-new-wave-cyber-attacks.html#ixzz1bu5tiBrR

When a computer attack hobbled Iran's unfinished nuclear power plant last year, it was

assumed to be a military-grade strike, the handiwork of elite hacking professionals with nation-state backing.

Yet for all its science-fiction sophistication, key elements have now been replicated in laboratory settings by security experts with little time, money or specialized skill.

It is an alarming development that shows how technical advances are eroding the barrier that has long prevented computer assaults from leaping from the digital to the physical world.

Exposed: Dillon Beresford said it took him just two months and $20,000 in equipment to find more than a dozen vulnerabilities in electronic controllers of the same type used in Iran

The techniques demonstrated in recent months highlight the danger to operators of power plants, water systems and other critical infrastructure around the world.

Scott Borg is director of the U.S. Cyber Consequences Unit, a non-profit group that helps the U.S. government prepare for future attacks

'Things that sounded extremely unlikely a few years ago are now coming along,' he said.

While the experiments have been performed in laboratory settings, and the findings presented at security conferences or in technical papers, the danger of another real-world attack such as the one on Iran is profound.

The team behind the so-called Stuxnet worm that was used to attack the Iranian nuclear facility may still be active. New malicious software with some of Stuxnet's original code

'controller' boxes that serve as the nerve centres for heavy machinery.

The attack on Iran changed all that. Now, security experts - and presumably, malicious hackers - are racing to find weaknesses. They've found a slew of vulnerabilities.

High risk: The 'Stuxnet' worm - a sophisticated cyber attack on the Bushehr nuclear plant in Iran (pictured here) opened a new era of cyber-warfare

and behaviour has surfaced, suggesting ongoing reconnaissance against industrial control systems.

And attacks on critical infrastructure are increasing. The Idaho National Laboratory, home to secretive defence labs intended to protect the nation's power grids, water systems and other critical infrastructure, has responded to triple the number of computer attacks from clients this year over last, the U.S. Department of Homeland Security has revealed.

For years, ill-intentioned hackers have dreamed of plaguing the world's infrastructure with a brand of sabotage reserved for Hollywood. They've mused about wreaking havoc in industrial settings by burning out power plants, bursting oil and gas pipelines, or stalling manufacturing plants.

But a key roadblock has prevented them from causing widespread destruction: they've lacked a way to take remote control of the electronic

Think of the new findings as the hacking equivalent of Moore's Law, the famous rule about computing power that it roughly doubles every couple of years. Just as better computer chips have accelerated the spread of PCs and consumer electronics over the past 40 years, new hacking techniques are making all kinds of critical infrastructure - even prisons - more vulnerable to attacks.

One thing all of the findings have in common is that mitigating the threat requires organizations to bridge a cultural divide that exists in many facilities. Among other things, separate teams responsible for computer and physical security need to start talking to each other and coordinate efforts.

Many of the threats at these facilities involve electronic

equipment known as controllers. These devices take computer commands and send instructions to physical machinery, such as regulating how fast a conveyor belt moves.

They function as bridges between the computer and physical worlds. Computer hackers can exploit them to take over physical infrastructure. Stuxnet, for example, was designed to damage centrifuges in the nuclear plant being built in Iran by affecting how fast the controllers instructed the centrifuges to spin. Iran has blamed the U.S. and Israel for trying to sabotage what it says is a peaceful program.

Security researcher Dillon Beresford said it took him just two months and $20,000 in equipment to find more than a dozen vulnerabilities in the same type of electronic controllers used in Iran. The vulnerabilities, which included weak password protections, allowed him to take remote control of the devices and reprogram them.

One of the biggest makers of industrial controllers is Siemens AG, which made the controllers in question. The company said it has alerted customers, fixed some of the problems and is working closely with CERT, the cybersecurity arm of the U.S. Department of Homeland Security.

Siemens said the issue largely affects older models of controllers. Even with those, the company said, a hacker would have to bypass passwords and other security measures that operators should have in place. Siemens said it knows of no actual break-ins using the techniques identified by Beresford, who works in Austin, Texas, for NSS Labs Inc.

Yet because the devices are designed to last for decades, replacing or updating them isn't always easy. And the more research that comes out, the more likely attacks become.

GROWING MENACE: THE WORST CYBER ATTACKS

Cyber attack: The nuclear power plant in Bushehr, southern Iran, which was the target of the Stuxnet worm

'What all this is saying is you don't have to be a nation-state to do this stuff. That's very scary,' said Joe Weiss, an industrial control system expert. 'There's a perception barrier, and I think Dillon crashed that barrier.'

Titan Rain: In 2004, secret military intelligence was stolen from NASA, Sandia National Laboratory and U.S. defence contractor Lockheed Martin. China was suspected to be behind the attack.

Stuxnet: Iranian nuclear facilities came under attack from a virus designed to specifically target

their computer hardware. Israel and/or the U.S. were strongly suspected of launching the attack.

Moonlight Maze: In 1998 the Pentagon, NASA and the department of energy computer systems were penetrated. The leak lasted for two years before it was eventually plugged - by which countless gigabytes of data had been stolen.

One of the foremost Stuxnet experts, Ralph Langner, a security consultant in Hamburg, Germany, has come up with what he calls a 'time bomb' of just four lines of programming code. He called it the most basic copycat attack that a Stuxnet-inspired prankster, criminal or terrorist could come up with.

'As low-level as these results may be, they will spread through the hacker community and will attract others who continue digging,' Langner said in an email.

The threat isn't limited to power plants. Even prisons and jails are vulnerable.

Another research team, based in Virginia, was allowed to inspect a correctional facility - it won't say which one - and found vulnerabilities that would allow it to open and close the facility's doors, suppress alarms and tamper with video surveillance feeds.

During a tour of the facility, the researchers noticed controllers like the ones in Iran. They used knowledge of the facility's network and that controller to demonstrate weaknesses.

They said it was crucial to isolate critical control systems from the Internet to prevent such attacks.

'People need to deem what's critical infrastructure in their facilities and who might come in contact with those,' Teague Newman, one of the three behind the research.

Another example involves a Southern California power company that wanted to test the controllers used throughout its substations. It hired Mocana Corp., a San Francisco-based security firm, to do the evaluation.

Kurt Stammberger, a vice president at Mocana, told The Associated Press that his firm found multiple vulnerabilities that would allow a hacker to control any piece of equipment connected to the controllers.

'We've never looked at a device like this before, and we were able to find this in the first day,' Stammberger said. 'These were big, major problems, and problems frankly that have been known about for at least a year and a half, but the utility had no clue.'

He wouldn't name the utility or the device maker. But he said it wasn't a Siemens device, which points to an industrywide problem, not one limited to a single manufacturer.

Mocana is working with the device maker on a fix, Stammberger said. His firm presented its findings at the ICS Cyber Security Conference in September.

Even if a manufacturer fixes the problem in new devices, there's no easy way to fix it in older units, short of installing new equipment. Industrial facilities are loath to do that because of the costs of even temporarily shutting its operations.

'The situation is not at all as bad as it was five to six years ago, but there's much that remains to be done,' said Ulf Lindqvist, an expert on industrial control systems with SRI International. "We need to be as innovative and organized on the good-guy side as the bad guys can be.'

Skype Security Flaw Potential Terrorist Threat, NYU Professor Says

Source:http://www.foxnews.com/scitech/2011/10/24/skype-security-flaw-potential-terrorist-threat-nyu-professor-says/?test=latestnews

A flagrant security flaw in the massively popular Skype video chat service may be putting Internet users worldwide at risk.

The serious security breach in the Internet video chat program, which boasts over 500 million users around the globe, means that any evil computer nerd could easily hunt down

users' whereabouts, according to a study co-authored by an NYU-Poly professor.

Skype was quick to downplay the importance of the research. But Keith Ross -- part of an international team of researchers who uncovered the problem -- said blackmailers or

other cybercrooks could, for example, use the flaw to track the travels of a cheating spouse.

And more alarmingly, terrorists or criminals could use the security gap to determine the

locations of groups of government officials or employees of a large organization, he told the New York Post. "Any sophisticated high school or college hacker could easily do this," Ross told the Post.

The flaw lets hackers determine the IP address from which a Skype user is logged in. That's a problem because IP addresses are usually specific to Internet users' physical locations. Hackers simply have to know how to grab their targets' IP addresses from simulated calls that Skype users would never notice -- and which leave no trace.

Adrian Asher, Skype's chief information security officer, said that IP addresses are easily uncovered in most web communications clients. "Just as with typical Internet communications software, Skype users who are connected may be able to determine each other's IP addresses. Through research and development, we will continue to make advances in this area and improvements to our software," he told FoxNews.com.

Skype places a priority on security and safety, he added. "We value the privacy of our users and are committed to making our products as secure as possible," Asher said.

Ross's study successfully tracked 10,000 randomly chosen Skype users over a two-week period, according to the New York Post. Researchers also used the flaw to successfully track one of their own as he traveled from New York to Chicago, back to New York and then to his home in France.

The flaw may also be a problem for other video chat services such as MSN Live, QQ and Google Talk, the researchers said.

Ross will present the results of the study -- titled "I Know Where You are and What You are Sharing" -- at a computer security conference in Germany next week.

Senior FBI official suggest creating alternative Internet

Source: http://www.homelandsecuritynewswire.com/srinfrastructure20111031-senior-fbi-official-suggest-creating-alternative-internet

With the number of cyberattacks on major corporations and government agencies on the rise, a top FBI official backed the call to create of a more secure alternative Internet.

Speaking at the Information Systems Security Association conference in Baltimore, Shawn Henry, the executive assistant director of the FBI, said U.S. networks will never be secure enough to prevent cyber intrusions and that threats facing critical systems were a permanent reality. "We can't 'tech' our way out of the cyber-threat," he said.

With cyberthreats constantly evolving and outpacing cyberdefenses, Henry suggested the creation of a secure Internet, separate from what individuals use now, to help secure critical infrastructure and financial systems.

On the alternative Internet, no users would be anonymous and only known and trusted individuals would be allowed access to the system. "We have to imagine things that haven't been imagined before" to stay ahead of attackers, Henry explained. He went on to say that the Internet needed better community-watch programs and more gated communities to protect systems and data.

On the alternative Internet, there would be a "guard post" that would define the rules for who could enter the secured environment and access the systems. Rules would have to be strict and the people allowed in to enter would have to aggressively report malicious actors and suspicious behavior. In addition, Henry suggested disconnected highly sensitive data from the Internet.

Cyberterrorism - The weapon of choice a decade after 9/11
By Scott Schober
Source: http://www.homelandsecuritynewswire.com/cyberterrorism-weapon-choice-decade-after-911

Scott Schober, the president and CEO of Berkeley Varitronics Systems, warns of the growing threat from cyberterrorists; he writes that in ten years, "the terrorists' weapon of choice may not necessarily be a 187,000 pound 767 jet loaded with fuel targeting" New York's skyline, instead it will be pajama-clad hackers taking down an electrical grid, causing mass confusion in the aviation system, or targeting a nuclear power plant's SCADA control system to create mass panic and chaos for millions

We lock our doors at night, set our alarms, and sleep in relative security throughout America. Yet, in the back of our minds we realize the world has changed in the past ten years. The anniversary of 9/11 is on everyone's mind with the looming thought of what if some radical terrorist is looking to cause havoc. Ten years later, the terrorists' weapon of choice may not necessarily be a 187,000 pound 767 jet loaded with fuel targeting New York City's 110 story iconic structures that fell, taking 2,753 innocent lives with it. Today's digital terrorist is sitting in his pajamas armed with a keyboard, mouse, and a computer that is anonymously connected into the world of the Internet. Oftentimes their target is not a specific person but rather an attack causing large scale disruptions that potentially affect millions of innocent computer users.

Cyberterrorism takes on several forms, but ultimately is a means of deliberately attacking or threatening targets by means of utilizing the internet as a common conduit which our computers and smart phones are intimately connected. The U.S. Department of Defense (DOD) has specifically charged United States Strategic Command (USSC) with the duty to combat the growing threat of cyberterrorism.

Ultimately, to thwart this growing problem each individual computer user can take precautions. In the past ten years more people have become dependent upon their wireless smart phone as their primary means of communications via email, text, or voice. With more than 5.3 billion mobile subscribers worldwide making up 77 percent of the world's population, that is a tremendous opportunity for unsavory individuals to direct their attacks. In 2011 over 85 percent of new handsets will have direct access to the mobile Web.

Oftentimes people feel the computer is the ultimate target of cyberterrorism, yet at the end of the day it may innocently be the housewife paying bills online, or the husband accessing his brokerage account. Far worse if the cyberterrorist has his/her sights set on taking the power grid down, causing mass confusion to the aviation industry, or monkeying around with a nuclear power plant's SCADA control systems. When major infrastructure is targeted, it can change the world as we know it overnight. Computers and our mobile phones are vulnerable to cyberterrorists, but effectively utilizing and securing this technology can at the same time be the most effective defense against terrorism.

Reflecting back over the past ten years, many doubt as they peer up into the New York City skyline that the new World Trade Center will not be taken down by radical terrorists in a jet. However, with the cyberterrorist's new weapon of choice they may opt to focus their efforts on the delicate infrastructure controlled by the vast interconnection of computers around the globe. These powerful computers are getting faster and smarter, but so are the armchair cyberterrorists of tomorrow.

Scott Schober is president and CEO of Berkeley Varitronics Systems, Inc.

Kaspersky and cyberterrorism

Source: http://www.forbes.com/sites/richardstiennon/2011/11/02/kaspersky-and-cyber-terrorism/

Of all the pronouncements coming out of the London Cyber Summit this week, the

statements of Eugene Kaspersky are the most provocative. Rather than pile on and criticize him for uttering the words "cyber terrorism" it is worth taking a deep breath and considering what could give rise to his statements.

Kaspersky of course is the founder of anti-virus powerhouse Kaspersky Lab, responsible for some of the best research into malware and the cyber criminals who create it. It is safe to assume that he has pretty good insight into the world of cyber threats. He is rather flamboyant

have sold their skills to the terrorists – and then...oh, God." "There is already cyber espionage, cyber crime, hacktivisim soon we will be facing cyber terrorism,"

Before the semantic police jump all over this (Terrorism involves death and destruction! You can't do that over the Internet!) let's define our terms. What would we call it when terrorists engage in cyber attacks? I am going to assume Kaspersky thinks along the lines I do. Cyber terrorism would be cyber attacks carried out by terrorist organizations. Is that possible? Has it happened? Is it likely to happen soon? First, is it possible for terrorist organizations to engage in cyber attacks? Of course. Denial of Service, defacements, doxing (publishing private information about public figures),

and has led a turbulent life; most recently rescuing his son from kidnappers in Russia. So yes, he may be prone to making controversial statements.

Sky News provides the following quotes:
"I don't want to speak about it. I don't even want to think about it," he said. "But we are close, very close, to cyber terrorism. Perhaps already the criminals

extortion, cyber crime, even Stuxnet-like cyber sabotage, could all be carried out by terrorists as easily as by the current bad actors (organized crime, Anonymous, Lulzsec, etc). I think the ease with which terrorists could engage in cyber attacks is what spurred Kaspersky to say what he did.
Have terrorists engaged in cyber attacks? In 2006 a

popular e-commerce site received an email claiming to be from Islamic Jihad and demanding that they take offensive material, offered by one of their resellers, off of their site. When they elected to ignore the demands their domain was subjected to a DDoS (Distributed Denial of Service) attack that took them down for several days. Forensics verified that the attacks originated in the Mid-East. I understand they reported the attacks to the FBI but never publicized the event, although it was clearly visible in up-time records kept by Netcraft.

This year the **CommodoHacker** (above), who claims to be a supporter of the Iranian regime, broke in to the Dutch Certificate Authority DigiNotar and created signed certificates for at least 500 organizations including CIA, MI6, Facebook, Microsoft, Skype, and Twitter. These fake certificates were used by Iran to spy on its own populace who use Google for email.

And of course trying to keep track of the hacking that goes on in the Mid-East against Israel is an overwhelming task. But just because a hacker supports the same cause as terrorist organizations is a tenuous claim of cyber terrorism. At the same time just follow the "Tango Down" posts of Th3J35t3r on Twitter to see all of the Jihadi recruitment sites that he has tasked himself with taking down. There is no question that terrorists use the Internet.

The final question of will terrorists engage in cyber attacks depends on their motivations more than their abilities, since the tools and capabilities are easily acquired. Will disrupting the Internet, major stock exchanges, banks, or government web sites be attractive to them? Since the costs and risks are so low you can see why Kaspersky is concerned.

Duqu mystery deepens as Iran admits infection

Source:http://www.homelandsecuritynewswire.com/dr20111118-duqu-mystery-deepens-as-iran-admits-infection

Iran recently revealed that the Duqu virus, a possible pre-cursor to a Stuxnet-like attack, has been discovered in its computer network.

spread to and what its impacts are has not been completed yet." Iran's semi-official Fars News Agency reported that Iran has developed

"We are in the initial phase of fighting the Duqu virus," said Gholamreza Jalali, the head of Iran's civil defense program. "The final report which says which organizations the virus has

anti-virus software to combat the virus and according to Jalali, "all the organizations and centers that could be

susceptible to being contaminated are being controlled."

News of Duqu was first released in October by the cybersecurity company Symantec. The virus contains code similar to Stuxnet, the computer worm that reportedly crippled Iran's nuclear program by attacking industrial control systems used to operate its centrifuges.

Symantec says that while Stuxnet was designed to cause direct damage to Iran's nuclear program, Duqu is different in that it gathers data that could be used for a future attack. In a report issued last month, the company stated,"Duqu is essentially the precursor to a future Stuxnet-like attack. Instead of being designed to sabotage an industrial control system, the new virus is designed to gain remote access capabilities."

The virus accomplishes its goal by exploiting a "zero-day vulnerability," or a previously undiscovered security loophole, in Microsoft Word. It utilizes a separate piece of malware known as a "dropper" to infect computers through a font embedded in a Word document.

Stuxnet utilized four such vulnerabilities, an unprecedented feat which led experts to speculate that the worm was created by hackers with government backing. It is widely believed that Israel's Mossad as well as the United States military was responsible for the cyberattack.

Further analysis into Duqu reveals that its creators have a sense of humor. According to the Moscow-based Kaspersky Lab, the e-mail which infected an unnamed company with Duqu in April was sent by a Mr. B. Jason, an apparent reference to the Jason Bourne spy novels by Robert Ludlum.

Additionally in one of the virus' strings of code is the phrase "Copyright 2003 Showtime Inc. All rights reserved. Dexter Regular version 1.00. Dexter is a registered trademark of Showtime Inc." Dexter Regular is the name of the font used to exploit targeted systems. Dexter is a television series about a CSI doctor who is also a serial killer.

Iran has claimed that Duqu is the third piece of malware to strike the country. In April, Iranian officials said they had detected a virus, dubbed "Stars," in its networks.

Kaspersky believes that Stars might actually be a product of Duqu. Just prior to the Iranian announcement, an unnamed company was contaminated with Duqu through an infected e-mail.

According to Alexander Gostev, the head of the Global Research and Analysis team at Kaspersky, "most probably, the Iranians found a keylogger module that had been loaded onto a system," he wrote. "It's possible that the Iranian specialists found just the keylogger, while the main Duqu module and the dropper (including the documents that contained the then-unknown vulnerability) may have gone undetected."

Symantec believes that attacks using Duqu may have begun as early as December 2010.

Subsequent research into the virus by Kaspersky found discovered drivers in the Duqu code compiled as far back as 2007. "If this information is correct, then the authors of Duqu must have been working on this project for over four years!" said Gostev.

DHS investigates attacks on New Jersey water supply

Source:http://www.northjersey.com/topstories/westmilford-hewitt-newfoundland/Homeland_Security_to _look_into_attacks_on_West_Milford_water_sewer_services.html

DHS agents and local authorities in New Jersey are investigating a series of attacks on the West Milford water system. Since July there have been more than fifteen attacks on local water and sewage facilities that in some instances have resulted in sewage flooding the street or losses in service all together.

Attacks on West Milford's water supply attract DHS attention // Source: northjersey.com

According to Kelly Love, the administrator for the town's Municipal Utility Authority (MUA), the attackers have shut off power to water systems, opened valves that should have been shut, and thrown a plank of wood into a sewage filtration system. "You are talking about acts that border on, or actually are, terrorism," said Eric Williams, the owner of Jersey Environmental Solutions, which took responsibility for the water system over the summer. "[The vandals] are creating a public health issue by messing with the water," Williams said.

He explained that by interfering with the mechanisms that chlorinate drinking water, dangerous bacteria could grow and infect the supply.

New Jersey

addition the New Jersey Department of Environmental Protection fined the facilities for $1 million and order residents to drink boiled water after dangerous bacteria was found in the supply.

Williams, the latest contractor to take over the facilities, said he was not sure if the attacks on the facility were actually the work of saboteurs or simply mistakes made by a new staff.

On 1 September, Williams said his doubts were laid to rest when he went to the Birch Hill water facility after residents complained of a loss in water pressure. Upon investigating the facility, he found that the main power lever had been pulled to the "off" position and that a recently opened valve had flooded the floor with two feet of water, which could have caused an electric fire. "It was very disturbing," Williams said. "Who would do this?"

Authorities are uncertain as to who is behind the attacks, but Love believes that the attacker "had to be someone who knew the plant and knows how it works — a regular person wouldn't know what to turn on and off."

MUA's facilities have long been a source for problems. In 2009 when Love first began working at MUA, she said the facilities were in poor condition after decades of neglect.

Most recently two employees filed lawsuits alleging workplace abuse and misconduct. In

U.K. unveils new cyber defense strategy

The U.K. government last week published its new Cyber Security Strategy; the government said the new strategy sets out "how the United Kingdom will support economic prosperity, protect national security, and safeguard the public's way of life"

The U.K. government last week published its new Cyber Security Strategy. The government says the new strategy sets out "how the United Kingdom will support economic prosperity, protect national security, and safeguard the public's way of life by building a more trusted and resilient digital environment."

CabinetOffice

The government said that new policy heralds a new era of cooperation between the government and the private sector on cyber security, thus making the United Kingdom a secure place to do business.

Around 6 percent of the U.K. GDP is generated by the Internet and is set to grow — making it a larger sector than either utilities or agriculture — with the Internet boom predicted to create 365,000 jobs over the next five years.

One purpose of the new policy is to create new opportunities for businesses and help build a thriving cyber security industry. The U.K. increasing

dependence on digital technologies, however, has given rise to new risks. For example, there are more than 20,000 malicious e-mails on government networks each month, 1,000 of which are deliberately targeted.

The government has already ranked cyber security as a tier 1 national security priority and committed £650 million over the next four years to bolster its cyber defenses.

The United Kingdom earlier this month hosted the London Conference on Cyberspace to drive forward international dialogue on building a secure digital world.

Prime Minister David Cameron said:

While the internet is undoubtedly a force for social and political good, as well as crucial to the growth of our economy, we need to protect against the threats to our security. This strategy not only deals with the threat from terrorists to our national security, but also with the criminals who threaten our prosperity as well as blight the lives of many ordinary people through cyber crime. Cyber security is a top priority for government and we will continue to work closely with the police, security services, international partners and the private sector to ensure that the UK remains one of the most secure places in the world to do business

Minister for Cyber Security Francis Maude said:

The growth of the Internet has revolutionized our everyday lives and promises untold economic and social opportunities in years to come. This strategy sets out how we will realize the full benefits of a networked world by building a more trusted and resilient digital environment, from protecting the public from online fraud to securing critical infrastructure against cyber attacks. The Government cannot do this alone. Closer partnership between the public and private sector is crucial. The strategy heralds a new era of unprecedented cooperation between the Government and industry on cyber security, working hand in hand to make the UK one of the most secure places in the world to do business.

Minister for Cyber Crime James Brokenshire said:

We want to ensure that everyone can make the most of the internet and online services while protecting themselves from crime. The new National Crime Agency will share knowledge and expertise across law enforcement agencies, building on the pioneering work done by the Metropolitan Police and SOCA. We are also reaching out to industry and the public to get involved. We all have a role to play in keeping ourselves and our families safe while enjoying the huge opportunities and benefits of surfing the web.

Minister for Business & Enterprise Mark Prisk said:

With one of the largest online economies in the world, valued at £100 billion a year, cyberspace is vital for the U.K.'s economic prosperity. However as well as bringing opportunities for businesses and their customers, cyberspace also brings threats.

That's why it's important that we help all companies, from big multi-nationals to our small businesses take some simple, practical measures to protect themselves and their customers online.

NOTE: You can download the full document from the Newsletter's website – CBRNE Papers section.

MIT report warns U.S. electrical grid vulnerable

Source:http://www.homelandsecuritynewswire.com/srinfrastructure20111212-mit-report-warns-u-s-electrical-grid-vulnerable

A new report from the Massachusetts Institute of Technology warns that the U.S. electrical grid is vulnerable to cyberattacks.

According to the report, titled "Future of the Electric Grid," the U.S. electrical grid's cybersecurity vulnerabilities stem from weaknesses in processes, technology, as well as the actual physical environment.

"Millions of new communicating electronic devices … will introduce attack vectors —

paths that attackers can use to gain access to computer systems or other communicating equipment," the report found.

This would in turn lead to an increased likelihood of "intentional and accidental communications disruptions" including "loss of control over grid devices, loss of communications between grid entities or control centers or blackouts."

In addition, according to the report, if hackers infiltrated critical data networks they could also steal sensitive data including which power lines are most vital for the distribution of electricity and which homes are vacant in addition to stealing personal information or corporate secrets.

The report noted that while the Federal Energy Regulatory Commission and North American Electric Reliability Corp. govern cybersecurity standards for the power system, no single entity regulates cybersecurity for the distribution system itself.

To bolster security, the report recommends that the government "designate a single agency to have responsibility for working with industry and to have appropriate regulatory authority to enhance cybersecurity preparedness, response and recovery across the electric power sector, including bulk power and distribution systems."

Patrick Miller, the president and CEO of the National Electric Sector Cybersecurity Organization, said he would gladly have a single agency with responsibility for cybersecurity.

"We would welcome a single authority," Miller said. "We've seen a lot of confusion around who would have authority in the event of a cyberattack [on the power grid]."

DHS Releases Cyber Blueprint

Source: https://www.infosecisland.com/blogview/18696-DHS-Releases-Blueprint-for-a-Secure-Cyber-Future.html

The Homeland Security Department earlier this week released a blueprint for managing and protecting the nation against cybersecurity threats. Not surprisingly, one aspect of the strategy includes investing in the cybersecurity workforce.

The plan -- the Blueprint for a Secure Cyber Future -- was released Dec. 12 and aims to better protect critical information infrastructure and build a stronger cyber ecosystem for the future. More specifically, the blueprint includes efforts to provide specialized and continuing security training to cybersecurity professionals, including training that allows them to design, build and operate IT systems that are "fundamentally secure and resilient."

The blueprint also includes efforts to create a "common body of knowledge" for cybersecurity workers, particularly through increased classroom-based and immersive learning environments as well as through rotational assignments of personnel between the public and private sectors. The plan also focuses on the development and use of capability and skills maturity models, which describe the general and technical skills necessary at various levels for cybersecurity work.

DHS also plans to build up both the public and private cybersecurity workforce as part

of the plan, in part by helping to develop a rigorous cybersecurity and software assurance curriculum through the National Initiative for Cybersecurity Education. The agency also emphasizes incentives like scholarships, grants, subsidies and tax incentives for cybersecurity workers as part of the plan.

Finally, the blueprint focuses on improving recruitment and retention of cyber workers through faster hiring, challenging assignments, structured career paths and employee satisfaction surveys.

"The increasing volume and sophistication of cyber exploitation demands heightened situational awareness, secure implementation of technology, coordinated incident response, demonstrated resilience in critical functions and a professionalized cybersecurity workforce that is dynamically managed," the blueprint states.

NOTE: You can download the full paper from Newsletter's website

Twelve Chinese hacker groups responsible for attacks on U.S.

Source:http://www.homelandsecuritynewswire.com/dr20111216-twelve-chinese-hacker-groups-responsible-for-attacks-on-u-s

U.S. cybersecurity experts say as few as twelve different Chinese hacker collectives, working at the behest of the government, are responsible for the majority of cyberattacks on U.S. businesses and government agencies.

The bulk of the attacks are stealthy in nature and have resulted in the loss of billions of dollars' worth of intellectual property and state secrets from the private and public sector.

According to cybersecurity experts speaking anonymously to *News24*, the Chinese hackers often have distinct digital signatures that U.S. officials use to link them to specific hacker teams.

Even though officials have traced the cyberattacks to China, it is notoriously difficult to pinpoint with certainty where a specific attack originates from. Additionally China has vehemently denied that it sponsors hackers and since the United States does not have an agreement with the Chinese government, it cannot prosecute hackers based there.

Cybersecurity experts and military officials are becoming increasingly frustrated with these attacks and are urging the government to do more.

"Industry is already feeling that they are at war," said James Cartwright, a retired Marine general and the former vice chair of the Joint Chiefs of Staff.

Cartwright has been vocal in his calls for the U.S. government to hold China and other countries that sponsor hackers accountable.

"Right now we have the worst of worlds," said Cartwright. "If you want to attack me you can do it all you want, because I can't do anything about it. It's risk free, and you're willing to take almost any risk to come after me."

Instead, the United States "needs to say, if you come after me, I'm going to find you, I'm going to do something about it. It will be proportional, but I'm going to do something… and if you're hiding in a third country, I'm going to tell that

country you're there, if they don't stop you from doing it, I'm going to come and get you."

Jon Ramsey, the head of Dell SecureWorks' counter threat unit, echoed General Cartwright's sentiments, stating, the government "needs to do more to increase the risk" for hackers.

"In the private sector we're always on defense. We can't do something about it, but someone has to. There is no

deterrent not to attack the United States," he said.

To that end, the Pentagon recently updated its military strike policy adding that cyberattacks on the United States could result in a physical response. The military has also been actively bolstering its own cyberdefense and warfare capabilities, standing up Cyber Command and training thousands of troops to wage war on digital battlefields.

In addition, a recently released Congressional report concluded that Chinese and Russian hackers backed by their respective states are actively stealing U.S. trade and technology secrets to boost their economic development.

"The pace of foreign economic collection and industrial espionage activities against major U.S. corporations and U.S. government agencies is accelerating," the report said.

In the past, Chinese cyberattacks primarily targeted the U.S. government, but in the last decade, hackers have focused more and more on private businesses, especially defense contractors and businesses in energy, finance, and other critical sectors.

To stop these attacks, General Cartwright said the U.S. government should implement a clear policy on how it responds to cyberattacks.

He said, once a hacker is detected, the State Department should first ask the country to stop the attack. If that country does not cooperate, then the United States has the right to shut down the computer server from allowing the attack to continue by any means necessary but being mindful to avoid collateral damage.

Terror News

Oslo-type attack in U.S. likely in next few years

Source: http://www.homelandsecuritynewswire.com/security-analyst-oslo-type-attack-us-likely-next-few-years

An expert on American-Muslims fears that with the rising anti-Islamic sentiments in the United States an "Oslo-type" attack could occur in the next few years at a U.S. mosque; speaking on a panel on security threats facing faith based organizations at the ASIS 2011 security conference, Nawar Shora, the CEO of Shams Training and Development, said, "I fear that in the next few years we'll have something like Oslo repeated here in this country, whether someone will go to an Islamic center or whether someone will try a massacre during a worship on Friday".

Impromptu shrine at site of Breivik's attaks // Source: wordpress.com

Speaking on a panel on security threats facing faith based organizations at the ASIS 2011 security conference, Nawar Shora, the CEO of Shams Training and Development and the author of "The Arab-American Handbook," said, "I fear that in the next few years we'll have something like Oslo repeated here in this country, whether someone will go to an Islamic center or whether someone will try a massacre during a worship on Friday."

Shora noted that prior to 9/11, the Muslim community rarely experienced vandalism or security threats at mosques, community centers, or places of worship, but after the 9/11 attacks hate crimes and anti-Islamic sentiments skyrocketed around the country.

The number of reported incidents eventually leveled off, but Shora and other Muslims fear that the most recent rash of anti-Islamic incidents could be the worst yet.

"More so than immediately after 9/11, the brewing Islamophobia today seems to be at an all-time high," Shora said.

According to the Council on American-Islamic Relations (CAIR), the number of reported civil rights complaints from the Muslim community has steadily risen since 9/11, but in 2008, complaints fell 14 percent for the second year in a row.

At the time the group stated, "Observing a second year's decline in reported hate crimes, CAIR reaffirms its cautious optimism that America may be witnessing a leveling-off of the post-9/11 backlash against Americans of the Islamic faith."

However the lull in anti-Islamic activity did not last long as the proposed Islamic center near Ground Zero in New York last year seemed to spark a new wave of hate crimes directed at Muslims. Multiple incidents of vandalism at mosques across the country appeared in the news as well as other incidents like the stabbing of a New York City cabdriver after the perpetrator confirmed he was Muslim, protests against proposed mosques across the country, and the organized burning of the Qur'an by a radical church in Florida.

Ibrahim Hooper, CAIR's spokesman, questioned whether the decline in hate crime statistics was deceiving and that anti-Muslim sentiment had not receded but actually festered during that time.

Another explanation could be that the recent explosion of Islamophobia is a result of faulty statistics. The bulk of hate crimes, vandalism, and other malicious acts directed at places of worship are grossly underreported, so the

2008 CAIR study could be based on poor data. Speaking on the same panel as Shora at the ASIS security conference, Jeffrey Barrett, the director of support services for the Church of Jesus Christ of Latter Day Saints, explained most churches tend to not report incidents, especially if it is relatively minor that can be easily fixed like spray painting or broken windows. In addition, most churches hesitate to contact local authorities for fear of negative publicity.

"I think the statistics that the government puts out are quite false. I'll that bet if we threw the statistics just from our church in there, we would probably exceed many of those categories just by our numbers alone. I know we've had multiple arsons in the last two years, and I know we've had far more than fifty vandalisms in a year's time," Barrett said.

Shora as well as fellow ASIS panelist Richard Raisler, the director of community-wide security for the Jewish Federation of Greater Atlanta, both stated that underreporting is endemic to all faiths. In the case of Muslims, Shora explained that the majority of Muslims do not report vandalism or hate crimes to local law enforcement due to a lack of trust.

"[Muslims] are too afraid to even contact law enforcement to say, 'We had an arson' or 'We had a threat.' Every so often you hear about it, but as a general rule, they're apprehensive," Shora said. "When it comes to the Muslim community, they fall short on both communicating with law enforcement and those that need to know about it and in some ways fear that they are not understood."

To help remedy this situation, Shora recommended that the Muslim community as well as law enforcement officials increase communication to build better understanding in the hopes that more incidents will be reported.

"I've always said our greatest challenge post 9/11 has been a lack of trust. And we get to the lack of trust through a lack of communication and a lack of understanding. If we flip all those elements to the positive, then the formula is simple – communications plus understanding equals trust.

Cutting Through the Lone-Wolf Hype

By Scott Stewart
Source:http://www.stratfor.com/weekly/20110921-cutting-through-lone-wolf-hype?utm_source=freelist-f&utm_
medium=email&utm_campaign=20110922&utm_term=sweekly&utm_content=readmore&elq=21a73ced1f144f
b1ad43d2480e06a8a4

Lone wolf. The mere mention of the phrase invokes a sense of fear and dread. It conjures up images of an

unknown, malicious plotter working alone and silently to perpetrate an unpredictable, undetectable and unstoppable act of terror. This one phrase combines the persistent fear of terrorism in modern society with the primal fear of the unknown.

The phrase has been used a lot lately. Anyone who has been paying attention to the American press over the past few weeks has been bombarded with a steady stream of statements regarding lone-wolf militants. While many of these statements, such as those from President Barack Obama, Vice President Joseph Biden and Department of Homeland Security Director Janet Napolitano, were made

in the days leading up to the 10th anniversary of the 9/11 attacks, they did not stop when the threats surrounding the anniversary proved to be unfounded and the date passed without incident. Indeed, on Sept. 14, the Director of the National Counterterrorism Center, Matthew Olsen, told CNN that one of the things that concerned him most was "finding that next lone-wolf terrorist before he strikes."

Now, the focus on lone operatives and small independent cells is well founded. We have seen the jihadist threat devolve from one based primarily on the hierarchical al Qaeda core organization to a threat emanating from a broader array of grassroots actors operating alone or in small groups. Indeed, at present, there is a far greater likelihood of a successful jihadist attack being conducted in the West by a lone-wolf attacker or small cell inspired by al Qaeda than by a member of the al Qaeda core or one of the franchise groups. But the lone-wolf threat can be generated by a broad array of ideologies, not just jihadism. A recent reminder of this was the July 22 attack in Oslo, Norway, conducted by lone wolf **Anders Breivik**.

The lone-wolf threat is nothing new, but it has received a great deal of press coverage in recent months, and with that press coverage has come a certain degree of hype based on the threat's mystique. However, when one looks closely at the history of solitary terrorists, it becomes apparent that there is a significant gap between lone-wolf theory and lone-wolf practice. An examination of this gap is very helpful in placing the lone-wolf threat in the proper context.

The Shift Toward Leaderless Resistance

While the threat of lone wolves conducting terrorist attacks is real, the first step in putting the threat into context is understanding how long it has existed. To

say it is nothing new really means that it is an inherent part of human conflict, a way for a weaker entity — even a solitary one — to inflict pain upon and destabilize a much larger entity. Modern lone-wolf terrorism is widely

considered to have emerged in the 1800s, when fanatical individuals bent on effecting political change demonstrated that a solitary actor could impact history. Leon Czolgosz, the anarchist who assassinated U.S. President William McKinley in 1901, was one such lone wolf.

The 1970s brought lone wolf terrorists like **Joseph Paul Franklin** (top) and **Ted Kaczynski** (bottom), both of whom were able to operate for years without

being identified and apprehended. Based on the success of these lone wolves and following the 1988 Fort Smith Sedition Trial, in which the U.S. government's penetration of white hate groups was clearly revealed, some of the leaders of these penetrated groups began to advocate "leaderless resistance" as a way to avoid government pressure. They did not invent the concept, which is really quite old, but they readily embraced it and used their status in the white supremacist movement to advocate it.

In 1989, William Pierce, the leader of a neo-Nazi group called the National Alliance and one of the Fort Smith defendants, published a fictional book under the pseudonym Andrew Macdonald titled "Hunter," which dealt with the exploits of a fictional lone wolf named Oscar Yeager. Pierce dedicated the book to Joseph Paul Franklin and he clearly intended it to serve as an inspiration and model for lone-wolf operatives. Pierce's earlier book, "The Turner Diaries," was based on a militant operational theory involving a clandestine organization, and "Hunter" represented a distinct break from that approach.

In 1990, Richard Kelly Hoskins, an influential "Christian Identity" ideologue, published a book titled "Vigilantes of Christendom" in which he introduced the concept of the "Phineas Priest." According to Hoskins, a Phineas

Priest is a lone-wolf militant chosen by God and set apart to be God's "agent of vengeance" upon the earth. Phineas Priests also believe their attacks will serve to ignite a wider "racial holy war" that will ultimately lead to the salvation of the white race.

In 1992, another of the Fort Smith defendants, former Ku Klux Klan Leader Louis Beam, published an essay in his magazine "The Seditionist" that provided a detailed roadmap for moving the white hate movement toward the leaderless resistance model. This roadmap called for lone wolves and small "phantom" cells to engage in violent action to protect themselves from detection.

In the white-supremacist realm, the shift toward leaderless resistance — taken because of the government's success in penetrating and disrupting group operations — was an admission of failure on the part of leaders like Pierce, Hoskins and Beam. It is important to note that in the two decades that have passed since the leaderless-resistance model rose to prominence in the white-supremacist movement there have been only a handful of successful lone-wolf attacks. The army of lone wolves envisioned by the proponents of leaderless resistance never materialized.

But the leaderless resistance model was advocated not only by the far right. Influenced by their anarchist roots, left-wing extremists also moved in that direction, and movements such as the Earth Liberation Front and the Animal Liberation Front actually adopted operational models that were very similar to the leaderless-resistance doctrine prescribed by Beam.

More recently, and for similar reasons, the jihadists have also come to adopt the leaderless-resistance theory. Perhaps the first to promote the concept in the jihadist realm was jihadist military theoretician Abu Musab al-Suri. Upon seeing the success the United States and its allies were having against the al Qaeda core and its wider network following 9/11, al-Suri began to promote the concept of individual jihad — leaderless resistance. As if to prove his own point about the dangers of belonging to a group, al-Suri was reportedly captured in November 2005 in Pakistan.

Al-Suri's concept of leaderless resistance was embraced by al Qaeda in the Arabian Peninsula (AQAP), the al Qaeda franchise group in Yemen, in 2009. AQAP called for this type of strategy in both its Arabic-language media and its English language magazine, "Inspire," which published long excerpts of al-Suri's material on individual jihad. In 2010, the al Qaeda core also embraced the idea, with U.S.-born spokesman Adam Gadahn echoing AQAP's calls for Muslims to adopt the leaderless resistance model.

However, in the jihadist realm, as in the white-supremacist realm before it, the shift to leaderless resistance was an admission of weakness rather than a sign of strength. Jihadists recognized that they have been extremely limited in their ability to successfully attack the West, and while jihadist groups welcomed recruits in the past, they are now telling them it is too dangerous because of the steps taken by the United States and its allies to combat the transnational terrorist threat.

Busting the Mystique

Having established that when a group promotes leaderless resistance as an operational model it is a sign of failure rather than strength, let's take a look at how the theory translates into practice.

On its face, as described by strategists such as Beam and al-Suri, the leaderless-resistance theory is tactically sound. By operating as lone wolves or small, insulated cells, operatives can increase their operational security and make it more difficult for law enforcement and intelligence agencies to identify them. As seen by examples such as Fort Hood shooter Nidal Hassan and Roshonara Choudhry, who stabbed British lawmaker Stephen Timms with a kitchen knife in May 2010, such attacks can create a significant impact with very little cost.

Lone wolves and small cells do indeed present unique challenges, but history has shown that it is very difficult to put the lone-wolf theory into practice. For every Eric Rudolph, Nidal Hasan and Anders Breivik there are scores of half-baked lone-wolf wannabes who either botch their operations or are uncovered before they can launch an attack.

It is a rare individual who possesses the requisite combination of will, discipline, adaptability, resourcefulness and technical skill to make the leap from theory to practice and become a successful lone wolf. Immaturity, impatience and incompetence are frequently the bane of failed lone-wolf operators, who also frequently lack a realistic assessment of their capabilities and tend to attempt attacks that are far too complex. When they try to do something spectacular they frequently achieve little or nothing. By definition and operational necessity, lone-wolf operatives do not have the luxury of

attending training camps where they can be taught effective terrorist tradecraft. **Nasir al-Wahayshi** has recognized this and has urged jihadist lone wolves to focus on simple, easily accomplished attacks that can be conducted with readily available items and that do not require advanced tradecraft to succeed.

It must also be recognized that attacks, even those conducted by lone wolves, do not simply materialize out of a vacuum. Lone wolf attacks must follow the same planning process as an attack conducted by a small cell or hierarchical group. This means that lone wolves are also vulnerable to detection during their planning and preparation for an attack — even more so, since a lone wolf must conduct each step of the process alone and therefore must expose himself to detection on multiple occasions rather than delegate risky tasks such as surveillance to someone else in order to reduce the risk of detection. A lone wolf must conduct all the preoperational surveillance, acquire all the weapons, assemble and test all the components of the improvised explosive device (if one is to be used) and then deploy everything required for the attack before launching it.

Certainly, there is far more effort in a truck bomb attack than a simple attack with a knife, and the planning process is shorter for the latter, but the lone wolf still must follow and complete all the steps. While this operational model offers security advantages regarding communications and makes it impossible for the authorities to plant an informant in a group, it also increases operational security risks by exposing the lone operator at multiple points of the planning process.

Operating alone also takes more time, does not allow the lone attacker to leverage the skills of others and requires that the lone attacker provide all the necessary resources for the attack. When we consider all the traits required for someone to bridge the gap between lone-wolf theory and practice, from will and discipline to self-sufficiency and tactical ability, there simply are not many people who have both the ability and the intent to conduct such attacks.

This is why we have not seen more lone-wolf attacks despite the fact that the theory does offer some tactical advantages and has been around for so long. The limits of working alone also mean that, for the most part, lone-wolf attacks tend to be smaller and less damaging than attacks conducted by independent cells or hierarchical organizations. Breivik's attack in Norway and Hasan's attack at Fort Hood are rare exceptions and not the rule.

When we set aside the mystique of the lone wolf and look at the reality of the phenomenon, we can see that the threat is often far less daunting in fact than in theory. One of the most vocal proponents of the theory in the white supremacist movement in the late 1990s was a young California neo-Nazi named Alex Curtis. After Curtis was arrested in 2000 and convicted of harassing Jewish figures in Southern California, it was said that when he made the jump from "keyboard commando" to conducting operations in the physical world he proved to be more of a "stray mutt" than a lone wolf.

Lone wolves — or stray mutts — do pose a threat, but that threat must be neither overstated nor ignored. **Lone attackers are not mythical creatures that come out of nowhere to inflict harm.** They follow a process and are vulnerable to detection at certain times during that process. Cutting through the hype is an important step in dispelling the mystique and addressing the problems posed by such individuals in a realistic and practical way.

Domestic Terrorism

Focus on Militia Extremism

Last March, nine members of an extremist militia group were charged in Michigan with seditious conspiracy and attempted use of weapons of mass destruction in

connection with an alleged plot to attack law enforcement and spark an uprising against the government.

According to the federal indictment, the nine individuals planned to kill a law enforcement officer and then use bombs to attack the caravan of cars taking part in the subsequent funeral procession, hoping that this violence would incite a larger armed conflict with authorities. Fortunately, the FBI and the Michigan State Police intervened and took the subjects into custody before they could carry out their alleged plot.

It's just one example of the dangers posed by so-called militia extremists—the latest topic in our series to educate the nation on domestic terror threats that the FBI investigates today. Previous stories have focused on anarchist extremists, eco-terrorists/animal rights extremists, lone offenders, and sovereign citizen extremists.

Who they are. Like many domestic terrorism groups, militia extremists are anti-government.

What sets them apart is that they're often organized into paramilitary groups that follow a military-style rank hierarchy. They tend to stockpile illegal weapons and ammunition, trying illegally to get their hands on fully automatic firearms or attempting to convert weapons to fully automatic. They also try to buy or manufacture improvised explosive devices and typically engage in wilderness, survival, or other paramilitary training.

Who and what they target. They usually go after the government itself—including law enforcement personnel, representatives of the courts, and other public officials, along with government buildings. When caught, most militia extremists are charged with weapons, explosives, and/or conspiracy violations.

What they believe in. Many militia extremists view themselves as protecting the U.S. Constitution, other U.S. laws, or their own individual liberties. They believe that the Constitution grants citizens the power to take back the federal government by force or violence if they feel it's necessary. They oppose gun control efforts and fear the widespread disarming of Americans by the federal government.

Militia extremists often subscribe to various conspiracy theories regarding government. One of their primary theories is that the United Nations—which they refer to as the New World Order, or NWO—has the right to use its military forces anywhere in the world (it doesn't, of course). The extremists often train and prepare for what they foresee as an inevitable invasion of the U.S. by United Nations forces. Many militia extremists also wrongly believe that the federal government will relocate citizens to camps controlled by the Federal Emergency Management Agency, or force them to undergo vaccinations.

One important note: simply espousing anti-government rhetoric is not against the law. However, seeking to advance that ideology

through force or violence **is** illegal, and that's when the FBI and law enforcement become involved.

What is the FBI doing to combat the militia extremism threat? In addition to our lawful use of sophisticated investigative techniques, we've expanded our work with other federal agencies such as the Bureau of Alcohol, Tobacco, Firearms, and Explosives and with our state and local partners. And we use intelligence and analysis to help identify gaps in our knowledge, emerging tactics and trends, and effective investigative strategies.

As always, the combination of intelligence, coordinated law enforcement efforts, and an informed public is the most effective way to counter the threats posed by domestic extremists.

Park51 Islamic Center Opens Its Doors Near Ground Zero

Source: http://www.huffingtonpost.com/2011/09/22/park51-islamic-center-ope_n_975585.html

An Islamic cultural center near the site of the terrorist attacks that destroyed the World Trade Center held its first exhibit Wednesday evening, the enthusiasm at the opening belying its troubled beginnings.

As a small orchestra played traditional Middle Eastern instruments, people crowded into the center, where a photo exhibit of New York children of different ethnicities lined the walls.

Sharif El-Gamal, the center's developer, said the biggest error on the project was not involving the families of 9/11 victims from the start.

"We made incredible mistakes," El-Gamal told The Associated Press in an earlier interview at his Manhattan office.

The building at 51 Park Place, two blocks from the World Trade Center site, includes a Muslim prayer space that has been open for two years. El-Gamal said the overall center is modeled after the Jewish Community Center on Manhattan's Upper West Side, where he lives.

"I wanted my daughter to learn how to swim, so I took her to the JCC," said the Brooklyn-born Muslim. "And when I walked in, I said, `Wow. This is great.'"

The project has drawn criticism from opponents who say they don't want a mosque near the site of the Sept. 11 terrorist attacks.

The center is open to all faiths and will include a 9/11 memorial, El-Gamal said. He called opposition to the center – which prompted one of the most virulent national discussions about Islam and freedom of speech and religion since Sept. 11 – part of a "campaign against Muslims."

Last year, street clashes in view of the trade center site pitted supporters against opponents of the center.

When the center was first envisioned several years ago, activist Daisy Khan and her husband, Imam Feisal Abdul Rauf, played a major, vocal role. But they soon left the project because of differences with the developer.

El-Gamal, 38, confirmed Wednesday that they parted ways because "we had a different vision." He declined to elaborate.

The couple said they had discussed plans for Park51, as the center is known, with relatives of 9/11 victims, first responders and others, including the possibility that it could become a multifaith center focusing on religious conflict. But El-Gamal wishes victims' families had been involved earlier – before the center became a point of contention.

"The biggest mistake we made was not to include 9/11 families," El-Gamal said, noting that the center's advisory board now includes at least one 9/11 family member.

An NYPD officer keeps watch at the grand opening of the Park51 community center and mosque on September 21, 2011 in New York City. The controversial Park51 plans to hold cultural and interfaith activities and is located a few blocks from the World Trade Center site in Lower Manhattan. Opponents have dubbed the property the "Gound Zero Mosque." (Photo by Mario Tama/Getty Images)

At first, "we didn't understand that we had a responsibility to discuss our private project with family members that lost loved ones," he said, and they did not "really connect" with community leaders and activists.

But today, "we're very committed to having them involved in our project. ... We're really listening," he said.

Pointing to the inclusivity of a center that critics feared would be polarizing, El-Gamal noted that the featured photographer in the "NYChildren" exhibit is Danny Goldfield, who is Jewish.

The Brooklyn photographer was inspired to create the exhibit by the story of Rana Sodhi, a Sikh who emigrated from India and settled in Arizona. His brother Balbir was killed in a retaliatory hate crime four days after Sept. 11.

Sodhi made the trip to New York for the opening and wore a tie decorated with heart-shaped American flags. He still runs the gas station where his brother was killed. "My heart is so

warm when I hear Danny is doing this exhibition in Park51," Sodhi said.

Goldfield said he has photographed children with roots in 169 countries since 2004. He hopes to find subjects representing 24 other countries to complete the project. Some of the photographs had been exhibited elsewhere, but the opening marked the first time all were shown together.

He said there was a synergy between the themes and spirit of his project and those of the center, particularly with regard to community participation and openness. "They want to build a center for everyone that's represented on the walls here," he said.

Recalling the controversy over the center, he said he didn't want to pass judgment on its opponents. But he said he'd like them to see the show "more than anyone."

Afsana Khundkar, a native of Afghanistan whose 12-year-old son, Waseem, was one of the children photographed for the

exhibit, said her family was honored to participate in the project. "It's promoting good things in the world," she said. "The most important thing is to involve the children in the good things."

The space had been cleared out and the walls painted a stark white for the exhibit. The renovations were funded with $70,000 raised on the website Kickstarter. The modest first-floor space is intended to function as a temporary center until groundbreaking on an entirely new building.

El-Gamal told the AP that fundraising is under way to complete a 15-story building that will also include an auditorium, educational programs, a

pool, a restaurant and culinary school, child care services, a sports facility, a wellness center and artist studios.

The mosque is especially needed in lower Manhattan, he said, because thousands of Muslims either work or live in the neighborhood, "and in our religion, we must pray five times a day."

At the opening, an ebullient El-Gamal told reporters the project had been framed by others throughout the debate over its existence. "Today, for the first time, everyone gets a little bit of a glimpse into the future of what Park51 is going to offer New York," he said.

Al-Qaeda in the Islamic Maghreb's Operational Revival in Northern Algeria

By Dario Cristiani
Source: http://www.jamestown.org

In the past few months, there has been a rather remarkable operational return of Al Qaeda in the

Islamic Maghreb (AQIM) in Algeria. On July 16, a double suicide attack

rocked a security compound in the small town of Bordj Menail, 60 km east of Algiers, with two people killed and 14 injured (*Algérie Plus*, Jul 16). A few days later, Algerian security forces in the area of Thénia intercepted an AQIM team alleged to be on its way to carry out an attack in Algiers (*Tout Sur l'Algérie*, Jul 26).

The most important attack occurred in late August, when another double suicide attack hit the military academy of Cherchell, about 100 km west of Algiers, killing 18 people and injuring another 20 (Algerian Press Service, August 27; *El Watan*, August 27). AQIM claimed responsibility for both attacks, blaming also the Algerian government for its support of Muammar Qaddafi (Afrik.com, July 20; AFP, August 20). An AQIM statement described the Cherchell attack as "a small gift to the families of the martyrs, the injured and the weak and subdued prisoners of Algeria, who have been suffering the worst of atrocities at the hands of France, making them subject, with metal and fire, to a criminal gang of Algerian army generals, transgressing across the land spreading much corruption. In fact, their corruption and crime even reached across the borders to neighboring countries, conspiring against the revolutions of our brothers in Tunisia and Libya" (al-Andalus Media/al-Fajr Media Center, August 27).

Following an overall decline in operations since 2008, AQIM's profile remained low in Algeria until April 2011. The causes for this were several:

- The "Sahelization" of AQIM as the geographical center of its activity shifted from Algeria to the Sahel.
- The increasing focus on illegal business activities rather than on terrorist actions.
- The consistent and effective counter-terrorist efforts of Algeria.
- The waning appeal of violence in a country that is still recovering from the psychological burden of two decades of violence.
- An internally divided and fragmented leadership, in which power is rather diffused, with its Salehian factions enjoying a strong autonomy and the formal leadership, based in Kabylia, exercising a rather loose control over the various AQIM units.

However, this situation has been changing since April. As well as the major attacks described above, there have also been strikes on individuals of the military, policemen and gendarmes, killing more than 50 people according to official sources (*Jeune Afrique,* August 5). What does this recrudescence mean and what are the reasons behind it?

- *Worsening of the Regional Security Picture*: The conflict in Libya has had a negative impact on the security of almost all its neighbors, though it was also overestimated to further national security interests and assist the survival of the political elites. Support for Mua'mmar Qaddafi was

equated with preserving regional stability, although this policy proved unsustainable in the long term. Though the regime was wary of the fact that the Algerian protests might indicate the beginning of a spillover effect from the Libyan conflict, it is clear that protests, strikes and mass rallies are constant elements of the Algerian political and social landscape. Nevertheless, the fear of a spillover effect has strongly influenced the Algerian regime's reaction to the Libyan conflict, and regional security has worsened through the spread of weapons from Libyan arsenals and ineffective control of Algeria's porous borders. The possibility that weapons and explosives have reached the country is high, and a nexus between the rising number of attacks in Algeria and the conflict in Libya can be identified.

- *The National Political Juncture*: Although Algeria's resilience to the Arab Spring has been greater than that of some other Arab countries, the protests in Algeria were still regarded as presenting a menace to the survival of the regime. Moreover, Algeria will likely experience an increase in political tension and divisions over the next few months. The major political personalities are already eyeing the 2014 presidential elections and many of them have begun creating alliances and strategies for this fundamental date (*Algérie 360*, May 20). The major party, the Front de Libération Nationale (FNL), is facing increasing internal fragmentation. Most notable of the factions to spin off from the FNL is the Mouvement de Redressement et de l'Authenticité, which is harshly critical of FNL secretary general Abdelaziz Belkhadem, one of the closest politicians to President Abdelaziz Bouteflika (*Le Journal d'Algérie*, August 15). In narrow security terms, the protests mean a greater focus by the government on

maintaining domestic political stability, hence a devotion of greater quantities of financial resources and security forces to control these protests. Subsequently, AQIM could have an interest in seizing the political momentum by exploiting this shift of focus in security on increasing its operational profile prior to destabilizing the state should the overall socio-political picture enter a precipitate decline.

- *External and Internal Symbolic Meanings*: These latest attacks could also have external and internal symbolic meanings. The external meaning encompasses the international dimension as well as a national one. Internationally, the attacks aim at showing that the group is alive even though its leader, Osama Bin Laden, has been killed. In the national dimension, they show that AQIM still has the capability to attack the most visible elements of state control -- the military installations. The internal meaning of the attacks could be a response to allegations of a decline in influence of the Algerian-based leadership over other factions of the group. Carrying out successful attacks against Algerian military installations could represent a means for AQIM Amir Abdelmalek Droukdel to boost his weakened leadership after the "Sahelization" of the movement entailed a shift in the group's internal balance of power.

Whether this acceleration in AQIM operations in Algeria will be effective in reviving the fortunes of the Algerian militants is unclear. The worsening regional picture and the increasing domestic troubles facing by the Algerian government could represent a major opportunity for AQIM to further increase its operational profile in Algeria. Internal rivalries could also push some factions to act more vigorously to reaffirm their power and influence within the organization. The ability of AQIM to return to its 2007-2008 levels of

violence in Algeria remains weak; however, it is undisputable that the strategic context in Algeria has changed slightly in favor of AQIM in the last few months.

Dario Cristiani is a PhD Candidate in Middle East and Mediterranean Studies at King's College London. Previously, he has been a teaching fellow in Political Science and Comparative Politics at the University of Naples "L'Orientale" and a political analyst with the Power and Interest News Report (PINR).

Hundreds of missiles go missing from regime's abandoned arms dumps

Source: http://www.independent.co.uk/news/world/africa/hundreds-of-missiles-go-missing-from-regimes-abandoned-arms-dumps-2351028.html

The long metal crates strewn on the grounds of the warehouse were empty. Hundreds of surface-to-air missiles, craved by terrorist groups and "rogue states", had disappeared in the past few days, looted from one of Libya's overflowing arms dumps.

Among the missiles taken away were 480 Russian-built SA-24s, designed for use against modern warplanes, which the US had been attempting to block from falling into Iranian hands, and the older SA-7s and 9s, capable of bringing down commercial airliners,

which al-Qa'ida has been striving to obtain.

As Libya's bloody civil war reaches its conclusion, myriad bunkers and barracks containing the regime's weaponry, from Kalashnikovs to missiles, armoured cars and tanks, have been left unguarded, many to be stripped bare by militia fighters and the public.

The numbers involved are far larger than the caches that armed the insurgencies in Iraq and Afghanistan. And in Libya there are even fewer guards at these sites. Unlike those two fronts of the "war on terror", there are no foreign troops present

in Libya, and the opposition forming the new government has its resources tied up attempting to subdue the remaining loyalist strongholds and repairing infrastructure to safeguard the arsenals. The ransacking of the depots containing missiles has set alarms ringing among security agencies in America and Europe. The SA-24 "Grinch" surface-to-air missile targets fighter-bombers, helicopter gunships such as Apaches, and even Cruise missiles, and can strike at as high as 11,000ft. Washington had lobbied the Russians to block sales to Hugo Chavez in Venezuela and to Tehran. The SA-7s and 9s are older but can destroy civilian jets or be used against military targets such as the drones increasingly employed by the US. Peter Bouckaert, emergencies director for Human Rights Watch, charting the arms depots, said: "The problem is pretty huge.

concerned. This lot can turn the whole of North Africa into a no-fly zone."

Nato air strikes destroyed an estimated 600 missiles, radar systems and storage facilities in the course of the campaign. In response, regime forces moved some of the weaponry away from military into civilian areas, where they could be accessed once the rebels gained control.

The missiles found to be missing yesterday had been taken from the Tripoli headquarters of the 32nd Brigade, under the command of Gaddafi's son, Khamis al-Gaddafi, to a commercial storage area. Although the missiles had gone, there were still dozens of cases of mortar rounds, artillery shells, rocket-propelled grenades and rifle ammunition left in the vast room.

Across the road, in an open field, lay piled-up boxes of anti-personnel mines, a weapon which

SA-14
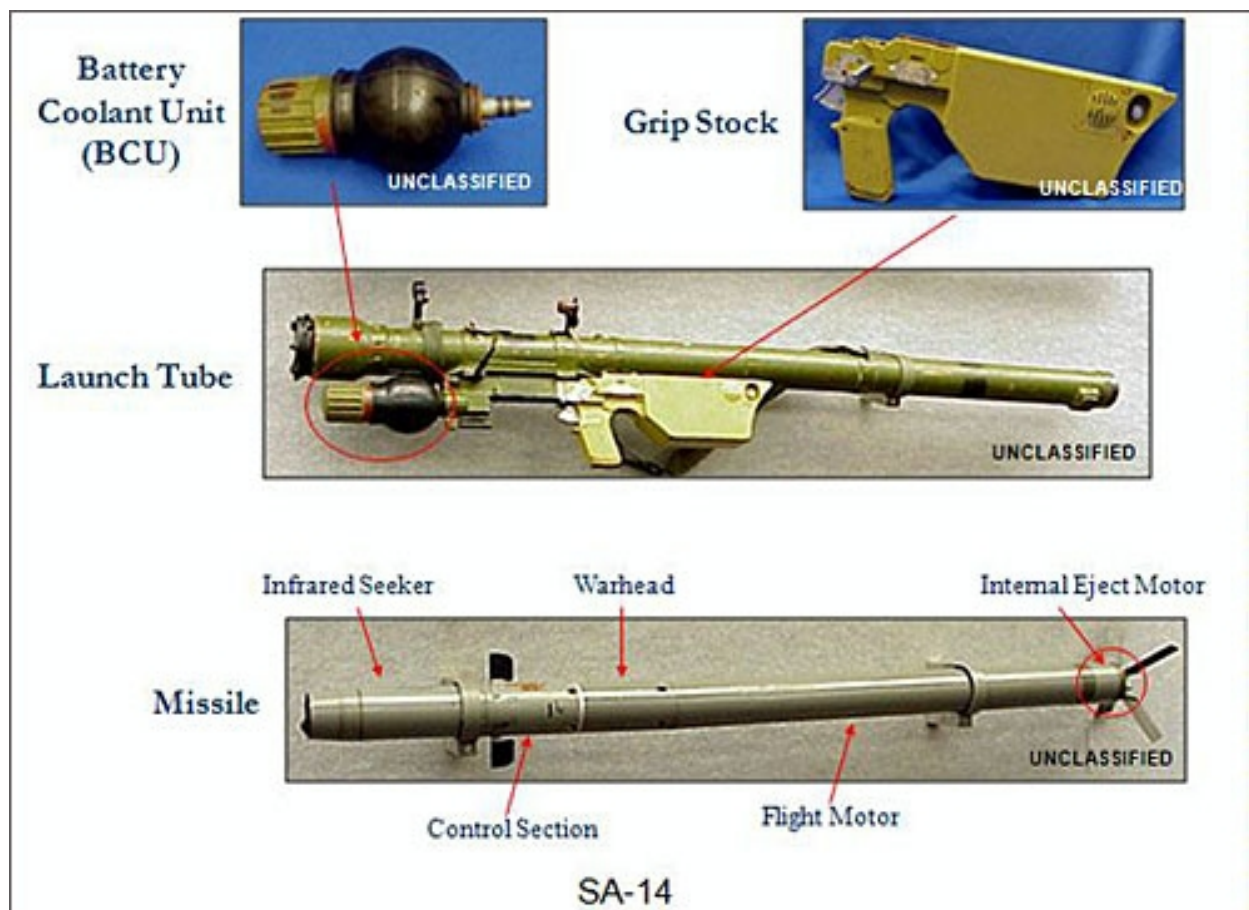
There are around 20,000 surface-to-air missiles in Libya and a hell of a lot of them are missing. The Western agencies are obviously pretty

has already caused a series of deaths, many among children, in districts where hostilities have

ended. Some 12,000 land mines were reported missing yesterday. Ian Martin, the UN's special adviser on Libya, said: "Proliferation of weapons is a major concern. We are taking this extremely seriously." Unmas (United Nations Mine Action Service) is supposed to be taking the lead on this matter but, due to security concerns, it has only one member of staff in the Libyan capital.

There is increasing evidence of arms from Libya slipping into other countries. Abdelkader Messahel, an Algerian Foreign Minister, claimed al-Qa'ida fighters are "reinforcing themselves with arms coming from Libya". The Chad government has reported that SAM-7s have arrived there from Libya, while the authorities in Niger are trying to track down consignments of Semtex, the plastic explosive once favoured by the IRA, heading for dissident Tuareg tribes.

At the town of Tarhuna, near Bani Walid, more than 100 Russian-made tanks and armoured personnel carriers are parked in hangars.

A group of armed local men had come to see whether they could make use of the armour. "These have been here for a long time," said Mahmood Ishmail Zubeidi.

"We thought maybe our villages could have our own tanks to protect the revolution. We have even got two drivers. But all the fuel has been drained. So we are going to Tripoli to get ourselves some other things like AKs [AK-47 assault rifles]. Maybe we'll get some machine guns as well."

How the Haqqani Network is Expanding From Waziristan

The Pakistani-Based Militant Group Needs a War In Afghanistan to Survive
By Michael Semple
Source: http://www.foreignaffairs.com/articles/68292/michael-semple/how-the-haqqani-network-is-expanding-from-waziristan?page=show

The looming U.S. drawdown in Afghanistan need not lead to instability. If it proceeds smartly, Washington can ensure that fewer U.S. soldiers will leave the country more secure, not less.

The recent spate of spectacular attacks in Kabul reveals as much about the struggle for supremacy within the Af-Pak insurgency itself as it does about the war between the insurgents and NATO. In the span of a single week, Afghans witnessed, first, the closing down of the center of the capital during a 20-hour siege on the U.S. Embassy, and then, exactly a week later, this past Tuesday, a political assassination: a suicide bomber packed his turban full of explosives and killed the chief of the High Peace Council, Burhanuddin Rabbani, a former president of Afghanistan.

Taliban spokesmen claimed responsibility for the Rabbani killing on Tuesday, but the group firmly denied any involvement on Wednesday. Investigations into Rabbani's death now need to establish exactly who tasked the suicide bomber;

if the Quetta-based Afghan Taliban in fact assassinated one of the group's main interlocutors, the movement cannot seriously expect to move forward as a key player in a political process. Another possible scenario exists: one in which regional spoilers who want to sustain the armed struggle are acting on their own. If the operation was run from the Pakistani tribal area of Waziristan, as some are now suggesting, the Rabbani assassination may be an operation on which the Quetta-based Taliban leadership simply was not briefed.

Think back to the attack on the embassy in Kabul. Immediately following the siege, nearly everyone pointed at the so-called Haqqani network, since the tactics used mirrored those of their previous exploits, such as the June attack on the Hotel Intercontinental and the August assault on the British Council.

Yesterday, even the Chairman of the Joint Chiefs of Staff Admiral Mike Mullen said that the Pakistani

intelligence services, or the ISI, were involved. But blaming the Haqqani network is like using a kind of militancy shorthand, as the much-used moniker fails to capture the complex nature of the politico-military organization that is expanding its scope, network, and political aspirations from a base in North Waziristan.

In fact, understanding militancy in Waziristan, especially if it served as the origin of the Rabbani assassination, is vital to charting a course for NATO's possible negotiations with the Taliban, and is unavoidable in any discussion of extricating NATO from South Asia.

Over the last two years the Haqqanis have developed what amounts to a special forces capability.

Here are the basics. Jalaluddin Haqqani was one of the leading Pashtun commanders of the jihad in Afghanistan in the 1980s. From the Zadran tribe, he is one of the few major commanders who made his peace with the Taliban, serving its government in the 1990s as a border affairs minister. The sons of the now aging Jalaluddin front the organization. Although the eldest son, Khalifa Seraj, is meant to be the senior decision-maker, his younger brother, Badruddin, is probably the family member most closely involved in the embassy siege and seems to be more active and accessible. In part, the brothers draw upon fighters from the Zadran tribe in the border provinces who were loyal to Jalaluddin during the 1980s. But the Haqqanis' lethal effectiveness derives from the wide range of Pakistani tribal fighters at their disposal. In effect, they have an unlimited supply of men for small-arms ambushes and attacks on NATO posts and administrative centers.

What is new here, and key to understanding the attack on the embassy (and perhaps even the

bombs. The Haqqanis draw on this expertise without actually controlling the groups who

Rabbani assassination), is that over the last two years the Haqqanis have developed what amounts to a special forces capability. They have built up intelligence-gathering networks and infiltrated government institutions in Kabul and the surrounding provinces. With the help of al Qaeda and Central Asian fighters, foreign militants in Waziristan have developed advanced combat training and technology for roadside

deliver it. Rather than the Haqqani Network, it would be more appropriate to call this the Waziristan Militant Complex.

Even if they outsource some of their special operations, the Haqqanis feverishly guard the one part of their operation they consider far too valuable to let out of their control: propaganda. Young fighters take

combat video courses in the North Waziristan capital of Miran Shah and then accompany their comrades on attacks to collect footage. The Haqqani video editors then splice the bloody footage with B-roll snatched from satellite channels and YouTube. The result is a library of slick jihadi videos, glorifying the fighters and martyrs, stressing the precise and devastating nature of their attacks, and lampooning the Afghan government. Some even include credits claiming to be made by the "Cultural Committee of the Islamic Emirate of Afghanistan." The Waziristan militants are projecting themselves as chiefs of the Islamic Emirate brand, which is important because they are trying to sideline, at least in the eyes of those watching, their Afghan jihadist counterparts.

Attacks such as the embassy siege speak volumes about the nature of the broader Af-Pak insurgency. The Haqqanis are boosting their political influence by taking center stage in the war. Granted, the Kandaharis in southern Afghanistan have launched their share of spectacular attacks -- such as the Sarposa prison break and the coordinated Fedayeen attacks in Kandahar City -- but in terms of impact on the public consciousness, the Haqqanis simply overshadow anything their counterparts in Kandahar have been able to pull off. Most significantly, there is no evidence that the Taliban's chief military commander, Qayyum Zakir, has anything to do with the planning and execution of this ongoing string of Waziristan-Kabul attacks. Traditionally, the Haqqani brothers have always been careful to stress that they are under the authority of Mullah Omar and the Taliban Movement. But the embassy assault suggests that that is changing.

For the moment, the war goes on, and, despite U.S. Ambassador Ryan Crocker's assertion that the embassy siege was "not a big deal," the fact is undeniable that Kabul remains as vulnerable as ever, as shown by the Rabbani assassination. Meanwhile, a more serious complication is coming into clear view. The Rabbani assassination notwithstanding, there is still a chance that the Taliban's Kandahari leadership in the south will, in the coming months, opt for a political process and negotiations. And despite their claims of allegiance, the Waziristan militants are positioning themselves as separate players in NATO's Afghanistan endgame.

If the Waziristan Militant Complex was, in fact, responsible for the Rabbani assassination, in an effort to spoil a possible political process, it is a starting pushback against the Kandahari Taliban leadership. Even within Waziristan there is a question of who runs each of the operations. Despite their origins as a marginalized border tribe, the Haqqani brothers may now be eyeing a future role on the Afghan national stage. The Haqqanis' backers in Pakistan will have to make their own decision about whether they are going to take part in a negotiated reconciliation, or if, as Washington has suggested, they will ramp up their proxy war inside Afghanistan.

The bottom line is that the militants in Waziristan depend on the jihad for their survival and thus have to oppose any settlement. After all, if there's no war in Afghanistan, they have no reason for being. But what does that mean for the future? At a minimum, NATO will have to deal with Waziristan separately from any deal made with the official Taliban leadership. As a corollary, in trying to make sense of Taliban intentions -- which is a difficult enough task in its own right -- it would be wise to regard the attacks coming out of Waziristan as a separate and distinct matter. Because as a negotiated settlement unfolds, the Waziristan Militant Complex will almost certainly be back again to sabotage it, with more spectacular attacks and the videos that always follow.

CBRNE Terrorism Newsletter – Winter 2011

Physical and Personnel Security
Source: http://www.usfa.fema.gov/fireservice/subjects/emr-isac/infograms/ig2011/39-11.shtm

In the past few days, the Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) observed that fire and police stations were attacked by gun fire. Although no one was injured, these incidents raise concern about physical and personnel security at facilities occupied by emergency responder departments and agencies.

To address this concern, the EMR-ISAC examined various sources to identify the basic measures of a time-efficient, cost-effective, and common-sense approach to bolster security in and around first responder stations. The following is a summary of preventive actions for the consideration of Emergency Services Sector leaders responsible for personnel and any type of physical location:

- Inspect randomly the security and condition of all facilities and storage areas.
- Keep all doors and windows closed and locked as much as practicable.
- Use appropriate locking systems for all station access points.
- Obtain a monitored intrusion detection system for locations not always occupied and in regular use.
- Prohibit sharing security codes or combinations with unauthorized persons.
- Change security codes or combinations at frequent intervals.
- Guarantee vehicles, apparatus, and equipment at exterior sites are always locked when unattended.
- Initiate and enforce a reliable identification system for department personnel and property.
- Screen all visitors and vendors and deny entry to anyone who refuses inspection.

- Develop inspection practices for incoming deliveries including postal packages and mail.
- Require personnel within the station to be vigilant for unauthorized persons and unusual activities.
- Prepare and enforce an SOP containing physical and personnel security measures at facilities.

For more information, see the Five Step Process and the crucial principles (deterrence, detection, delay, response, recovery, and re-assessment) at the Integrated Physical Security Handbook. Another pertinent source is the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.

National Disaster Recovery Framework
(Source: FEMA)
The Federal Emergency Management Agency (FEMA) released this week the National Disaster Recovery Framework (NDRF). This document outlines how community recovery is supported and organized on a national level. It builds on scalable, flexible, and adaptable coordinating structures to align key roles and responsibilities, while linking local, state, tribal, and federal governments, the private sector, and voluntary faith-based and community organizations that perform vital tasks in recovery.

Similar to the National Response Framework the NDRF identifies recovery support functions that have a designated federal coordinating agency to provide leadership, coordination, and oversight for state, tribal, and local communities in their recovery. The Emergency Management and Response—Information Sharing

and Analysis Center (EMR-ISAC) noted that
FETA considers the NDRF as guidance for
developing measures of successful recovery
based on the state and community's recovery
objectives, effective decision making and
coordination, and also the integration of
community recovery planning processes.

The NDRF is consistent with the vision set forth
in the Presidential Policy Directive 8 (PPD-8),
National Preparedness, which directs FEMA to
work with interagency partners to publish a
recovery framework. "The National Disaster
Recovery Framework is a first step toward the
PDD-8 objective to achieve a shared
understanding and a common, integrated
perspective across all mission areas—
Prevention, Protection, Mitigation, Response, and
Recovery—in order to achieve unity of effort and
make the most effective use of the Nation's
limited resources."

Quick Drills for Fire Department Personnel
(Source: Fire Engineering)
The Emergency Management and Response—
Information Sharing and Analysis Center (EMR-
ISAC) reviewed an article at Fire Engineering
regarding the efforts by chief officers to lead,
train, and develop company officers and crew
members. The author, Battalion Chief Steve
Prziborowski of the Santa Clara County (CA) Fire
Department, proposed that personnel look to
their chief officers for leadership, guidance,
direction, training, and support.
In his article, Chief Prziborowski maintained that
the top priority is "to ensure firefighters go home
safely at the end of their shift and that they are
trained and prepared for the worst-case
scenario." He advised that chief officers, who are
burdened with numerous administrative projects,
should be very creative when training and
developing their crews, and have some realistic
quick drills from which to select.

The author offered twelve quick drills a chief
officer can use "to inspire personnel to be the
best they can be and to ensure they are prepared
to do their job when the bell goes off." The first
five of the quick drills are summarized as
follows:

- Turnout drill. Prepare for the worst-
  case scenario by striving to have a
  turnout time of less than 60 seconds.
  This refers to the time it takes for the
  apparatus to start moving toward the
  incident after the alarm has sounded.
- Portable master stream operation.
  Inform crew members that they are
  dispatched to a structure fire and
  direct them to put their portable
  master stream (e.g., deck gun) into
  operation. Conduct rehearsals on
  how to get it off the apparatus, pull
  the appropriate amount and size of
  hose, and secure it to the ground in
  a quick and safe manner.
- Large-handline operation. Instruct
  the crew to practice putting a 2½-
  inch handline into operation to
  accommodate the "big water."
- Pre-incident planning. Bring the crew
  to their first-due area for building and
  site familiarization. Direct the first-
  due officer to lead a facility tour and
  discuss the necessary strategy and
  tactics to combat a fire should one
  occur.
- Drill tower training. Take the drill
  tower training off site and use large
  parking lots or structures to make the
  training more realistic.

Seven more recommended quick drills can be
seen in pages 4 and 5 of Chief Prziborowski's
article at Fire Engineering.

NYPD probably couldn't take down a jetliner, key police source says

CBRNE Terrorism Newsletter – Winter 2011

Source:http://www.nydailynews.com/news/ny_crime/2011/09/27/2011-09-27_plane_speaking_unlikely_big_jets_on _nypd_hit_list.html?r=news/ny_crime

Police Commissioner Raymond Kelly, in a "60 Minutes" interview Sunday, answered in the affirmative when asked if the "NYPD has the means to take down an aircraft."

"I prefer not to get into the details, but obviously this would be in a very extreme situation," Kelly answered.

There was speculation he meant a jetliner, like the ones that took down the twin towers. The source suggested that's not the case.

The Daily News first reported the revamping of the NYPD's aviation fleet in 2005.

The source confirmed that what the paper reported then still holds: The city has Agusta 119 helicopters armed with .50-caliber semiautomatic rifles that

The NYPD has enough firepower to bring down a crop duster but probably not a jet airliner, a key police source says.

"It's not surface to air missiles or a weapon that has rockets," the source said Monday.

Instead, the city's air defenses are calibrated to take down a much more modest target.

"What was envisioned was a small aircraft ... coming down the Hudson," the source said. "Al Qaeda was talking about targeting the West using crop dusters. There was a specific concern about using this type of aerial spraying of anthrax and some other biological chemicals. That also led to plans to equip our aircraft."

could blast moving boats, planes or tractor-trailers from hundreds of yards away.

Mayor Bloomberg said the NYPD has other capabilities specifically designed to derail an aerial terror attack: "The New York City Police Department has lots of capabilities that you don't know about and won't know about," he said.

U.S. military and government officials declined comment on whether the NYPD has the authority to blast planes from the sky, but Rep. Pete King (R-L.I.) said what the NYPD has is "absolutely essential." "Local law enforcement has to provide national defense, and that started on Sept. 11," King said.

London 2012: More than one security alert every day at Olympic Park

Source: http://www.mirror.co.uk/news/top-stories/2011/09/29/london-2012-more-than-one-security-alert-every-day-at-olympic-park-115875-23453137/#ixzz1ZPtovQxs
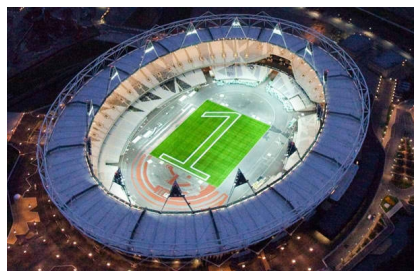
MORE than 1,000 security passes to the 2012 Olympic Park and athletes' village have been lost or stolen so far this year.

During the same period there have been 357 security alerts at the two venues – more than one a day. The Olympic Delivery Authority said passes are immediately

CBRNE Terrorism Newsletter – Winter 2011

de-activated when they are reported missing or stolen and special controls mean they would have to match hand prints to grant access. It refused to give a more detailed response to the Freedom of Information request on safety grounds. The ODA said: "Disclosure of details of security alerts which have occurred at the Olympic site could assist the preparation of hostile action before or after the Games." The Games face several potential terror threats – from al-Qaeda to dissident Irish nationalists and anarchists.

Making a Point about Lasers

Illegal Use of Devices a Serious Crime
Source:http://www.fbi.gov/news/stories/2011/september/laser_092611/laser_092611?utm_campaign=email -Immediate&utm_medium=email&utm_source=fbi-top-stories&utm_content=33788

Justin Stouder was aiming a laser pointer at a distant tower from his suburban St. Louis yard one April evening in 2010 when a police helicopter appeared in his line of sight more than a mile away.

At the time, the 24-year-old had no idea that his decision to point the laser at the helicopter was a federal felony—or that the beam of light might have serious consequences for the pilot and his crew. "It's equivalent to a flash of a camera if you were in a pitch black car at night," said St. Louis Metropolitan Police Officer Doug Reinholz, the pilot on patrol that night when Stouder's green hand-held laser "painted" his cockpit. "It's a temporary blinding to the pilot," he said during a recent news conference highlighting the danger of lasers directed at airplanes and helicopters.

Interfering with the operation of an aircraft is a crime punishable by a maximum of 20 years in prison and a $250,000 fine, and laser incidents are on the rise. Since the FBI and Federal Aviation Administration (FAA) began keeping records of laser events in 2004,

"there has been an exponential increase every year," said Tim Childs from the Federal Air Marshal Service, who serves as a liaison officer with the Bureau on laser issues.

In 2009, there were 1,489 laser events logged with the FAA—that is, pilots reporting that their cockpits were illuminated by the devices. The following year, that figure had nearly doubled to 2,836, an average of more than seven incidents every day of the year. And the overwhelming number of the incidents involved green lasers—especially dangerous because the human eye is most susceptible to damage from the yellow-green light spectrum.

Hand-held lasers—about the size of fountain pens—are used legitimately by astronomy hobbyists and in industrial applications. Anyone can purchase one, and technology has made them inexpensive and more powerful. Lasers costing as little as $1 can have ranges of two miles— strong enough to target a variety of aircraft.

And what appears as a dot of light on the ground can illuminate an entire cockpit, disorienting a pilot or causing temporarily blindness. That's because the farther the beam travels the more spread out it becomes. "At 500 feet," Childs said, "that two-centimeter dot you see on your wall can be six feet wide." To date, no aircraft have been lost as a result of laser incidents, he added, but there have been eye injuries, and perpetrators have gone to jail.

Those responsible for "lasering" aircraft fit two general profiles, Childs explained. "Consistently, it's either minors with no criminal history or older men with criminal records." The teens are usually curious or fall victim to peer pressure, Childs said. The older men simply have a reckless disregard for the safety of others. There are also intentional acts of laser pointing by human traffickers or drug runners seeking to thwart airborne surveillance, Childs added.

As for Justin Stouder, the helicopter pilot he lasered helped guide police to his house, where he was arrested minutes after the incident. "I had no idea it illuminated the whole cockpit and blinded everybody inside," Stouder said during the news conference. He offered a public apology and volunteered to tell his story in the hopes of educating the public about the dangers of laser pointing. "It was really a selfish mistake," he said of his actions.

NOTE: Watch the video available in the source's URL.

A GREAT IDEA

Connecticut town considers charging centers for power outa

Source: http://www.mywesthartfordlife.com/news.php?cid=2&id=723

Following Hurricane Irene which left thousands without power up and down the East Coast, a town in Connecticut is considering building several **charging stations for residents to power up their hand held electronics** during a natural disaster or prolonged power outage

Global Islamic group rising in Asia

Source: http://www.thejakartapost.com/news/2011/10/01/global-islamic-group-rising-asia.html

The chanting crowd at the radical Muslim protest in Indonesia stood out for its normalcy: smartly dressed businessmen, engineers, lawyers, smiling mothers, scampering children.
At a time when al-Qaida seems to be faltering, the recruitment of such an educated, somewhat mainstream following is raising fears that Hizbut Tahrir, an enigmatic global movement, could prove more effective at radicalizing the Islamic world than outright terrorist groups.
Active in 45 countries, Hizbut is now expanding in Asia, spreading its radical message from Indonesia to China. It wants to unite **all Muslim countries** in a globe-spanning bloc ruled by strict **sharia law**. It targets **university students and professionals**, working within countries to try to persuade people to overthrow their governments.

The movement's appeal to an often influential conveyer belt to terrorism," in the words of Zeyno

وَلْتَكُن مِّنكُمْ أُمَّةٌ يَدْعُونَ إِلَى الْخَيْرِ وَيَأْمُرُونَ بِالْمَعْرُوفِ وَيَنْهَوْنَ عَنِ الْمُنكَرِ وَأُوْلَـئِكَ هُمُ الْمُفْلِحُونَ
"Let there be among you a group that invites to the good, orders what is right and forbids what is evil, and they are those who are successful." [TMQ 3:104]

حزب التحرير
Hizb ut Tahrir

English | Forum   المنتدى | العربية

part of society worries experts. Its goal of an Islamic state may be far-fetched, but it could still undercut efforts to control extremism and develop democracy in countries such as Indonesia, which the U.S. hopes will be a vital regional partner and a global model for moderate Islam.

"Our grand plan over the next five to 10 years is to reinforce the people's lack of trust and hope in the regime," said Rochmat Labib, the group's Indonesia chairman in a rare interview with a Western reporter. "That's what we are doing now: converting people from democracy, secularism and capitalism to Islamic ideology."

Hizbut Tahrir, which means The Party of Liberation, is also raising its profile in the U.S. after operating largely underground since the 1990s. Its first major event was a 2009 conference, followed by another one in Chicago this June.

Starkly conflicting views swirl around Hizbut. It has been described as both a peaceful movement to restore one-time Islamic glory and a breeding ground for future suicide bombers, "a

Baran, an expert on Islam in the modern world.
Banned in most countries, Hizbut remains legal in others, including the United States, Great Britain, Australia and Indonesia, where its leaders say it has spread to all 33 provinces. It is closely monitored everywhere, and often operates on the knife-edge of legality.

"The rhetoric they have goes to the fringe of democracy," said Hans Joergen Bonnichsen, the former head of Denmark's intelligence service. But the Danish Justice Ministry has twice asked the nation's top prosecutor if Hizbut could be banned under Danish law, and both times the answer was no.

Its new frontier in Asia ranges from Indonesia and neighboring Malaysia to Pakistan and China, where Beijing has accused it of inciting violence among Muslim Uighurs in the remote west. It has also become the most widespread, and persecuted, radical Muslim group in Central Asia.

The Indonesia chapter is believed to be the largest, with a following estimated in the hundreds

of thousands, according to Sidney Jones, an expert on Islam in Southeast Asia. "They are a real force here. They are a greater long-term threat to Indonesia than people who use violence," said Jones, a Jakarta-based analyst with the International Crisis Group think tank. "Collectively, hardline civil society can have a bigger effect than jihadists and terrorists."

Her words are echoed by anti-terrorism expert Zhang Jiadong of China's Fudan University, who said **Hizbut is "more harmful than terrorist organizations, because it has more influence on ordinary people."** The group, estimated at up to **20,000 members in China**, is more likely to foment riots or rebellions than terrorist attacks, he said.

Ismail Yusanto, the group's urbane spokesman in Indonesia, insists that "we area peaceful Islamic movement."

"We believe people can be influenced by their environment, so so-called terrorists could be influenced by everyone, not just us. But Hizbut itself is committed to not being violent. There is no evidence," he says, when asked whether some adherents later veer to violence.

The claims of nonviolence contrast with the movement's fiery rhetoric, which calls for the annihilation of Israel - that's what led to it being outlawed in Germany in 2003 - and exhorts Muslims to fight coalition forces in Iraq and Afghanistan. One flyer shows a decapitated Statue of Liberty with New York City aflame in the background.

The U.S. State Department says the group "may indirectly generate support for terrorism but there is no evidence that it has committed any acts of terrorism."

Hizbut followers may later "graduate" to terror under the tutelage of other groups. Often cited are the first British suicide bombers, Asif Hanif and Omar Khan Sharif, who attacked a Tel Aviv bar in 2001 and had past Hizbut links.

Reports have also linked Hizbut to Khalid Sheikh Mohammed, the Sept. 11 mastermind, and Abu Musab al-Zarqawi, the former al-Qaida chief in Iraq, but they have never been proven.

Hizbut calls for the establishment of a caliphate, uniting all Muslim nations under centralized Islamic rule in emulation of such entities that flourished in the past.

This is to be attained by changing Muslim mindsets to think beyond national borders, then pressing the message among political leaders, the armed forces and other power brokers until governments crumble.

Taquiddin an-Nabhani, a Palestinian lawyer who

founded the movement in 1953, didn't rule out violence during the last stage of creating the caliphate, or the possibility of fighting Western nations to protect it or expand it into non-Muslim countries. In earlier days, Hizbut staged failed coups in Jordan, Syria and Egypt, and it is now largely banned in the Middle East.

In Indonesia, Jones said, Hizbut appeals to those who believe that neither the country's earlier dictatorship or present democracy has worked.

She said it has been able to infiltrate the top cleric body, the Indonesian Ulema Council, and local governments and exercises some clout on issues such as introducing sharia law, banning non-mainstream Muslim sects and opposing the operations of Western companies in Indonesia.

Unlike many Islamist groups, it welcomes women, who make up about a third of the membership, according to Ratu Erma, the head of its women's organization. It also enjoys a following among parts of the elite.

"Some of them work by day in Jakarta's main business district making the wheels of capitalism turn and after work talk about

overthrowing the country's infidel system. It's one of the conundrums about the HT," says Greg Fealy, an Indonesia expert at Australian National University who is adamant that at least in Indonesia the group is nonviolent.

In Malaysia, young hard-liners disillusioned with the moderating stances of mainstream political parties have turned to Hizbut because "they feel it is sticking to Islamic principles more closely," said Mohamed Nawab Mohamed Osman of Singapore's Nanyang Technological University.

Nawab, an expert on the group in Asia, said that Hizbut, which barely filled a meeting room in Malaysia in 2004, recently drew more than 1,000 to a conference and is present in every state but one.

Leaders and followers interviewed in both countries dodge questions about their numbers and inner workings, even the whereabouts of the current global leader, Ata Khalil Abu-Rashta, except to say he is based in the Middle East.

Behind its public face, Hizbut is built along Marxist-Leninst lines with secretive cells as key building blocks. Nawab says "students" may go through up to five years of arduous training and indoctrination to prove their commitment and become members. Some 60 percent don't make the grade.

Hizbut members have been imprisoned in Russia, Central Asian nations and elsewhere, but some experts say the broad definition of terrorism in these countries - rather than any acts committed - landed many of them in jail, and sometimes before execution squads.

Within the U.S., opinion is divided. **The State Department doesn't name Hizbut as a terrorist group**, but the New York City Police Department, in a document obtained by The Associated Press, identified it as a "tier one extremist group" in 2006.

The British government came close to banning the group after the 2005 London bombings, and government officials say membership has shrunk to fewer than 2,000 members. But Britain remains an important base for fundraising, propaganda efforts and recruiting senior members. Many leaders in Indonesia and Malaysia were once asylum seekers in the U.K. who got an education and made connections and then returned home.

Ed Husain, who described his time as a British member in the 2007 book "The Islamist," said that globally the movement is "strong, robust, growing."

"I still believe that the message and ideology of Hizbut Tahrir is as potent as ever," he said in an interview.

"Their antidemocratic, anti-West, anti-Israel and anti-Muslim governments stance remains firm. As such, they implant confrontational, radical ideas and thus attitudes among young Muslims."

EDITOR: The new al-Qaeda?

Anwar al-Awlaki killed in Yemen by U.S. drone

Source: http://www.homelandsecuritynewswire.com/anwar-al-awlaki-killed-yemen-us-drone

Anwar al-Awlaki, the 40-year, old New Mexico-born firebrand jihadist preacher was killed last night by a missile fired from a UAV operated by the U.S. Joint Special Operations Command (JSOC); he is the most prominent al Qaeda figure to be killed since bin Laden's death in May; in April 2010 President Barack Obama approved al Awlaki's targeted killing; this was a first such order for the targeted assassination of an

American citizen, and as such required special approval from the White House

Anwar al-Awlaki, the 40-year, old New Mexico-born firebrand jihadist preacher was killed last night by a missile fired from a UAV operated by the U.S. Joint Special Operations Command (JSOC). He is the most prominent al Qaeda figure to be killed since bin Laden's death in May. He was killed in a car which was driving on a road about five miles from the town of Khashef, some eighty-seven miles from the capital Sanaa. Another American militant, Samir Khan, who produced "Inspire," an English-language al Qaeda Web magazine, was also killed in the strike, along with several body guards.

The Telegraph quotes U.S. officials to say that al-Awlaki was implicated in several terrorist attacks:

- He is believed to have played a significant role in the Christmas 2009 Detroit airline bomb attempt
- The actions of Army psychiatrist Maj. Nidal Hasan, who is charged with thirteen counts of premeditated murder and thirty-two counts of attempted premeditated murder in the attack at Fort Hood, Texas.
- In New York, Faisal Shazad, the Pakistani-American man who pleaded guilty to the May 2010 Times Square car bombing attempt said he was "inspired" by al-Awlaki after making contact over the Internet.
- Al-Awlaki also is believed to have had a hand in mail bombs addressed to Chicago-area synagogues, packages intercepted in Dubai and Europe in October 2010.
- U.S. intelligence sources also have evidence that he had sought to use poisons including cyanide and ricin in attacks.

Ben Venzke of the the Alexandria, Virginia-based private intelligence monitoring firm IntelCenter told the Telegraph that al-Awlaki's death "will especially impact the group's ability to recruit, inspire and raise funds as al-Awlaki's influence and ability to connect to a broad demographic of potential supporters was unprecedented." Venzke said, though, that the terror group al Qaeda in the Arab Peninsula will remain the most dangerous regional arm "both in its region and for the direct threat it poses to the United States following three recent failed attacks," with its leader Nasir al-Wahayshi still at large.

Al Qaeda infighting led to Awkali killing in Yemen. Ayman Zawhiri is in Yemen

Source: http://www.debka.com/article/21350/

The tip-off which enabled two American drone-borne Hellfire missiles to kill the US-born Anwar al-Awkali by locating his convoy in the Khashef in the Jawf province of Yemen, 140 kilometers east of the capital Sanaa, reached US intelligence as a result of a power struggle within Al Qaeda's leadership in Yemen.

Killed too was a second US-born al Qaeda operative.

debkafile's counter-terror sources disclose that the internal strife which led to their deaths was sharpened by the recent arrival in Yemen of the new Al Qaeda leader Ayman Zuwahiri.

Exactly when he arrived and by what route is not known. Zuwahiri is thought to have come to check out Yemen as his next permanent base in view of his plans for transposing al Qaeda's center of operations from the

Pakistani-Afghan arena to the Middle East, North Africa and the Sahara.

In North Africa, the Al Qaeda leader has learned that the Muslim extremists fighting in Libya's National Transitional Council ranks against Muammar Qaddafi have cemented their control not just of Tripoli, the capital, but also of Tobruk near the Egyptian border. debkafile's counter-terror sources report that those Islamists, while pretending to defer to the NTC, in fact deny its officials access to the key Libyan cities under their fists.

This is the first time that military forces linked to Al Qaeda have attained control of major Mediterranean ports and the use of a military airfield.

In Yemen, the situation is not very different from Libya. Al Qaeda has seized large parts of Abyan Province in the south and is fighting in sections of the Red Sea port of Aden.

Tuesday, Sept. 27, an Al Qaeda suicide bomber managed to maneuver a car loaded with explosives right up to the convoy of Yemeni defense minister Mohamed Nasser Ali. The minister survived the blast but several of his bodyguards did not.

If Yemen's central government in Sanaa continues to disintegrate, there will be nothing to stop Al Qaeda from grabbing all of Aden Port as well as Abyan and Hadramauth. Even without control of the big port city, the jihadis are within easy reach of anchorages along the Gulf of Aden coast with free access to the Red Sea, the Indian Ocean and the Persian Gulf. Intelligence experts suspect Zuwahiri may have been spirited into Yemen through one of those anchorages from a boat which brought him from Pakistan. He arrived with big plans and new ambitions: One is to expand Al Qaeda's control of South Yemen in conformity with his quest for new strongholds with access to the sea. Its bastions in

Afghanistan and Pakistani Waziristan were landlocked and without an airfield.

But over and above this strategic push, neither Zawahiri nor Osama Bin Laden, who was killed by US commandos in Abbottabad, Pakistan, on May 2, ever completely trusted Anwar al Awakli.

Although US President Barack Obama lauded the death of "the leader of external operations" of Al Qaeda in the Arabian Peninsula, AQAP, Bin Laden and his successor never let him have this title – or even command of the Yemen sector - despite his pleas. Neither was ready to countenance an American whom they didn't entirely trust in a position of high command in their organization

Awakli made his name in the West as a skilled and powerful spokesman for al Qaeda's cause. He never distinguished himself as an operational commander. Therefore, our counter-terror experts have always been wary of attributing to him personally the failed attempt to blow up a US airliner on Christmas 2009 and the planting of a bomb aboard a cargo plane in October 2010. He was certainly linked to the Palestinian US Major Nidal Malik Hassan's murder of 13 US military and security personnel at Ford Hood in November 2009, although more likely by inspiration than specific directives. The second American who died in the US drone-borne missile strike Friday was Samir Khan, editor of Al Qaeda's English-language Inspire Magazine.

From the point of view of the West, Al Qaeda has lost two senior operatives. But to hardline Zuwahiri, Al Qaeda in Yemen has been purged of its American module. Therefore, while the US justly celebrates a major victory in its war on the Islamist terrorist organization, its new leader most probably decided to sacrifice his two American assets for the sake of tightening the ranks of AQAP and drawing a denser curtain of secrecy than ever before over his next steps.

The Inside Story Behind the Awlaki Assassination
By Steven Emerson
Source: http://www.steveemerson.com/10435/awlaki-assassination

Anwar Al Awlaki, killed Friday morning (Sept, 30), in an American strike in Yemen, has been on the U.S. radar for several years, ever since, as one U.S. official stated, he turned from "inspirational to operational." He was believed to be behind the Nigerian "underwear" bomber who tried to ignite his explosives planted on his body as his airplane was landing in Detroit. And he was believed responsible for the cargo bomb plot targeting the United States last fall.

U.S. intelligence officials, aware of other planned attacks, had arrested several Muslim American converts who returned here after "studying" in the Sudan. Most of their time was spent on terrorist training and learning from Awlaki and his advisors about the precepts of jihad and Islam. Intelligence officials believe that "hundreds" of American and European converts to Islam, along with other indigenous Muslims from Islamic countries, have trained with Awlaki, making many of them "ticking time bombs."

Awlaki lived in the southern Yemen province of Shabwa, an area beyond the reach of Yemen's military and central government. Much of Yemen is like the Wild West, with no central governing authority. The numerous tribes settle disputes among themselves. Awlaki came from the Awalik tribe.

Intelligence gathered last year from Yemeni authorities and from debriefings with several American converts who returned to the United States after training with Awlaki, helped narrow Awlaki's location to a 100 square mile area. He moved at night, often in convoys of armored SUVs in order to prevent U.S. drones and surveillance from determining which vehicle he was in. But the drones, which have advanced in the ability to recognize faces on the ground, hovered above the area where Awlaki was believed to be. Electronic intelligence – including telephone intercepts –also were used, although Awlaki was said to be careful in limiting his use of electronic communication, aware that he could be tracked that way.

In the past several months, American drone operators were confident they had identified Awlaki as he moved from among a series of underground bunkers. An initial drone missile targeting him was fired at an al-Qaida training camp but missed him.

Meanwhile, U.S. intelligence and law enforcement agents collected as much personal data about Awlaki as they could from his extended family living in western countries. For example, he had an ex-wife living in Ireland that no one knew about until a close relative living in the United States identified the family tree for agents in early January. The relative proved to be a goldmine of information about Awlaki's siblings, parents, wives, and children.

Intelligence officials learned about the American relative in January through other Yemeni expatriates living here who knew her. She agreed to cooperate and provided extensive information about close relatives living either with him, elsewhere in Yemen, or in different parts of the world. Telephone numbers belonging to a close relative living in Yemen's capital Sanaa that the American relative provided to U.S. intelligence officials proved the most critical.

The relative knew that Awlaki called that number. The National Security Agency (NSA) quickly was able to triangulate the phone numbers and determine almost exactly where Awlaki was when he called the Sanaa number. The American relative also provided information on other Awlaki relatives who apparently had direct contact with Awlaki, either through email or other electronic means. That knowledge helped track other communication and confirm Awlaki's whereabouts.

Up to a dozen additional drones were dispatched to the southern part of Yemen in a search for the exact coordinates of Awlaki's location. Drone operators felt that Awlaki was most vulnerable during the day whenever he was outside moving from one hideout to another. Officials also had recruited Yemeni informants to pose as Awlaki students to try to provide intelligence on Awlaki's location. But the drones, which could not be seen by the naked eye, hovered nonstop in a massive effort to cover large parts of southern Yemen and ensure that

Awlaki had not left. He knew the United States wanted to assassinate him, as evidenced by the lawsuit brought by his father, Nasser Al-Awlaki—a U.S. citizen living in Yemen. The suit challenged the legality of a presidential order to kill Awlaki, an American citizen, without due process.

In the last month, drone operators became convinced they had identified Awlaki in various convoys. Previous strikes were considered but withheld out of concern of causing too many civilian casualties. Although the Yemen central government claims that it was in charge of the operation, the reality is that the United States acted independently.

A recent intelligence tip indicated that Awlaki was going to be traveling Thursday or Friday in a multi-SUV convoy. By early Friday afternoon Yemen time, the drones had clearly identified Awlaki's convoy—which apparently was distinct from other traveling cars in the poor region of his province—providing a clear video to drone operators in Virginia. President Obama had already given the orders to kill Awlaki if a clear shot was available.

The president was notified on Thursday about Awlaki's expected travel via convoy and that drone operators likely would have a clear shot at him. The president authorized the strike and was joined overnight by aides to monitor the video that was beamed from the drones. At one point, believed to be around 4 a.m. in Washington, the drones broadcast images of Awlaki's convoy traveling openly and without any cloud cover. Several missiles were fired. At least two of the vehicles were destroyed. Within hours, Yemen's military has secured the area and taken DNA samples from several of the remains of the bodies in the decimated vehicles. The samples were flown to Washington this morning and matched with Awlaki's relatives living here.

One source offered a slightly different version of events, saying that the relatives' DNA samples were within the U.S. Embassy in Yemen. In either case, forensic scientists compared the DNA samples and confirmed the match.

In addition, two other top lieutenants to Awlaki were also killed. One was Samir Khan, also an American, but the name of the other top assistant could not be obtained.

There was jubilation at the CIA, the Pentagon and the White House as the leading global al-Qaida recruiter had finally joined his mentor, Osama bin Laden. The FBI and Department of Homeland Security issued a warning to field offices around the country to be on guard against any revenge attacks. The charismatic English speaker and leader of al-Qaeda in the Arabian Peninsula had been eliminated.

COUNTER
TERROR EXPO
25-26 April 2012
Olympia London
www.counterterrorexpo.com

See what's
new for 2012

POLICE

FIRE & RESCUE
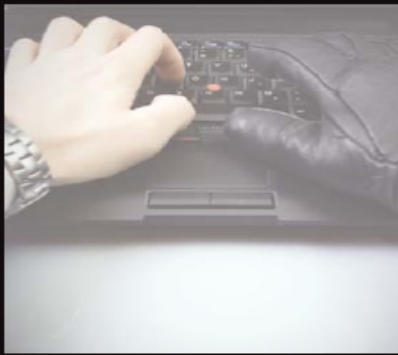
SECURITY

Clarion Defence and Security Exhibition Portfolio

COUNTER TERROR EXPO   COUNTER TERROR EXPO   DSEI   FIRE & RESCUE MIDDLE EAST   ITEC   LAAD DEFENCE & SECURITY   LAAD SECURITY   UDT

Mitigating terror threats is a critical priority for civil, military and private sector stakeholders.

Counter Terror Expo is the premier international event delivering buyers and specifiers from across the world within Government, Military, Law Enforcement, Emergency Services, Private Sector and the Security Services. This market leading event hosts the most comprehensive showcase of technology, equipment and services designed to protect nations, borders, crowded places, national infrastructure, companies, assets and individuals from the threat of terrorist attack.

The event has been established to deliver a unique and secure environment in which a dedicated audience of security professionals and leading experts within the critically important counter-terror and crisis management arena can come together to buy products, share experience and gain knowledge.

One of the fastest growing events in the UK, the 2011 event featured 400 market leading exhibitors and delivered:

7745 Attendees from

79 countries

7042 Visitors to the exhibition

637 Conference Delegates

66 Members of the press

Visitor Demographics

GEOGRAPHICAL
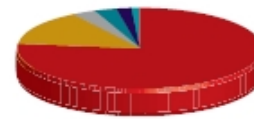
■ UK & Ireland	77%
■ West Europe	14%
■ East Europe	3%
■ Middle East	3%
■ Americas / Canada	2%
■ Rest of World	1%

BY SECTOR

■ Private Sector Organisation / Corporate Company	22%
■ Police & Law Enforcement	13%
■ MOD / Intelligence Services / Armed Forces	11%
■ Building & Facilities Protection	10%
■ Emergency Response	8%
■ Training / Consultancy	7%
■ Systems Integrators / Installers	7%
■ Transportation Security	3%
■ Critical National Infrastructure	3%
■ Central, Regional & Local Government	2%
■ Border Control / Customs & Immigration	1%
■ Other	13%

DECISION MAKING POWER
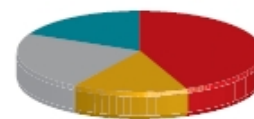
■ Yes	44%
■ No	15%
■ If no, do you influence purchasing decisions?	23%
■ Not Specified	18%

67% of the attendees to CTX 2011 were a buyer or specifier of equipment and services

ANNUAL SPEND

■ Over £1 Million	9%
■ £100k - £1 Million	14%
■ £10k - £100K	22%
■ £0K - £10K	21%
■ Not Specified	34%

" Spending on counter-terrorism will remain high, with over £2 billion set aside for counter-terrorism policing alone in the next four years. In several areas we will have to develop new capabilities in response to the technology and techniques that the terrorists are now deploying against us. "

THERESA MAY
HOME SECRETARY
3 November 2010

The 2011 attendees
Primary Product Areas of Interest

* multiple interest response

CCTV and Covert Surveillance Equipment	3904
Access Control / Biometrics / ID Solutions	3220
Perimeter Security and Intrusion Detection	2933
Information and Communication Systems	2748
Location Monitoring and Tracking Systems	2407
Personal Protection Equipment / Clothing and Body Armour	2247
Systems Integration	2071
Screening & Scanning Equipment	2099
Barriers / Bollards / Gates / Turnstiles	2049
Emergency Response Equipment	1945
CBRNE Detection and Protection	1621
Sighting and Image Recording and Processing	1794
Explosive Ordnance Disposal / Improvised Explosive Device Disposal	1619
Blast Containment	1540
Human Resources and Training	1681
Electro Optics	1384
ANPR Software & Hardware	1327
Database Management Solutions	285
Seals / Tamper Evident	981
Canine Services	612

* Source: EAS Accredit

Targeted Buyer &
Specifier Delivery Campaigns

UK VISITOR PROGRAMME FOR KEY CT AUDIENCE GROUPS:
- Police
- Fire Brigade
- MOD & Government Agencies
- Government & Private Sector

INTERNATIONAL VISITOR PROGRAMME:
- Critical Infrastructure
- Corporate Organisations
- Paramilitary

DSEi VISITOR PROGRAMMES FOR KEY CROSS OVER AUDIENCE GROUPS:
- Special Operations
- Homeland Security
- Civil Defence

In association with

DSE

MEET THE VIP BUYER PROGRAMME:
- Face to Face Private Meetings
- Buyer & Seller matched based on requirement and capability
- Meet buyers with active purchasing requirements of up to £15 million

For more information on the CTX attendee profile and areas of interest call the team on
+ 44 (0) 208 542 9090 or
email info@niche-events.com

New Product Features

ARMOURED VEHICLE ZONE

In association with **DSE**

Armoured vehicles offer crucial protection to the services of Homeland Security, Counter Terrorism, Police Security, Force Protection and SWAT teams as well as protecting key personnel in more volatile areas of the world. Aimed specifically at fleet buyers and specificers from Police, Military, Tactical, Special Ops and Private Security, this area will:
- Feature a dedicated Armoured Vehicle Zone within the Exhibition Hall
- Highlight Armoured Vehicle Solution Suppliers throughout the show
- Showcase Retro-fit, Up-armouring & Upgrade Solutions

CCTV FOCUS

CCTV is critical in assessing whether a security alert is real, and is often vital in any post incident investigation, particularly of a terrorist nature. Designed to raise the profile of high-end CCTV and Surveillance solutions, and aimed specifically at end users as well as Integrators, the CCTV Focus within the show will feature:
- A dedicated CCTV Integrators Lounge on the show floor
- CCTV Workshop to debate IP, Storage, Video Analytics and more
- Plus an update from ONVIF's Chairman

CBRN AND PROTECTIVE CLOTHING & EQUIPMENT SHOWCASE

High quality CBRN and PPE is often the difference between life and death, and in counter terror operations, success and failure. The showcase will specifically target Police, MoD, Private Security, Emergency Services, EOD and Hazmat Teams with:
- A Live Runway within the Exhibition Hall to show off the latest manufacturer ranges for 2012
- Set against a large video screen backdrop to allow buyers a better view of the products
- Narrated live by a Presenter to highlight each products unique benefits

IEDD DEMONSTRATION THEATRE

Perhaps the most common and widely used weapons of the terrorist are Improvised Explosive Devices (IEDs). This feature was one of the most popular events for the 2011 show targeted specifically at EOD Regiments, Police Disposal, Fire, Military and Special Ops Teams, and for 2012 we are expanding and enhancing it to cover:
- ROV (Remote Operated Vehicle) Demonstrations
- NEW Ancillary Equipment Demonstration Theatre
- Active scenario based IED disposals before a live audience

SMALL ARMS & LIGHT WEAPONS

In association with **DSE**

Provide close-quarter protection for a myriad of tasks including high risk policing, counter terrorist response and resolving siege and hostage situations. Small arms and light weapons have Increasing relevance to Tactical Ops, Police Firearm Units, SWAT, Private Security & Close Protection who will be targeted for the show by providing:
- On-Site Armoury
- The ability to display weapons on stands
- Increased number of weapons suppliers within the show

ACCESS CONTROL FEATURE

Gaining access to a building or facility, especially critical areas within the facility, is sometimes all the terrorist needs to successfully carry out an attack. Securing these access points is therefore one of the highest priorities. Targeted at Integrators and End-Users the Access Control Feature will include:
- A wide range of manufacturer solutions
- Using a series of doors & access points buyers will get a first-hand walk-through experience
- A dedicated workshop examining the capabilities and vulnerabilities in securing key access points

Why Exhibit?

TARGETED EVENT
Meet hard to reach buyers and specifiers from the public and private counter terrorism arena who rarely attend generic events

GLOBAL REACH
Attendees come from 79 countries

NETWORKING
The complete buying chain attends: End users, systems integrators, installers, and manufacturers

LAUNCH PLATFORM
Opportunity to launch new products through the exhibition, technology workshops, and live demonstrations

BRAND AWARENESS
Receive increased exposure in the lead up to, during, and after the event through our extended marketing campaign and dedicated exhibitor promotions

THOUGHT LEADERSHIP
Exhibiting alongside our high level conference and expert speakers provides you with the latest updates on regulations, legislation and procedures.

Stand Packages

SPACE ONLY £449 + VAT PER M2
Includes: floor space only, listing in the official event guide and website.

SHELL SCHEME £499 + VAT PER M2
Includes: floor space, carpets, walls, name board, listing in the official event guide and website.

ELITE PACKAGE £569 + VAT PER M2
Includes: floor space, carpets, walls, name board, furniture, literature rack, lights, power socket, listing in the official event guide and website.

Exhibitor Profile

Counter Terror Expo 2012 will offer a forum for senior buyers and specifiers to see the very latest solutions available to assist in global anti terrorism and counter terrorism measures.

The exhibition will showcase a wide range of technologies and services from over 400 exhibitors.

Product areas covered in the exhibition include:
- Access Control
- ANPR Software & Hardware
- Armoured Vehicles
- Barriers / Bollards / Gates / Turnstiles
- Biometrics
- Blast Containment
- CBRN Detection and Protection
- CCTV / Covert Surveillance Systems
- Communication Systems
- Database Management Systems
- Electro Optics
- Emergency Response Equipment
- Explosive Detection
- R.O.V / E.O.D
- Information Management and Security Systems
- Location and Tracking Systems
- Medical and Evacuation Equipment
- Perimeter Security and Intrusion Detection
- Personal Equipment & Body Armour
- Screening and Scanning Equipment
- Seals / Tamper Evident Solutions
- Special Vehicles and Transportation
- Sighting and Image Recording and Processing
- Technical Clothing and Protection
- Training Services
- Weapons and Ammunition

Contact Details

To discuss the event in further detail please feel free to contact:

MONIKA LUIS
t: +44 (0) 20 8542 9090
e: monika.luis@clarionevents.com

PHILIP BLOXSOME
t: +44 (0) 208 542 9090
e: philip.bloxsome@clarionevents.com

CLARION EVENTS

www.counterterrorexpo.co.uk/salesbrc

Aon's first Piracy Update confirms regional shift in piracy activity

Source:http://www.4-traders.com/AON-CORPORATION-11659/news/AON-CORPORATION-Aon-s-first-Piracy-Update-confirms-regional-shift-in-piracy-activity-13801181/

Aon Risk Solutions, the risk management business of Aon Corporation (NYSE: AON) today announced its first in-depth piracy report for ship owners worldwide. Collated by Aon's specialist Kidnap and Ransom Practice, Aon's Piracy Update uses piracy data from 2009 to 2011 to clarify the changing trends in regional and seasonal Somali piracy activity to allow ship owners to better manage their exposure to piracy. The report also looks at the emerging threat of piracy off the west coast of Africa.

Nearing the end of the monsoon season, a time when an increase of seasonal piracy activity is often seen, the update gives both commercial and private ship owners comprehensive insight into piracy risk and insurance and, in addition to a review of emerging piracy threats on the west coast, it also provides an analysis of piracy activity in four key risk zones off the east coast of Africa.

Aon's analysis confirms an increase in overall piracy activity while it reveals a general decline in successful attacks on vessels over the last year. The update explains a shift in regional activity, which has been attributed to an increase in anti-piracy measures. **The most notable shift has been seen in the Gulf of Aden, historically a piracy hotspot, to the Arabian Sea, which has experienced a 267 percent increase of attacks year on year.**

"This report has been produced to support ship owners in understanding the risks of piracy and how they can best mitigate and transfer those risks. Our team has many years of experience dealing with kidnap and ransom risks and, more recently, experience with the risks of piracy. While there has been no shortage of anecdotal accounts in recent years, access to fact-based data removes the speculation and supposition associated with activity in high-risk areas," Clive Stoddart, Aon Risk Solutions' global head of Kidnap and Ransom said. "Our clients benefit from the use of this data as we give credence to insurers' requests to verify their statistical analysis. The report is also designed to clarify key elements of cover and key issues in Marine K&R policies."

▶ To request the full report please contact: crisismanagement@aon.co.uk

The exploitation of a weak state: Al Qaeda in the Arabian Peninsula in Yemen

By Nicholas J. Hedberg
Lieutenant, United States Navy
B.A., Political Science, Gonzaga University, 2005
Submitted in partial fulfillment of the
requirements for the degree of
MASTER OF ARTS IN SECURITY STUDIES (MIDDLE EAST, SOUTH ASIA, SUB-SAHARAN AFRICA)
from the
NAVAL POSTGRADUATE SCHOOL (June 2010)

Abstract
Yemen is a weak state, as the government does not have the capability to assert effective control over the entirety of its territory. The Yemeni government faces three major challenges today including: the Houthi Rebellion, secessionists, and growing political unrest due to

its failing economy and inability to provide basic social services to its people. Al-Qaeda in the Arabian Peninsula (AQAP) has recently made a resurgence in Yemen since its near destruction in 2003. Yemen's weak state characteristics, along with the failure of jihad in Saudi Arabia, and the lack of Yemeni political will to combat the threat of AQAP and their global jihadist agenda have made the state an ideal location for the regional organization. AQAP has been able to exploit Yemen's weaknesses and build strong ties with the Yemeni tribes in the areas of Yemen where the government has little control. The study argues that due to these circumstances, Yemen has the strong possibility of becoming a safe haven for transnational terrorism akin to al-Qaeda's base in Pakistan today. To prevent al-Qaeda from using Yemen as their next base for transnational terrorism, the international community must help Yemen address the factors that have allowed AQAP to exploit the country.

NOTE: You can download the full thesis from the Newsletter's website (CBRNE-CT Papers section)

Conservative Party Conference: 'family life' loophole will go

Source:

http://www.telegraph.co.uk/news/politics/conservative/8805480/Conservative-Party-Conference-family-life-loophole-will-go-says-Theresa-May.html

The Home Secretary will tell the Conservative Party conference that she will stop foreign offenders using the "right to a family life" to remain in Britain.

Her speech comes as a Liberal Democrat security expert backs Conservative criticisms over the Human Rights Act, saying it is preventing the deportation of extremists who could mount attacks during next year's Olympic Games.

The Act, which incorporates into British law the European Convention on Human Rights (ECHR), is one of the flashpoints of the Coalition Government.

Critics, including Conservative ministers, say it is widely misused to help criminals and others escape justice, while Lib Dems insist it is misunderstood and should stay in place.

Article Eight of the convention, which ensures the right to a family

life, has been cited by some foreign criminals fighting expulsion from Britain.

Scores have avoided deportation by claiming that because they have partners or children in the UK, being thrown out of the country would infringe their rights under Article Eight.

David Cameron, the Prime Minister, said on Tuesday, that the courts gave too much weight to the Article.

"The problem here is that there are foreign criminals in Britain, people sometimes actually who still threaten our country or could threaten our country," he told BBC Breakfast.

"We are unable to deport them because they appeal to the courts under Article Eight of this charter, which is the right to a family life.

"We believe that the courts are currently giving too much attention to that rather than the protection of the UK."

He added: "You are able to change the immigration rules and ask them to look more carefully about the danger these individuals pose.

"The right to a family life is not an inalienable right in the European convention so I believe this change will work. It is not the whole solution to the problem but it is a good start."

Last year there were 102 successful appeals against deportation on human rights grounds which cited Article Eight.

Mrs May will announce today that immigration rules will be rewritten to set out explicit exemptions which would allow deportation regardless of family.

The new rules will direct the courts to give greater weight to sections of the ECHR which allow exceptions to be made.

Clause Two of the article permits exceptions that are "necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country".

Mrs May will say that the courts should consider that a range of factors outweigh a foreigner's right to a family life.

Such factors will include criminal offences, breaches of immigration rules and relying on welfare benefits for income and housing.

Lord Carlile, a senior Lib Dem lawyer, today backs Conservative attacks on the controversial act, warning that it could allow some known extremists to remain in the UK.

In an article for the Policy Exchange think tank, Lord Carlile, a former government reviewer of terrorism laws, warns that the "promiscuous use" of Article Eight could put Britain's security at risk by preventing the deportation of foreign terrorists now in jail.

He says there are more than 100 extremist offenders in custody, some of whom are to be released soon.

If allowed to stay in the country, he suggests, they could attack the 2012 London Olympics.

"This is not scaremongering. It is a realistic assessment of what we may face," he says.

He also calls for changes to restrict the use of Article Three of the ECHR, which prohibits torture. Terrorists such as Siraj Yassin Abdullah Ali, jailed for helping in the 21/7 attacks in London, have used Article Three to remain in the UK.

What the U.S. Can Learn from the Two-Pronged Attack in Norway
By Eric Stern
Source:http://www.emergencymgmt.com/safety/US-Learn-Two-Pronged-Attack-in-Norway.html?elq=33bb280b 9870460782e322d510cc5b97

The July bombing and shooting attacks in Oslo, Norway — where a citizen terrorist struck the prosperous, peace-loving nation with a devastating act of political violence — claimed at least 80 lives, injured nearly 100 people and captured the world's attention. The shock was amplified by the fact that Norway had

previously been largely spared from the kind of political violence that has chronically afflicted its European neighbors and the United States. These acts reflected a deadly combination of elaborate planning, deception and diabolical creativity.

Borrowing from military science, terrorism experts often use the term "operational art" to describe the evolving modi operandi and tactics of terror groups. The term is doubly apt in describing acts of "performance violence" — attempts to orchestrate public spectacles of destruction to broadcast a message to the world. Like other forms of art, operational art is cumulative and referential in an important sense. A given operation draws inspiration (and differentiates itself) from those that have gone before. The script from the July 22 massacre in Oslo contains familiar elements.

The use of a fertilizer bomb by an extremist to target government buildings, for example, appears to be taken straight from the Oklahoma City bombing template, with Norwegian right-wing extremist Anders Behring Breivik (a.k.a. Andrew Berwick) cast in the role played by Timothy McVeigh. Breivik's so-called manifesto — itself following in the footsteps and drawing upon that of Ted Kaczynski, the so-called Unabomber, — indicate that he identified with McVeigh. The use of tightly sequenced attacks is reminiscent of several recent cases in Mumbai, India.

Targeting youth, in this case, participants in a political party youth retreat, is reminiscent not only of Chechen terrorist acts, but also school shootings in the United States, such as those at Columbine High School and Virginia Tech. The use of deception and manipulation in the form of a false police uniform to gather and herd intended victims evokes associations with Nazi extermination methodology — and it also enabled

the alleged perpetrator's access to the site of the youth movement retreat.

It's important to note that Breivik's plan included significant manipulative aspects aimed at first responders. The first attack was intended to strike at the symbolic heart of the Norwegian government, but also included an element of diversion and misdirection — leading first responders and the security services to concentrate attention and resources on downtown Oslo and possible additional threats to government leaders and buildings when the real threat was elsewhere. Other terrorists have used manipulative tactics targeted at first responders. A classic case of this is the 2004 Madrid bombings, in which secondary charges are thought to have been timed to detonate after a deliberate delay designed to allow the Spanish first responders to arrive on the scene.

Breivik's dance of death on July 22 was choreographed in minute detail — it was the result of meticulous planning and preparation spanning several years. By purchasing a farm, he was able to order large quantities of chemical fertilizers without attracting attention. A substantial part of this preparation focused both on the operational side of his mission and on how to communicate his message for maximum impact. Enormous effort was devoted to documenting the narrative of his journey and developing propaganda materials clearly designed to go viral and capitalize on the instant celebrity that comes with the commission of these kinds of atrocities. Breivik groomed himself for this role by taking steroids, and preparing glamour shots of himself decked out in medieval costume, and futuristic military apparel and equipment. Reportedly he even underwent cosmetic surgery to prepare himself as the intended poster boy for his crusade against multiculturalism in Norway and Europe.

Breivik took full advantage of the fact that he did not fit the profile of a "typical" terrorist as perceived by the Norwegian authorities. As a citizen terrorist of traditional Norwegian ancestry and

Nordic appearance, he was able to blend in and evade scrutiny.

Several recent United States cases serve as vivid reminders that so-called insiders, including those employed by the government, can pose a serious threat and are easily overlooked. The perpetrator of the Fort Hood Massacre of 2009, in which 13 people were killed and 29 wounded, was a U.S. Army psychiatrist, Maj. Nidal Malik Hasan.

September 2011 will not only mark the 10th anniversary of the 9/11 attacks, but also of the Amerithrax attacks when deadly anthrax spores were mailed to members of Congress and prominent media figures.

The FBI and U.S. Department of Justice concluded that the perpetrator was a leading anthrax specialist employed at a U.S. Army research lab. An exhaustive study by an Expert Behavioral Analysis Panel found that the expert had motive, opportunity and a behavioral disposition consistent with the attacks. The

anthrax expert was psychologically unstable, according to the findings, and shouldn't have been allowed continued access to deadly biological agents.

As a result of this incident, the panel prepared reform proposals designed to enhance the rigor of personnel reliability programs to prevent psychologically unstable or otherwise inappropriate individuals from accessing dangerous or other forms of sensitive materials and information.

Sadly the events of July 22 will add a new montage to the discourse of political violence and will inspire other fanatics to new acts of monumental and devious cruelty. Hasan's attack on Fort Hood has apparently already spawned at least one (fortunately rather inept) copycat in the form of Pfc. Naser Jason Abdo. This raises some very troubling questions: Who will follow Breivik, and how and where will he or she choose to strike?

Eric Stern is the co-chairman of the Critical Incident Analysis Group at the University of Virginia and professor of political science/crisis management at the Swedish National Defense College.

NEW BOOK: It's Not About The Money

By Daniel Byman (Author)
Source: http://www.citizen-times.eu/its-not-about-the-money/

Counterterrorism and trauma go hand in hand, yet this relationship has been a deeply neglected topic in Middle East Studies and in other political conflicts. The best research on both has been coming out of Israel since before the creation of the State. A High Price begins with the British Mandate Period writing forward, up through the present in a balance manner covering not only the Arab based Palestinian
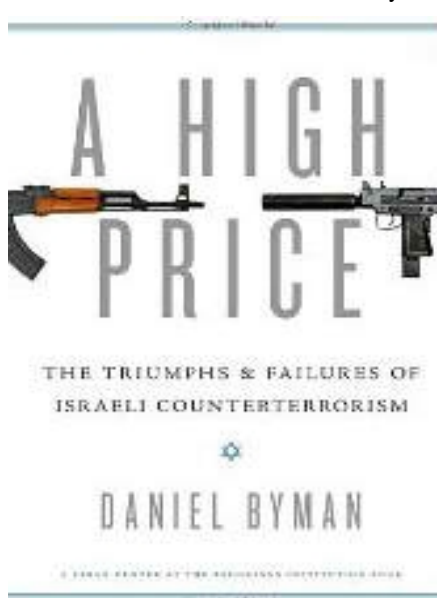
terrorism expanding out to the rigidly religious ideological groups such as Hamas, Palestinian Islamic Jihad, to the global Al Qaeda and the Shia Hizbollah but also very importantly the Jewish terrorist groups, the extreme streak within the settler movement, Tag Mechir (Price Tag) and even such lone wolves as Yigal Amir.

Daniel Byman (2011): A High Price: The Triumphs and Failures of Israeli Counterterrorism. Oxford University Press, 496 pages, 27,99 Euro

A High Price: The Triumphs and Failures of Israeli Counterterrorism is written

by a leading scholar, Professor Byman, who teaches at Georgetown University in the School of Foreign Service. He is also senior fellow at the Saban Center for Middle East Policy at the Brookings Institute. Author of Deadly Connections: States that Sponsor Terrorism (2007), The Five Front War (2007) and Keeping the Peace (2002), he is deeply involved in counterterrorism. He has served on the 9/11 committee. Hence, he is eminently qualified to research and produce such a book. Moreover he has linguistic, cultural and historical knowledge of the Middle East. He conducted in depth interviews with some of the major players in Israel like Avi Dichter, Boaz Ganor, and Yoram Schweitzer just to name a few. In addition he has uncanny psychological insight concerning the actors, the violence and the function of terrorism. Byman's narrative adeptly describes these interlocking conflicts, showing how one action precipitates a counter response often with the escalation of violence rather than its diminution. Byman develops the context within which these interlocking dynamics occur as it diachronically plays out. He is brilliant in documenting, detailing and plotting the scope and depth of how Israelis are famous for "tokh c'dei t'nuah" improvising as they go but faltering terribly when it comes to long term planning, especially with the interplay between national security planning and counterterrorism. One could even see this in the "Israeli summer tent protests" and their chants for social justice. The lament is the same, that there is no leadership, only politicians. Byman's section on "A System Designed for Chaos" puts it well:

In over sixty years of fighting terrorism Israel has at times empowered radicals at the expense of moderates, tarnished its diplomatic image, allowed terrorists to use propaganda to turn defeat into victory, and otherwise failed at strategic level. Such failures are in part due to the difficulty of the challenge Israel has faced and continues to face. But many of these mistakes must be laid at the door of the country's poor national security decision-making system. Israel's national decision making is as disastrous as its military and intelligence services are impressive."

The final section of the book on Findings and Conclusions does not disappoint as it deals with interrogation dilemmas to targeted killings, the security fence or wall depending which side you are on figuratively and literally along with what needs to be reorganized in order to be more effective in countering terrorism. He ends on a realistic but pessimistic note of fading hopes for peace with a splendid chapter concerning "What Israel can teach the world and what Israel should learn."

Byman unwittingly provided tons of information indirectly concerning the dynamics of terrorism's violence and its squeal of trauma, disclosing the elephant in the room, a dysfunctional Palestinian family system (shame honor culture) with its attendant devalued female and over idealized mother supported by extremist religious ideologies as in the case of Hamas, etc. that yields impoverished social skills and causes the perpetuation of grievances across the generations, perpetual victimhood, i.e. intergenerational transmission of trauma. All of this impedes healthy psychological infrastructure for an individual still trapped in cult-like clans/hamula and tribes, whose challenged familial dynamics, to put it diplomatically, replay as shoddy civic infrastructure lacking democracy. To cite only a few examples that to a large degree ummi, the Arab mother, is the terrorist's Achilles' heel and to a lesser extent Imaleh, the Israeli Jewish mother serves as a kind of mirror image making it difficult for counter terrorist experts to deal with the blind spot. Byman offers some anecdotal moments for an unwritten history of the role of the mother in political terrorism. See page 31 on the orphaned motherless Arafat, as an example of many terrorist leaders who were abandoned orphans. It is not unusual that he would be likely to recruit young terrorists with no purpose in life as they would be perfect targets to work under his warped tutelage. His lifelong anger and split personality derives from this early deprivation. He was known to be a pervasive liar. See also pages 54,106, 146, 189, 337 alluding to the terrorist mother and

read most especially Duha, the four year old daughter of the female suicide bomber Reem Riyashi, singing to her dead mother in a Hamas made for tv children's program. "My mother , my mother… Instead of me you carried a bomb in your hands; I know what was more precious then us," and promising, "I am following Mommy in her footsteps."

Byman does not let the Israelis off the hook, and rightfully so, for falling into the trap of stooping to the level of the Palestinian terrorist's maternal conflict when he takes the Givati Brigade to task about a T-shirt "displaying a bull's eye on a pregnant Palestinian woman…" See pages 142 and 241 concerning Imaleh, the Israeli Jewish mother.

The Egyptian sociologist, Halim Barakat, has written that the family is the microcosm of the society. Byman also notes that "The family and the tribe often form the basis for recruitment, particularly for the more elite units that carry out terrorism." He quotes Shai Nitzan's argument before the Israeli Supreme Court, claiming that "the family is a central factor in Palestinian society" and through it terrorists can be deterred." These maternal moments were probably unintended as such to carry the narrative weight of A High Price. Yet they give a human dimension to such triumphs and failures and they are at the eye of the storm.

I quibble with Byman over one omission concerning the settlers' movement toward violent behavior and the withdrawal from Gaza. There were in fact two self-immolations. One by a settler Russian woman and one by a young man. This is part of the slippery slope phenomenon into what could have become Jewish suicide bombings and still may in the future. There is no guarantee. Judaism in extremis could participate in this kind of perverse aberrant hysterical phenomenon. Suicide bombing is incredibly imitative, it degrades some of those it comes in contact with, murders many, maims brutally and spreads like wild fire. Immolation is key to suicide bombing. The second quibble concerns Yahiya

Ayash the Hamas Engineer and exactly whom was he told that was on the other end of the cell phone call that blew off his head — his mother or father? Byman offers two conflicting reports which just goes to show the reader what a careful researcher he is. Finally, I wish that Byman had underscored the symbolic meaning of stoning and stone throwing by Palestinians as well as Muslims when he cited the Mitchell Commission's investigation. Stone throwing is considered a crime in Israel. But more than that, stone throwing is revealing behavior — potentially lethal, concrete and autistic.

Byman repeatedly notes the difficulty in breaking through those terrorists that hold to a religious ideology. Could this be an indicator of a much more recalcitrant psychopathology, showing a cognitive paranoid deficit? It would behoove counter terrorist experts to move beyond the surface of this phenomenon to factor in an earlier developmental problem which is perhaps similarly shared by those non Arabs who become radicalized. Ultimately neuroscience will probably help us understand their glaring lack of empathy for the other.

To conclude, A High Price is not about the money, rather it is about learning to develop balance between countering terrorism and national security needs for its citizenry. This book should be required reading for every student in political science, conflict resolution, counterterrorism and national security studies to say nothing of the need for all diplomats dealing with the Middle East as well. Above all the text needs to be translated into Hebrew and Arabic so that all Israelis and the Arab Springers can come to understand the dilemma which they mutually face – how to make Israel safe and the Arab minority better integrated into Israeli society, while at the same time making the Arab regional majority safe and democratic. Byman's A High Price enters the canon of counterterrorism studies. I place it at the center.

Europe's Underestimated Islamists

By Ian Johnson
Source: http://www.meforum.org/3059/europe-islamists

In early 1959, a small West German intelligence operation stumbled over a sensational find: U.S. collusion with the Muslim Brotherhood. According to the West German sources—two ex-Wehrmacht soldiers who were in Washington's pay but still felt loyalty to their old German bosses—Washington was supporting one of the Brotherhood's top men, the Geneva-based Said Ramadan, son-in-law of the movement's founder Hassan al-Banna, in the hope of using him in the global battle against communism. The U.S. double-agents wanted to know if the West Germans would also help support Ramadan.

Bonn's response was an unequivocal "no": not because of ethical qualms about doing business with the Brotherhood but because of practical considerations. "Ramadan doesn't possess the slightest influence in the Orient," read an evaluation by the head of the West German intelligence operation, Gerhard von Mende. "A connection with him would only yield negative consequences."[1]

Von Mende was neither the first nor the last to have underestimated the Brotherhood or its leaders. In its 83-year history, the movement has time and again been written off as out of date,

broken, or otherwise a non-force. Most recently, Western analysts of the Middle East upheavals were quick to portray the Brotherhood as out of touch and, basically, inept. U.S. director of national intelligence James Clapper reduced it to a "largely secular" movement[2] while anthropologist Scott Atran argued that its "failure to support the initial uprising in Cairo on Jan. 25 [2011] has made it marginal to the spirit of revolt now spreading across the Arab world."[3] News pages had similar coverage with the Brotherhood's absence in some Cairo neighborhoods seen as indicative of its declining importance.[4]

Of course, as is now known, the Brotherhood played a leading role in the Egyptian uprising and its wake.[5] This should have come as no surprise. For all its flaws, mistakes, and disastrous decisions, the Brotherhood is one of the most resilient organizations in modern history. Its longevity is due to one of its defining characteristics: an almost intuitive ability to assume new forms while pursuing its ultimate goals and carving out niches of influence. In its eagerness to write off the Brotherhood, the West has shown a distinct lack of attentiveness to the group, leading to decades of blunders.

In an unassuming office complex in Herndon, Virginia, the Muslim Brotherhood's European leaders set up the International Institute of Islamic Thought (IIIT) as a beachhead for spreading Islamist thought in the West. IIIT's headquarters were raided by the FBI in 2002 for connections to terrorists, and the institute was cited in 2010 by the Justice Department as an unindicted coconspirator in the Holy Land Foundation terrorism financing case.

Nowhere has this phenomenon been more starkly demonstrated than in Europe. For half-a-century—unlike in the Arab world—the

Brotherhood has been able to grow without any restrictions, going from a one-man operation centered around Ramadan to being the

continent's foremost Islamist force. How this happened illustrates the Islamist movement's potency and hints at ways it can be dealt with today. A decade after the 9/11 attacks, why is the West still grappling with Islamism, not so much as a force for terrorism—though that risk remains potent—but as an important political force throughout the Middle East and beyond?

Planting the Seeds

Gamal Abdel Nasser's 1954 ban of the Brotherhood forced the group to reorganize abroad. While many of its senior leaders would spend years in Egyptian jails and its top theoretician, Sayyid Qutb, would be executed, the group was fortunate in having two havens where it was able to regroup. One was Saudi Arabia where it laid down deep roots, eventually melding with indigenous Islamist movements to create a powerful and violent challenge to the ruling royal family.[6] The other, less well-known haven was Europe. Ramadan had already been to the continent several times and was studying law at Cologne University. When the Egyptian ban came into effect, he was living in Geneva, which he would make his home until his death forty years later.

This was a period before the great influx of migrant workers was to transform Europe. Muslims were few and far between. Germany, for example, had just two mosques, one in Hamburg and the other in Berlin. But this does not mean that Islam was not on the radar of Western policymakers. The process of decolonization was creating dozens of newly independent states, many of them Muslim. Western intelligence agencies were eager to use covert propaganda to influence these countries for broader, strategic purposes, such as the battle against communism. West Germany was home to several hundred Muslims (estimates vary with the upper limit around 2,000) who had served in the Wehrmacht and the Nazi SS. They had been former Red Army soldiers who had been captured by the Germans and changed sides, either for fear of death in the horrific German prisoner-of-war camps or because of their belief in the Nazis' promise to liberate their Soviet-ruled homelands.

After the war, most were repatriated but some managed to stay on, congregating for various reasons in Munich.[7]

Many of these began working for von Mende, who had spent the war years in the Reich Ministry for the Occupied Eastern Territories (usually known as the Ostministerium), coordinating Muslim and other Soviet minorities. After the war, he set up a series of quasi-free intelligence operations that have remained unstudied to date, eventually settling on the name "Research Service East Europe" (Forschungsdienst Osteuropa) that was co-financed at various times by the West German Interior Ministry, Foreign Office, External Intelligence Service, and Domestic Intelligence Service. Von Mende tried to rally the Muslims who stayed behind—many of them his old Ostministerium colleagues—in order to achieve West German foreign policy aims, including the long-term recovery of lost German territories east of the Oder-Neisse border. One of his methods for winning over the Muslims was to promise them a mosque in Munich.

Ramadan stepped into this complex situation in 1958. Under von Mende's guidance, the Munich Muslims set up a registered, legal organization to build the mosque,[8] inviting young Arab students for extended stays in the city. Ramadan was thus invited from Geneva to Munich and within a year kicked out von Mende's Muslims and took over the project, using his position as head of the Munich Mosque Construction Commission[9] to traverse the Muslim world with his assistant (and later rival), Ghaleb Himmat.

Ramadan was aided significantly by the Central Intelligence Agency, which allegedly paid for his travel and backed his efforts to take over the mosque. Suspicions by the West German and Swiss intelligence services that he was a CIA operative have never been positively proven, but the archives show an early U.S. fascination with the Brotherhood, one that would recur in the subsequent decades.[10]

Whatever the reasons behind the U.S. support for Ramadan and the Brotherhood, the latter made good

use of their European platform. Through dint of hard work and organizational prowess they used the mosque as a springboard to create a European-wide network.[11]

Consolidation and Expansion

An initial effort at forming a framework for Islamism in Europe took place in 1973, just a few months before the Munich mosque opened. Held in London's theater district, the Islamic Cultural Centers and Bodies in Europe was designed to establish a network of like-minded groups. Several dozen activists attended, including Ghaleb Himmat, freshly minted as head of the Islamic Community of Southern Germany—the official name of the Munich mosque. Reflecting Saudi Arabia's efforts to dominate organized Islam, the chairman was a Saudi. Himmat was elected to the governing council, along with Khurshid Ahmad, a leading Pakistani activist. The meeting did not immediately succeed in setting up a European network, but it was a first step.[12]

Four years later, the Brotherhood scored a crucial success. A meeting in the Swiss lakeside resort of Lugano, headed by Himmat and Yusuf Nada, another key person in the mosque, with the participation of prominent activists, notably Yusuf al-Qaradawi, now widely described as the Brotherhood's spiritual leader, initiated the arduous process of rebuilding the organization after the years of Nasserite repression. In Europe, protected by laws and institutions, they were free to set up lasting structures, beginning with the International Institute of Islamic Thought (IIIT), whose real task was to provide the theoretical underpinnings for the spread of Islamism in the West. In 1978, the group met in Saudi Arabia and decided to relocate IIIT to the United States where it would be headed by Ismail Faruqi, a leading Islamist thinker who had also been in Lugano and who held a teaching post at Temple University in Philadelphia.[13]

Meanwhile, the Islamic Center of Munich continued to grow in importance, and in 1982, changed its name to the Islamic Community of Germany, reflecting its growth across the country. The Islamic Center of Munich was still important but now primarily as the headquarters of a national group that oversaw a chain of mosques and cultural centers. The exact number of these, in the early 1980s, cannot be ascertained, but it had branches in all major West German cities.

Reflecting its international importance, the group continued to add members from abroad, turning membership in the mosque into a badge of honor. Khurshid Ahmad, for example, joined. He had been at the 1973 London meeting and was the most important representative in Europe of Jamaat-e-Islami, the South Asian version of the Muslim Brotherhood. Another key person to join was Issam al-Attar, the charismatic head of the Muslim Brotherhood's Syrian branch, who had moved to Belgium in the early 1960s and settled in the West German city of Aachen in 1968.[14]

Their joining was emblematic of the international Islamist movement's ability to overcome the ethnic divisions that had split Islam. Although men like Himmat, Attar, and Ahmad had their ideological and personal differences, in Europe they had far more in common. From their point of view, they were the vanguard of a new Islamist wave in the West, pioneering minorities in Christian lands. But they had little to do with ordinary Muslims or the mosque they were supposed to be leading; they did not live in Munich, and the mosque was just a vehicle for their struggle. The group's disconnect from West Germany was highlighted by Himmat, who sent in the protocols of the 1982 meeting by registered mail from his villa overlooking Lake Lugano, 250 miles away from Munich.[15]

By the 1990s, an alphabet soup of organizations had stretched across Europe. The Islamic Community of Germany—as the organization based at the mother mosque in Munich—was a founding member of the Brussels-based Federation of Islamic Organizations in Europe linking Brotherhood groups in more than twenty countries. Attached to it is the Dublin-based European Council on Fatwa and Research that issues religious opinions to European Muslims. A funding arm, the U.K.-registered Europe Trust, channels money

from the Persian Gulf to groups sympathetic to the Brotherhood in Europe, primarily to build mosques. And the European Institute of Human Sciences trains imams at three campuses in France and Wales. All these bodies and organizations are linked to the Brotherhood through interlocking directorates and senior advisors, such as Qaradawi. These groups also receive significant funding from foreign donors such as the Maktoum Foundation.[16]

This frenzy of institution building highlights an important point about the Brotherhood, namely that it is not a religious society with theological goals. It has had one or two important thinkers, but their main point has been simple: The Qur'an should be interpreted in a relatively literal fashion so as to shape every aspect of temporal society. Most of its members, especially the key institution builders and functionaries who run it, have no theological training or knowledge. Many held degrees in engineering, medicine, or law, leading to the sometimes mocking term of "engineer Islam." This personnel mix, however, is ideally suited for institution building. Back in Egypt before it was banned, it imitated 1930s-style fascist parties. The Brotherhood had political parties, newspapers, youth associations, women's groups and a quasi-military wing. In Europe, these diligent functionaries dutifully duplicated much of this structure (minus the military wing). The main difference is that the Brotherhood is operating as a minority religion, so it uses its structures not to Islamize mainstream society—which is an unrealistic task—but to dominate the West's Muslim communities. It aims to shield them from the West's secular and multicultural societies, providing an alternative reality for its members. It also tries to convert other Muslims into "better" Muslims, who follow the Brotherhood's narrow vision of Islam.

This goal is all the more important given the fact that since the abolition of the caliphate (in 1924), the Islamic world has had no overarching religious authority or structure. If a group set up a body and claimed to speak for Muslims, few could challenge it unless a rival group was set up. The Brotherhood, with its organizational prowess, has been quicker and more efficient than other Muslim groups to assert its preeminence in Europe—from Ramadan's pan-European Muslim conference sponsored by the CIA in the 1960s to the pan-European federation today. It is no coincidence that in both cases—and all in between—outsiders have financed the Brotherhood's activities. That is because at its heart, the Brotherhood outside of Egypt is not a mass organization. It is a group of elite organizers who have set up the structures to define Islam in the West. The Islamic Center of Munich and all successor organizations have never numbered more than a few dozen members. These people did not serve Munich's Muslim community—indeed, the Turkish Muslims who by the 1970s made up 90 percent of the city's Muslims were explicitly denied membership. Instead, the leadership was obsessed with setting up structures. In the Cold War, these groups were relatively unimportant. If anyone paid attention to them it was with a view to using them to fight communism. But as they developed, something unexpected happened: Europe, once outside the Muslim world, became central to its future, and the Brotherhood, after years of laborious organizational work, was suddenly poised to lead the charge.

Conduit to Terrorism

The Brotherhood may be influential in Muslim circles, but is it involved in terrorism? The answer to this is, yes, but this is to some extent a moot point. Since 9/11, terrorism has become a far-too-narrow test for Western evaluation of Islamist groups. If they are violent (usually defined in terms of attacks against Western targets), then they are bad; otherwise, they are good. The Brotherhood has managed to slip through relatively unscathed—yet another indication of the underestimation of its real importance.

To illustrate this point, it may be useful to return to the Munich mosque and two of its brushes with terrorism. Mahmud Abouhalima, the man convicted of the 1993 World Trade Center bombing, for example, had been a

regular at the mosque[17] and had sought spiritual counseling from Ahmad al-Khalifa, then the mosque's chief imam. Khalifa and the center denied any connection with the plot, saying Abouhalima had simply come for spiritual counseling.

There was also the case of Mamduh Mahmud Salim, widely seen as al-Qaeda's finance chief and bin Laden's personal mentor. He was arrested in 1998 in a small town near Munich while on a business trip to Germany. Before being extradited to the United States, he called up Khalifa and asked for spiritual guidance. (He was later put on trial in New York and sentenced to thirty-two years in prison.) Khalifa confirmed to having met both men but described the contacts as being purely humanitarian work.[18]

German intelligence was, nevertheless, alarmed and launched an all-out investigation into Salim's contacts. One, in particular, stood out: Mamun Darkazanli—a Syrian businessman living in Hamburg, who attended a small mosque there called al-Quds. German police bugged Darkazanli's home and observed his contacts at the mosque, including one particular man, Muhammad Atta, but being unsure about the nature of their findings decided to drop the investigation. Two years later, on September 11, 2001, Atta flew the first plane into the World Trade Center, and al-Quds mosque emerged as a place where the hijackers had been radicalized. Darkazanli was never prosecuted, but he was yet another less-than-glorious link between the Islamic Center of Munich and political-religious extremism.[19]

Shocked by the 9/11 attacks, the U.S. government swung hard against the Brotherhood. Investigators were especially fascinated by one of Nada's investment vehicles, Banque al-Taqwa. Himmat sat on its board, and seemingly every Islamist in Europe had bought shares in it, making its shareholder list a who's who of the Muslim Brotherhood in Europe. Nada had set up the bank as one of the first financial institutes to operate in conformity with Islamic law. Instead of offering depositors interest, the bank called its customers investors and offered them profits

from money it lent out. But he had invested the money amateurishly—Nada himself says he put most of it in Malaysian businesses shortly before the 1997 Asian financial crisis—and the bank went under. U.S. prosecutors, however, concluded that the bank was a conduit for terrorist money. Washington declared Nada and Himmat terrorist financiers and had the designation endorsed by the United Nations. Both men's bank accounts were frozen.[20]

The Islamic Community of Germany suddenly faced a financial crisis. The community's chief officer, Himmat, signed the group's checks, but now anything he touched was frozen. There was also a painful interview in the Munich mosque's publication al-Islam, in which Khalifa tried to justify why Himmat, who had lived in Lugano for decades, was running the group. After twenty-nine years at the helm, Himmat resigned in early 2002.[21]

But this did nothing to combat terrorism. As the Munich mosque's links to the 9/11 attacks show, the Brotherhood is not so much—at least in terms of Western targets—an active promoter of terrorism. Instead, it creates the milieu from which terrorism arises. Atta did not receive instructions from anyone affiliated with the Munich mosque, but the mosque was part of an Islamist environment with links to Atta. This is why the government's attempts to cripple Nada and Himmat financially were inappropriate. The problem that both men posed was ideological and needed to be countered on this level. Their lack of direct links to terrorism was proven by Washington's inability to prosecute them. Eight years after freezing their accounts, Washington had to acquiesce as they were unfrozen.

This parallels a broader and equally uninformed rapprochement between Western governments and the Brotherhood. By the second term of George W. Bush, efforts were already underway to renew Washington's decades-old links to the group. The State Department organized conferences between the European Brotherhood and American Muslims—who are also in groups descended from that

organization.[22] All of this was backed by CIA analyses, with one arguing that the Brotherhood featured "impressive internal dynamism, organization, and media savvy."[23] Ignoring warnings from Western allies against supporting the Brotherhood in Europe, the CIA pushed for cooperation. This policy has continued under the Obama administration.

Conclusion

Why the enduring interest in the Brotherhood? Since its founding in 1928, the movement has managed to voice the aspirations of the Middle East's downtrodden and often confused middle class. Although it has many adherents at the lowest-rungs of society, it is run and organized by educated professionals. An organization run by such people and appealing to the masses is naturally intriguing to Western policymakers eager to influence this strategic part of the world.

But how the Brotherhood achieves its appeal makes it a dubious partner. Most Muslim societies have lived through more than a century of oppression by corrupt and brutal elites, and Islamists have invariably presented the establishment of religious rule as the only road to a more just society. In truth, however, the Brotherhood has offered a fundamentally anti-

modern, political program and ideology, exalting the small number of "true" Muslims who adhere to a literalist view of the Qur'an and writing off the rest—including most Muslims—as apostates.

Many Brotherhood spokesmen claim it renounces violence, but its chief theoreticians have not been able to bring themselves to do so. Qaradawi, for one, has regularly railed against "Zionists and Jews"—although some analysts claim this is not so serious and that he is actually a moderate (at least in comparison to al-Qaeda). Yet he has explicitly endorsed suicide bombings against Israeli civilians, including children (because they will grow up to be adults), expressing his desire to die as a martyr "at the hands of a non-Muslim."[24]

This means that a decade after 9/11, the West is still unsure how to deal with Islamism. Just as in the 1950s, policymakers tended to either lionize Islamists as potential allies in the struggle against communism or write them off as passé; these two extremes have been much in play in the decade attending the attacks. What is missing is a middle way that treats Islamism for what it is: a potent ideology that is likely to be a threat for the foreseeable future.

Sources:

[1] "Aktennotiz Betr. Besuch von Shamil and Magoma," German Foreign Office Political Archive, Berlin, AA PA ZA 105731, Feb. 3, 1959.

[2] YnetNews (Tel Aviv), Feb. 11, 2011.

[3] Scott Atran, "Egypt's Bumbling Brotherhood," The New York Times, Feb. 2, 2011.

[4] See, for example, The New York Times, Feb. 15, 2011.

[5] Ibid., Mar. 24, 2011.

[6] Stephane Lacroix, Awakening Islam: Religious Dissent in Contemporary Saudi Arabia (Cambridge, Mass.: Harvard University Press, 2011).

[7] Alexander Dallin, German Rule in Russia: A Study in Occupation Politics, 2nd ed. (London: The MacMillan Press Ltd., 1981. p. 540.

[8] "About the Muslim Brotherhood," Global Muslim Brotherhood Daily Report, accessed June 24, 2011.

[9] Ian Johnson, "The Muslim Brotherhood in Europe," briefing before the Congressional Human Relations Caucus, U.S. House of Representatives, Washington, D.C., Feb. 9, 2006.

[10] Ian Johnson, A Mosque in Munich: Nazis, the CIA, and the Rise of the Muslim Brotherhood in the West (New York: Houghton Mifflin, 2010).

[11] Lorenzo Vidino, "The Western Brotherhood," The New Muslim Brotherhood in the West (New York: Columbia University Press, 2010).

[12] Impact International, May 25-June 7, 1973, p. 3.

[13] Muhammad Shafiq, Growth of Islamic Thought in North America: Focus on Ismail Raji al-Faruqi (Brentwood, Mass.: Amana Publications, 1994), p. 27-9.

[14] "Protokoll," Amtsgericht München (Munich district court), Dec. 4, 1982, p. 1.

[15] Ibid.

[16] Author's interview with Ahmad Rawi, former head of the Federation of Islamic Organizations in Europe, Markfield, U.K., July 21, 2004.

[17] Time Magazine, June 24, 2001.

[18] Al-Islam (Munich), June 2001, pp. 16–8.

[19] Ian Johnson and Alfred Kueppers, "Missed Link," The Wall Street Journal, Oct. 19, 2001.

[20] Matthew A. Levitt, "The Role of Charities and NGOs in the Financing of Terrorist Activities," Subcommittee on International Trade and Finance, U.S. Senate Committee on Banking, Housing, and Urban Affairs, Washington, D.C., Aug. 1, 2002.

[21] Amtsgericht München, Jan. 13, 2002. Himmat gave the explanation of the frozen accounts in a telephone interview, June 1, 2005.

[22] Tom C. Korologos, U.S. ambassador to Belgium, "Islamist Extremism in Europe," testimony before the Subcommittee on European Affairs, U.S. Senate Foreign Relations Committee, Apr. 5, 2006.

[23] "Muslim Brotherhood: Pivotal Actor in European Political Islam," Central Intelligence Agency, Langley, Md., May 10, 2006.

[24] BBC News, July 7, 2004; Global Muslim Brotherhood Daily Report, Jan. 31, 2011; see, also, "The Qaradawi Fatwas," Middle East Quarterly, Summer 2004, pp. 78-80.

Ian Johnson is an author based in Berlin and Beijing who specializes in the intersection of religion and civil society. He was Germany bureau chief for The Wall Street Journal and, in 2010, published A Mosque in Munich: Nazis, the CIA and the Muslim Brotherhood in the West (New York: Houghton Mifflin Harcourt).

US blacklists Greek anarchist group

Source: http://www.fmnewschicago.com/news/article.aspx?id=891697

The Obama administration has added a Greek anarchist group to a terrorism blacklist that subjects the organization and its members to U.S. financial sanctions.

The State Department said Thursday it had placed the Conspiracy of Fire Nuclei, or SPF, on its list of specially designated terrorists, a move that freezes any assets the group may have in U.S. jurisdictions and bars Americans from giving it any material support. It said the group, which first emerged in 2008, had targeted civilians and government officials in a number of countries, including Greece, in an attempt to spread its ideology.

SPF has attacked car dealerships and banks with fire bombs and last year attempted to mail parcel bombs to European Union offices in Germany and Italy and foreign embassies in Greece, it said.

Arson attacks disrupt German train system

CBRNE Terrorism Newsletter – Winter 2011

Source: http://www.ajc.com/news/nation-world/arson-attacks-disrupt-german-1199159.html

German authorities sent scores of police to secure the nation's railways on Wednesday after a series of firebombs disrupted train traffic for thousands of passengers.

Police officers examine a utility shaft nearby the rail tracks of the northern exit of Berlin's central train station tunnel in Berlin, Germany, Monday, Oct. 10, 2011. German police say they thwarted an arson attack on Berlin's central train station at the last minute. Police spokeswoman Nadine Marschner said Monday experts secured seven bottles filled with flammable liquid bundled together and linked to a fuse. She says railway employees alerted authorities midday after detecting suspicious items at the north end of one of the station's tunnels, just 100 yards (meters) from the train platforms. Police say similar devices were used in a second arson attack earlier just east of Berlin along a high-speed link to Hamburg. The blast in a utility shaft caused some damage and brought train traffic temporarily to a halt. Marschner had no immediate comment on possible motives of the attacks. (AP Photo/Michael Sohn)

A public train passes a cable shaft in Berlin, Germany, Tuesday, Oct. 11, 2011 where three separate explosives devices were found. A railway employee found the devices placed on cables along a railway track in eastern Berlin on Tuesday morning and alerted security. The devices did not explode and were defused by police experts. Parts of Berlin's train services to and from the city's southeast were halted for more than two hours due to the incident. (AP Photo/Michael Sohn)

Travellers wait for the departure of trains at Berlin's central train station in Berlin, Germany, Tuesday, Oct. 11, 2011. Police searched for further explosives after they found several explosives near the main train station and on railtracks outside Berlin. An arson attempt Monday on Berlin's central station using seven bottles filled with flammable liquid bundled together and linked to a fuse was thwarted at the last minute. A similar device exploded in a utility shaft next to a high-speed train line west of Berlin a few hours earlier, causing damage but no casualties, and halting train traffic there for the day. (AP Photo/Michael Sohn)

Police officers carry away paper bags with suspected explosive devices at the rail tracks nearby the Staaken station in Berlin, Germany, Wednesday, Oct. 12, 2011. Three more arson attacks have targeted Berlin's railway network, police said Wednesday. Two of the attacks were thwarted, while a third device caught fire but caused no injuries. It brings the total of attempted arson attacks in and around Germany's capital to six since Monday.(AP Photo/Michael Sohn)

Authorities have detected a total of 15 firebombs in seven different locations since Monday and hundreds of trains were delayed due to partial shut-downs, but no one has been injured in any of the arson attacks.

The attacks "are criminal, terrorist acts," German Transport Minister Peter Ramsauer said.

The Federal Prosecutors' Office, responsible for terrorism-related crimes, announced it was taking over the investigation from local authorities, conducting it on suspicion "of anti-constitutional sabotage."

said. Two other firebombs failed to explode near train lines in Berlin's south and center.

The other four arson attempts occurred Monday and Tuesday, with one of the devices exploding in a cable shaft along a high speed train link between Berlin and Hamburg, but causing no casualties.

A previously unknown leftist group has claimed responsibility for one of firebombs, saying it hopes to cause widespread disruption and that it opposes Germany's roles in the Afghanistan war. Police assume all the devices planted at the

"I have ordered police to be reinforced, with uniformed and plainclothes officers," Interior Minister Hans-Peter Friedrich said in a televised statement. "We will do everything to arrest the perpetrators."

One firebomb went off midday Wednesday on a train track in the western area of Staaken in Berlin, police spokesman Michael Gassen said. The device caught fire but didn't explode, he

same time, possibly Sunday. They believe some may have failed to explode thanks to persistent rain in the region since the weekend.

Officials said it was possible that more firebombs were still hidden.

German railway operator Deutsche Bahn promised to pay a euro100,000 ($136,000) reward for hints leading to the perpetrators.

A group calling itself the **Hekla Reception Committee Initiative for more Eruptions in Society** claimed responsibility for one of the first attacks, saying in an online posting. The group's name is an apparent reference to Iceland's Hekla volcano.

Germany is a large contributor to the NATO-led International Security Assistance Force in Afghanistan, with about 5,000 soldiers stationed in the north of the country.

In recent months, there also have been several arson attacks in Berlin blamed on unidentified leftist extremists.

One of them targeted a utility shaft at an important railway hub in the city's east in May, causing massive disruption that left thousands of passengers stranded.

More than 100 cars also have been torched in Berlin over the past several months, some of them blamed on vandalism motivated by animosity against the rich.

Al Qaeda: The End of a Legend?

By Prof. Michel Chossudovsky
Source: www.globalresearch.ca/index.php?context=va&aid=26908

Throughout the post 9/11 era, Al Qaeda and the "threat of Islamic terrorism" have played a central role in defining Washington's diplomatic agenda, shaping its rhetoric at World summits as well as establishing the contours of US military doctrine.

The pre-emptive "defensive war" doctrine against Al Qaeda and its alleged "State Sponsors" constitutes the foundation of America's post 9/11 National Security Strategy (NSS), first formulated in early 2002.

In the wake of 9/11, the Al Qaeda Legend became part of the mainstay of US foreign policy. Contained in the 2002 NSS is the notion of a "global jihadist network of terrorists" and "state sponsors of terrorism". The response of the US administration is to launch "a war of global reach", a "Global War on Terrorism" (GWOT):

> *"The war against terrorists of global reach is a global enterprise of uncertain duration. ...America will act against such emerging threats before they are fully formed.*
> *...Rogue states and terrorists do not seek to attack us using conventional means. They know such attacks would fail. Instead, they rely on acts of terror and, potentially, the use of weapons of mass destruction (...)*
> *The targets of these attacks are our military forces and our civilian*

> *population, in direct violation of one of the principal norms of the law of warfare. As was demonstrated by the losses on September 11, 2001, mass civilian casualties is the specific objective of terrorists and these losses would be exponentially more severe if terrorists acquired and used weapons of mass destruction.*
> *The United States has long maintained the option of preemptive actions to counter a sufficient threat to our national security. The greater the threat, the greater is the risk of inaction— and the more compelling the case for taking anticipatory action to defend ourselves, (...). To forestall or prevent such hostile acts by our adversaries, the United States will, if necessary, act preemptively."*

The underlying objective of the 2002 NSS was to present "pre-emptive military action" --meaning war as an act of "self-defense" against two categories of enemies, "Rogue States" and "Islamic terrorists", both of which were said to possess "Weapons of Mass Destruction". The "Rogue States" are also defined as "State sponsors" of terrorism.

The 2002 NSS as well as subsequent National Security

documents identified a list of "Axis of Evil" countries which had been singled out for preemptive military intervention under the "Global War on Terrorism". These included Iraq, Iran, Sudan, Syria, Libya, North Korea.

While former enemies Russia and China of the Cold War era were not officially designated as part of the "Axis of Evil", they were, nonetheless, included (in several military documents) in the list of targetted countries for military intervention.

From the outset in 2001, a vast Public Relations campaign was launched by the Pentagon with a view to shaping and manipulating World public opinion. The PR stunt consisted in leaking reports on links or relations between Al Qaeda and its alleged State sponsors (e.g. How Saddam was supporting bin Laden, etc). The objective was to justify preemptive military actions against countries which were "harboring the terrorists".

There was no truth or rationale in these statements emanating from higher authority. "Going after Bin Laden" became part of an unbending consensus. Fear and insecurity prevailed over common sense. What we are dealing with is an outright and blind acceptance of the structures of power and political authority.

In the wake of 9/11

In the immediate aftermath of the 9/11 attacks, Afghanistan was accused of harboring Al Qaeda leader Osama bin Laden, the alleged mastermind behind the 9/11 attacks.

Afghanistan was identified as a "state sponsor of terror". The 9/11 attacks were categorized as an act of war, an attack on America by a foreign power. The right to self-defense was put forth.

The US-NATO aggressor was portrayed as the victim.

On September 12, less than 24 hours after the attacks, NATO invoked for the first time in its history "Article 5 of the Washington Treaty - its collective defence clause" declaring the 9/11 attacks on the World Trade Center (WTC) and the Pentagon "to be an attack against all NATO members."

There was foreknowledge of 9/11. Military analysts will confirm that the war on Afghanistan launched on October 7, 2001, was planned well in advance of 9/11.

Public opinion was led to believe that war preparations got underway on September 12th on the spare of the moment, that it was the result of indignation and outrage.

Homeland Security

"The Homeland" emerged as a political concept in the wake of 9/11 leading to the establishment of the US Department of Homeland Security.

The doctrine of pre-emptive war and "defense of the Homeland" are intimately related. Al Qaeda, the alleged perpetrator of the 9/11 attacks threatens "the American Homeland" with the support of the State sponsors of terrorism.

The late Osama bin Laden was defined as the Bogeyman, the "Number One enemy of America" who threatened the Homeland.

The objective was to sustain the illusion that "America is under attack" by Al Qaeda. Washington has a self-proclaimed holy mandate to extirpate Islamic fundamentalism and "spread democracy" throughout the world. The logic of the "outside enemy" and the evildoer, allegedly responsible for American civilian deaths, prevails over common sense. In the inner consciousness of Americans, the attacks of September 11, 2001 justify acts of war and conquest, directed against the State sponsors of terrorism, including Afghanistan, Iraq and Iran.

In this regard, the post 9/11 "American Inquisition" as an ideological construct, is, in many regards, similar to the inquisitorial social order prevailing in France and Spain during the Middle Ages. The inquisition, which started in France in the 12th century, was used as a justification for conquest and military intervention.

The Global War on Terrorism (GWOT)

Terrorist acts are said to be conducted by non State jihadist organizations, which allegedly are supported and abetted by the governments of several Muslim countries, described as

the "State Sponsors" of terror.

Afghanistan, Iran, Iraq, Syria,

Pakistan and Saudi Arabia were accused by Washington of supporting Al Qaeda.

9/11 remains the pretext and justification for waging a war without borders. In the wake of the NATO sponsored "Liberation" of Libya (August 2011), Syria and Iran, both identified in US military doctrine as State Sponsors of Terror, constitute the next phase of the US-NATO military roadmap.

Al Qaeda portrayed as a Sunni fundamentalist network is increasingly upheld as a global jihadists organization, a base, a decentralized network comprised of affiliated national and regional organizations.

The "Global War on Terrorism" is established with a view to defending the American Homeland as well as the "Western Way of Life". It requires "going after" the terrorists, using advanced weapons systems including nuclear warheads. It upholds a pre-emptive religious-like crusade against evil, which serves to obscure the real objectives of military action.

The American people's acceptance of this crusade against evil is not based on any rational understanding or analysis of the facts. The lies underlying 9/11 are known and documented. The evidence amply confirms that Al Qaeda was established with the support of the CIA in liaison with Pakistan's Military Intelligence, the Inter-Services Intelligence (ISI). From the Soviet-Afghan war to the present, Al Qaeda and its affiliate organizations constitute US sponsored "intelligence assets" used in the implementation of CIA covert operations.

America's inquisition is used to extend America's sphere of influence and justify military intervention, as part of an international campaign against "Islamic terrorists". Its ultimate objective, which is never mentioned in press reports, is territorial conquest and control over strategic resources.

Ten Years Later: Continuity of the 9/11- Al Qaeda Presidential Discourse

The GWOT dogma was initially enunciated and formulated by Washington's neoconservative think tanks. It was embodied into US military doctrine. It remains part of a bipartisan consensus. From George W. Bush to Barack Obama it has become a central theme in presidential speeches and White House press conferences:

[George W. Bush, Septmeber 2001]
"We've been warned there are evil people in this world. We've been warned so vividly. ... And we'll be alert. Your government is alert. The governors and mayors are alert that evil folks still lurk out there. As I said yesterday, people have declared war on America and they have made a terrible mistake. ... My administration has a job to do and we're going to do it. We will rid the world of the evil-doers," (George W. Bush, CNN, September 16, 2001, emphasis added)

[Barack obama, September 2011]
"Make no mistake, they will keep trying to hit us again, but as we are showing again this weekend we remain vigilant. We are doing everything in our power to protect our people... They [the terrorists in Afghanistan and Iraq] want to draw us into endless wars, sapping our strength and confidence as a nation. But even as we put relentless pressure on al-Qaeda we are ending the war in Iraq and beginning to bring our troops home from Afghanistan. After a hard decade of war it is time for nation building here at home," (Barack Obama, September 2011, Free Internet Press: President Obama: Al-Qaeda Threat Still Remains :: Uncensored News For Real People, September 11, 2001)

The objective of the "Global War on Terrorism" launched in September 2001 was to galvanize public support for a Worldwide campaign against heresy. For the last ten years, an

understanding of fundamental social and political events is replaced by a World of sheer fantasy, where "evil folks" are lurking.

Meanwhile, in the wake of the 9/11 attacks, Al Qaeda has established numerous affiliate organizations throughout the Muslim world.

Al Qaeda has mushroomed. Wherever the CIA is conducting counterinsurgency operations, there are Al Qaeda affiliated organizations including:

- Al Qaeda in Iraq (AQI),
- Al Qaeda in the Arabian Peninsula (AQAP),
- Al Qaeda in the Islamic Maghreb (AQIM),
- The Libya Islamic Fighting Group (LIFG),
- Al-Qaeda in the Arabian Peninsula, (which comprises Al Qaeda in Saudi Arabia, and Islamic Jihad of Yemen),
- Al-Shabaab (Mujahideen Youth Movement) in Somalia,
- Egyptian Islamic Jihad,
- East Turkestan Islamic Movement in Xinjiang, China, etc.

Wherever Al Qaeda has set up shop, the US has waged counterinsurgency operations under the banner of the "Global War on Terrorism". There are indications that many of these Al Qaeda affiliates were set up with the support of the CIA, using Pakistan's Inter Services Intelligence (ISI) as a go-between.

Wherever Al Qaeda is present, where "bad guys are lurking", America has an obligation to intervene on behalf of "the international community". The terrorist threat is used as a pretext to interfere in the internal affairs of sovereign countries, including the sending in of special forces and the conduct of drone attacks, without an actual declaration of war. These types of operations are described in the Project of New American Century (PNAC) as constabulary functions.

In turn, large scale military campaigns have been waged in several countries as part of the Global War on Terrorism (GWOT). The wars on Afghanistan and Iraq were conducted under the banner of the Global War on Terrorism. Both the Afghan and Iraqi governments were identified as "state sponsors of terrorism".

The Islamic Republic of Iran is also said to support Al Qaeda. The Administration's pre-emptive war doctrine hinges upon this alleged relationship between non state terrorist organizations and their terrorist State sponsors. It is understood, pari passu, that the state sponsors of terrorism, whoever they be, are also responsible for the 9/11 attacks, namely for having supported and abetted Al Qaeda.

The Tehrik-e-Taliban Pakistan's Expanding Western Connections

By Raffaello Pantucci
Source: http://www.jamestown.org

As the United States breathed a sigh of relief that the 10th anniversary of 9/11 had passed without any major incident, the U.S. Justice Department announced that three men had pled guilty to charges of trying to smuggle a member of the Tehrik-e-Taliban Pakistan (TTP) into the United States. As one of the suspects, Irfan ul-Haq, put it, it was "not their concern" what the smuggled individual might "want to do in the United States – hard labor, sweep floor, wash dishes in a hotel, or blow up. That will be up to them." [1] The men were apparently part of a network of people smugglers that was willing to help Pakistani TTP members enter the United States, highlighting once again the menace posed by the group to the United States, as perceived by the American security community.

The histories of the three men at the heart of this case are unclear. They were arrested on March 10 in Quito, Ecuador, as part of an operation by American forces (NTN24 [Bogata], September 20, 2011). In court documents released later, prosecutors laid out a case showing that from January 2011, undercover agents dispatched by a law enforcement agency

approached two of the men in Quito, Irfan ul-Haq and Qasim Ali, to inquire about smuggling a fictitious person from Pakistan into the United States. The initial approach was to ul-Haq, who directed them to talk to Ali in order to obtain fraudulent documentation. The two men then met and spoke with the undercover agents a number of times to work out the details and a month later ul-Haq seems to have brought a third man, Zahid Yousaf, into the conspiracy. [2] It was at about this time that one of the undercover agents told the suspects he was a member of the TTP and that the individual who was intended to be smuggled was also a member – information that elicited the callous response highlighted before. [3] While it is unclear whether the suspects were actually supportive of TTP aims, their capacity to smuggle individuals out of Pakistan and into the United States using fraudulent documentation would have provided the TTP with a useful network were they able to connect with it. At one point the suspects provided the undercover agents with a sample fake British passport and ul-Haq boasted of having contacts in Pakistani immigration that could provide exit stamps for people who were wanted by security services.

This in turn highlights the general growing concern about the increasing internationalization of the TTP. On July 29 the UN Security Council agreed to add the TTP to the list of proscribed groups. [4] In an electronic interview with Terrorism Monitor, Richard Barrett, coordinator of the UN's al-Qaeda-Taliban Monitoring Group, said the move was "an important symbolic consequence" that showed "the international community as a whole condemns [the TTP] without reservation. This universal condemnation acts as an encouragement to all those who are opposed to TTP and have suffered from its violence." [5] The move follows earlier decisions to proscribe the TTP by Pakistan, the UK, the United States and most recently, Canada. [6] The threat to the West was brought into focus when Waliur Rehman, the head of TTP in South Waziristan, announced: "Soon you will see attacks against America and NATO countries,

and our first priorities in Europe will be France and Britain" (al-Arabiya, June 28).

This is not the first time the group has threatened the West and it has attempted in the past to carry through on these threats. Back in January 2008, the group was connected to a plot to attack Barcelona, Spain and other possible EU targets by deploying a network of twelve men, ten Pakistanis and two Indians. According to prosecutors and an informant within the cell, some of the men had undergone training with TTP in Waziristan. The informant reported that the then-TTP leader Baitullah Mahsud had specifically identified him as a potential suicide bomber. The link to the TTP was confirmed in August 2008 when TTP spokesman Maulvi Omar released a video in which he stated, "the [foiled attack] in Barcelona was conducted by twelve of our men. They were under pledge to Baitullah Mahsud and the TTP has already claimed responsibility because [of] Spain's military presence in Afghanistan." [7]

While this plot was disrupted, responsibility for Faizul Shahzad's failed car bombing in Times Square in May 2010 was claimed by TTP soon afterwards in a video that featured footage of Shahzad at a TTP camp. According to the indictment that was handed down against him, Shahzad admitted to having trained alongside the group in Waziristan in December 2009. Having returned to the United States, Shahzad received some $5,000 in February 2010 to help him carry out an attack there. He then went about purchasing a gun and locating the necessary equipment to build a car bomb. [8]

While it is unclear whether Shahzad had any contact with TTP networks in the United States, the existence of these networks now seems to have been confirmed. Aside from the group arrested in Quito, FBI agents in Miami moved in May to disrupt a network based around a pair of imams in Florida who were allegedly running a fundraising network to send money to the TTP. According to prosecutors, the group sent at least $50,000 to Pakistan and discussed the terrorist attacks it was going to

support with their contacts there (Miami Herald, May 14). This came after an August 2010 operation codenamed "Samosa" in Ottawa, Canada that was mounted by Royal Canadian Mounted Police forces to disrupt a network that was sending funds to the TTP and accumulating bomb making material locally (National Post, July 5).

Successful attacks have yet to emerge from these TTP support networks, but it seems likely that more plots will follow in the future. Given the ongoing trickle of foreigners drawn to Pakistan and the TTP's ongoing campaign at home against the Pakistani state and its American backers, it is likely that this connection will continue to be a focus of concern for Western intelligence agencies.

Notes:

1. USA vs. Irfan ul Haq, Factual Proffer in Support of Guilty Plea, filed September 12, 2011. http://www.investigativeproject.org/documents/case_docs/1683.pdf.
2. USA vs. Irfan ul Haq, Qasim Ali, Zahid Yousaf, Indictment filed March 3, 2011. http://www.investigativeproject.org/documents/case_docs/1678.pdf.
3. USA vs. Irfan ul Haq, Factual Proffer in Support of Guilty Plea, filed September 12, 2011. http://www.investigativeproject.org/documents/case_docs/1683.pdf.
4. http://www.un.org/sc/committees/1267/NSQE13211E.shtml
5. Author's email interview with Richard Barrett.
6. Public Safety Canada – Currently Listed Entitities, http://www.publicsafety.gc.ca/prg/ns/le/cle-eng.aspx#TTP.
7. http://www.nefafoundation.org/multimedia-intvu.html
8. USA vs. Faisal Shahzad, indictment, http://www.cbsnews.com/htdocs/pdf/Shahzad_Faisal_Indictment.pdf .

Raffaello Pantucci is a Consulting Research Associate with the International Institute for Strategic Studies (IISS) and an EU Science and Technology Fellowship Programme (China) Research Fellow. He is a regular contributor on terrorism issues for newspapers, magazines and journals on both sides of the Atlantic, and is currently working on a book looking at the roots of the British Jihad.

Bringing Shari'a Rule to Yemen and Saudi Arabia: Al-Qaeda in the Arabian Peninsula's Post-Revolution Strategies

By Murad Batal al-Shishani
Source: http://www.jamestown.org

Since it began last February, the youth-led peaceful revolutionary movement in Yemen demanding an end to President Ali Abdullah Saleh's regime has provided a political alternative to the Yemeni people which has marginalized the rhetoric of al-Qaeda in the Arabian Peninsula (AQAP). At the same time the violent response of the Yemeni regime to all oppositional social and political forces has increased the chaos and tension in the country. As a result many ungoverned areas have emerged and the absence of the state has fuelled AQAP's re-emergence on the political scene of Yemen.

Before the revolution, AQAP had a strong presence in three governorates: Abyan, Ma'rib and Shabwah. Since the movement re-emerged AQAP has expanded in new areas such as Hadramawt and Aden. Other areas have witnessed limited but active cells of AQAP, such as in the capital Sana'a and the Zaidi Shiite dominated al-Jawf and Sa'da regions. [1] In certain areas AQAP has established Shari'a rule and even installed checkpoints.

Alongside the geographical expansion, AQAP has benefited from the instability in Yemen by adopting various strategies to present their ideology as an alternative to the Saleh regime. AQAP has also kept the pressure on the Saudi royal family in neighbouring Saudi

Arabia. In an audio message discussing President Saleh's policies, AQAP ideologue Adel al-Abbab (a.k.a. Abu al-Zubair al-Abbab) said: "Ali Abdullah Saleh, [it] is not [a] secret to you that AQAP is founded only for the recovery of Shari'a [which is] replaced by secularism. And you should know that the cause of wielding a weapon in your face is not for [the] sake [of] influence, money or a position, but to implement Shari'a, which does not exist under your rule." [2]

Local Strategies

AQAP has started to present itself as part of the "Arab Spring" in Yemen. Yemeni Journalist Abdulrazaq al-Jammal spent several days as a guest of AQAP in the areas they control and has interviewed one of the prominent leaders of the movement, Fahd al-Quso. [3] Al-Jammal asked the AQAP commander what led the movement to attempt to control the Abyan Governorate after avoiding public appearances previously. Al-Quso replied that the move came about because "All the Yemeni people refused this regime and expressed their absolute desire to end the rule of Ali [Abdullah] Saleh and combined their efforts with us to this. And we are an integral part of this people's journey towards dignity and freedom under the banner of Islam" (Al-Quds al-Arabi, September 19).

In order to establish their influence in the areas they control AQAP started to rule these areas by Shari'a, establishing Harakat Ansar al-Shari'a (Movement of Shari'a Supporters) to further this effort. This movement, as AQAP ideologue al-Abbab explains, aimed to win the locals' support and "attract them to Shari'a rule." By this movement AQAP hopes to turn Shari'a rule "into popular action instead of keeping it as an elite one…by providing public services and solving people's problems" said al-Abbab. [4] Al-Quso confirms this by saying that "all Muslims are supporters of Shari'a, and Ansar al-Shari'a includes all the mujahideen who [work for] Shari'a to rule in the country" (Al-Quds al-Arabi, September 19).

AQAP has formed Ansar al-Shari'a from tribesmen in the areas where they are imposing Shari'a rule. Al-Jammal noticed that in Abyan "many of those who are members of Ansar al-Shari'a are from the inhabitants of [Ja'ar] province, so any internal fighting will certainly have effects that extend to the coming years in a country where taking revenge is on the top of the list of troubles" (al-Wasat, September 14).

By relying on local elements, AQAP was able to gain support on the ground, but the absence of the state also played a major role in achieving this support. According to al-Jammal, in the areas where AQAP imposed Shari'a rule, they "succeeded in creating a status of amiability between them and the inhabitants of those regions, especially that many of the fighters belong to those regions. The model of al-Qaeda is very perfect in comparison with the model of the Saleh regime. In addition to the unprecedented security stability, the organization presents some services to the citizens, especially in the aspect of livelihood…[and] many crimes like murders, stealing [and banditry] have disappeared dramatically since the Ansar al-Shari'a entered their areas" (al-Wasat, September 18).

During their presence in the Jaar directorate and many of the regions of the Abyan province, the fighters of the Al-Qaeda organization were able to create a status of amiability between themselves and the inhabitants of those regions in particular because many of the fighters are from those regions. The model of Al-Qaeda is perfect in comparison with the model of the Saleh regime. In addition to the unprecedented security stability, the organization presents services to the citizens, including livelihoods. I have seen lists given to me by the media officials of the organization, which consist of the types of supplies that are presented to large numbers of citizens. There are even two pickups that have been assigned to distribute water to the houses, which is considered a great thing for a people who never depended on their government. The citizens of the Jaar directorate say that many crimes like murders and stealing have disappeared dramatically

since the Ansar Al-Sharia entered their areas.

Regional Strategies

Since Saudi and Yemeni jihadists merged in 2009 to found AQAP, most jihadist literature considers the proximity to Saudi Arabia a causal effect for the presence of jihadists in Yemen. Jihadists desire to use Yemen as a launching pad against Gulf States, but as AQAP is unable presently to launch an open campaign as it did between 2003 and 2007 on Saudi soil, the movement has resorted to sending small cells from Yemen or recruiting Saudis to assassinate the Kingdom's officials and royal family members. According to Saudi border guards in the Jizan region, they have managed to stop more than 25,000 illegal entries into Saudi Arabia from Yemen and thwarted the smuggling of close to 10,000 weapons in September alone (al-Jazeera, October 4).

Last August, Saudi Khadir al-Zahrahni and two others attacked Interior Minister Prince Muhammad bin Nayf's palace in Jeddah. Al-Zahrani was killed and the other two were arrested by Saudi forces (Arabnews.com, August 6; al-Jazeera, August 6). This attack came on the second anniversary of an assassination attempt on Prince Nayf's son, Assistant Interior Minister for Security Affairs Prince Muhammad bin Nayf, by a suicide bomber. The assassination tactic is preferred by AQAP with their inability to launch an open confrontation with Saudi authorities (see Terrorism Monitor, November 25, 2009).

The Saudi position towards Saleh was perceived among Yemenis as support for the regime. AQAP in turn started to use more "political" rhetoric directed towards the Saudi royal family. Well-known AQAP ideologue Ibrahim al-Rubaish released an audio message addressing Prince Nayf after the attack on his palace and threatened him of the consequences of the Arab Spring: "Today we are in an era of revolution. These revolutions succeeded in overthrowing the most repressive and tyrannical of Arab regimes, those which used to teach Nayf and his criminal gangs how to use methods of repression are collapsing by the gatherings of the youth." [5]

Al-Rubaish who previously set seven conditions to end the fight against the Saudi royal family, has listed significant new politically-oriented demands in addition to the historic demands of the Saudi Arabian jihadists. These demands include "the expulsion of infidels from the Kingdom and the nullification of all man-made laws which fill your various ministries, those which you call with various names, such as rules and regulations". Further demands by al-Rubaish include:

"Restore to the Islamic judiciary its usurped independence and respect, and grant its judges the right to investigate all cases, allowing its rulings to be carried out on all people, noble or ignoble, the rulers or their subjects."

"Grant the Presidency for the Promotion of Good and Prevention of Vice total jurisdiction to carry out their tasks, with both their hands and their tongues as suitable, against individuals, princes, establishments, and government institutes."

"The Islamic propagators and students [are] to be granted the freedom to speak the truth, fearing no repercussions from anyone, and that the Interior Ministry have no authority to plant or dismiss Friday preachers."

"Release all people in your prisons who are not serving criminal sentences."

"Do not stand as an obstacle to those who seek to defend and aid the Muslims in Palestine, Iraq, or any other Muslim land with their lives, wealth, or tongues." [6]

Conclusion

AQAP, like most Salafi-Jihadist groups, has been demonstrating a strong ability to adapt to the pressures they are experiencing; most notably the pressure the Arab Spring has put on such movements to present a political alternative to the Arab masses.

This being said, AQAP has adopted new strategies locally and regionally that aim to gain local support as well as to assist in representing the group as an integral part of the youth movement. AQAP aims to present Shari'a rule (according to their

understanding of it) as the most suitable alternative to Arab political systems. This means that the defiant and violent response of Arab regimes, including Yemen, to peaceful protests demanding political change, will ultimately be the major factor in restoring al-Qaeda and affiliated groups' status as defenders against these regimes.

Notes:
1. Adel al-Abbab, in a Pal Talk conversation released on April 22, gave details on AQAP activities in these areas (http://www.ansar1.info/showthread.php?t=32700). See also Murad Batal al-Shishani, "Is al-Qaeda establishing a small Shari'a emirates in Yemen?" Open Democracy, May 19, 2011.
2. http://aljahad.com/vb/showthread.php?t=381, September 10, 2011.
3. For further information about al-Quso see Militant Leadership Monitor, August 27, 2010.
4. http://www.ansar1.info/showthread.php?t=32700
5. Ibrahim Sulaiman al-Rubaish: Yokhrboon Beoutahm Be Aydeehm (Destroying Their Homes with Their Own Hands), http://as-ansar.com/vb/index.php, August 29.
6. Ibid.

Murad Batal al-Shishani is an Islamic groups and terrorism issues analyst based in London. He is a specialist on Islamic Movements in Chechnya and in the Middle East.

Shame Honor Cultures: The Root Cause of Radicalization
Review on Rik Coolsaet: Jihadi Terrorism and the Radicalisation Challenge

Source: http://www.citizen-times.eu/shame-honor-cultures-the-root-cause-of-radicalization/#.TpsHc3Lw1v0

someone become operational, that is what turns the faucet on which unleashes the violent rage of the individual, either in the collective or as a lone wolf. It seems that we are still in the early stages of understand such a complex phenomena. Jihadi Terrorism and the Radicalisation Challenge concerning European and American experiences is an important updated second edition volume edited by Rik Coolsaet. He is eminently qualified to undertake this task as Professor of International Relations at Ghent University, Belgium as well as Senior Associate Fellow at the Egmont Institute in Brussels. He writes a stirring account of the recent problems concerning jihadi terrorism and its precursor phenomenon, radicalization.

There are many nuggets of information and thoughts that are found in this new and improved text. There are five new voices too: Leena Malki, Clark McCauley, Robert Lambert, Marc Sageman and most especially Lorenzo

One of the most salient issues concerning radicalization and jihadi terrorism is what makes

Vidino. Authors Cesari, Crenshaw, Fraihi, Peters, Roberts, Roy and Van de Voorde have either completely written new essays for this edition or have revised and update their former contributions of 2008 when the first edition appeared.

Rik Coolsaet (2011): Jihadi Terrorism and the Radicalisation Challenge: European and American Experiences. Second edition, Ashgate.

'Radicalization' means "to cause (someone) to become an advocate of radical political or social reform" and it derives from the Latin radix. However, with this second volume I couldn't help but associate to another word related etymologically – 'radish' because this root is eaten raw and is pungent, like the crudeness of the violence of the jihadis.

There is much that I agree with in this volume, for example "the ideological narrative is not the root cause of radicalization" and that radicals are not produced in a vacuum, the context is extremely important. I would hasten to add that culture plays a significant role. Furthermore the "intersection of personal history, and that enabling environment" such as in the case of Muhammad Bouyeri who brutally murdered Theo Van Gogh is crucial to understanding what unleashed his regression into such psychotic behavior.

The term 'humiliation' appears along with another concept 'code of honor' throughout the volume as an emotional root of the problem. Yet the key emotion really is shame which was missing. The context of these environments or breeding grounds for radicalization occur in shame honor cultures where the female is completely devalued. Even in the West there are pockets of shame honor cultures or families, which helps to explain the converts draw to jihad. The female suicide bombers merely internalize male hatred of the female as self-hatred and under the guise of a suicide bombing operation can mask their complete lack of social standing and value as well as years of blatant abuse and manipulation. This is why the issue of honor killing and the

suppression of women's rights is so important because, for example, the Centre for Social Cohesion in Britain did geomapping of areas where they found honor killing and jihadis. Lo and behold, they were nearly the same areas. Yet few wish to connect the dots between the behavior and the ideology. The ideologies act like a girdle for a very weak and fragile, bullying personality of an emasculated male.

True, the concept of social bonding is discussed in a series of these essays, especially Sageman's work in which he refers to the 'bunch of guys' phenomena or Malkki on the radical left terrorist campaigns in Europe and the US. However, social bonding and leaderless jihad can not have arisen de novo. There have to have been underlying major characterological psychopathology which contributed to this pathological social bonding. Elsewhere I have argued that the first bond in life with the mother is the attachment pattern for later in life. In shame honor cultures the maternal bonding is most problematic at best, again because the female is completely devalued and abused.

Van de Voorde cites Jerrold Post's work while not naming his Political Paranoia text per se, nonetheless the fact that paranoia surfaces in this discussion, inadvertently links back to the mother once again. This makes for prime problems in future social bonding. We see this in the importance of kinship and friendship bonding about which Coolsaet writes. Muriel Degauque, the female suicide bomber convert, exemplifies this bond as well. There also is discussion of attachment to a role in Horgan and Taylor's essay on Disengagement, De-radicalization and the Arc of Terrorism. This attachment can be understood as a kind of metaphor for a problem in social bonding and attachments. Professor Diego Gambetta, who is not a contributor to this volume, is one of the few counterterrorist experts who has raised the question of jihadis being schizoid, meaning forming attachments to hard, cold weapons as well as computers and cyber space rather than being able to bond to people without resorting to violence.

Terrorists lack empathy.

Along these lines it is interesting to note that the work of Jessica Stern is drawn upon but not her most recent moving memoir Denial. The defense mechanism of denial points to how highly dissociated terrorists are. Paranoia by definition means that one is dissociated from reality and seeks to defend against it because it is too painful to acknowledge vulnerability and death.

The question of recidivism looms large for those working to rehabilitate jihadis from lapsing back into terrorist behavior. A future area of inquiry which might be helpful to explore is the recidivism of sex offenders. Jihadis have very problematic fetishes and psychosexual problems. We see this

in their choice of introducing bombs into breast implants, the anus and even underwear to say nothing of shoe, which speaks to a developmental obsession and obviously a perversion.

Nevertheless Coolsaet and his colleagues have done an admirable job of informing the expert and lay readers about the challenges which we continue to face. Perhaps a third future volume might include recent developments in neuroscience, biometrics and even the area of the unconscious. This volume makes a great reader for students of this subject matter.

Updates on Balkan Islamic extremism

By Ioannis Michaletos
Source: http://rimse.gr/?p=343

The Balkan Islamic extremism, although it is considered as a taboo theme by most of the mainstream media, is still an issue debated in high-level and sensitive discussions between policy makers across the world, due to importance of the region as a historical fault line between the West and the East, in parallel with the ongoing interstate competitions that are cantered around South-eastern Europe.

In a leaked cable of the U.S State Dept, dated back in 2005, the then Ambassador of the States in Bulgaria, John Beyerle noted that "Foreign international organizations and institutions praise Islamic extremism in Bulgaria…the official Islamic charities depend financially on them…Muslim Bulgarian women in Southern Bulgaria are imitating Arabic looks". The cable was classified as secret and events that have happened over the past few years have testified the existence of the aforementioned findings.

According to information by various international security services, in the Balkans and in Bulgaria in particular, quite a few Islamic extremist groups are functioning and a number of Arabic descent Bulgarians are assisting organizations such as Hezbollah in financial terms by diverting a part of

the profits they make through trafficking, car theft and narcotics trade.

Moreover, Chechen Islamic extremists operate in Bulgaria and deal drugs sending capital to their brethren in the Caucasus. The Kurdish KGK is also active in Bulgaria and Iranian diplomats have been noted taking part into radicalizing segments of the Pomak minority in the South of the country which is primarily Muslim.

In Kosovo, a recent established political-social movement named "Bashkohu", which means "participation", strives for the acceptance of the hijab in local schools and it includes amongst its circle groups of devout Muslims that want to openly declare the region as a "Muslim territory" and away from European norms and canons. Although the movement was not able yet to acquire the necessary clout to implement its ideas, the overall activity of certain Muslim circles -that has been extensively researched in previous articles and reports- is still gathering pace and it is estimated that as soon as NATO and international forces exit the Province; then it will manifest in an explicit form.

Back in 2009 an Albanian from Kosovo that lived in New York, was arrested by the American authorities as an Al Qaeda member who aimed to kill American troops in the Balkans.

The 23 year old Kaziu Betim went to Cairo in 2009 and came into contact with Pakistani Jihadists. In parallel he tried to recruit himself into the Al Shabab Somali terrorist group. His plan foiled when the FBI noticed his ventures and was subsequently arrested. Since 2006 there have been cases both in USA and in Germany involving aspiring Jihadists from Kosovo and at the same time there is constant surveillance of the activities of Middle Eastern sponsored individuals and NGO's in the region by at least 11 different intelligence services. The amount of attention Kosovo is receiving regarding the threat by radical Islam is an issue that has not been thoroughly researched by mainstream media and remains for the moment the task of specialized analysis agencies and political risk consultancies. In early July 2011, a significant number of Islamists gathered in the streets of Pristina and staged street prayers, as well as, demonstrations in order to demand the creation of a mega Mosque in the city centre, which hosts quite a few. What the real demand was, that a new large Mosque should be built in order to cover the view of the Catholic Church nearby. The demonstrators held flags of Hamas and many of those were dressed in Middle Eastern fashion.

The issue of radicalized Islam is in reality a pan European issue and not a Balkan one. In France and in Belgium the governments have passed laws prohibiting the use of the Burqa and niqab in public spaces and in Switzerland in a 2009 referendum, there was 58% nay concerning the creation or not of new Mosques in the country. In the UK, since 2007 there have been certain restrictions by the Ministry of education regarding the dress of students in public schools, whilst a recent poll by the French daily "Le Monde" revealed that 42% of the French public and 40% of the German one view Islam as a "threat", and up to 70% view the integration of the Muslim citizens as "problematic" for the French and German societies.

In November 2010 the German Chancellor Merkel admitted the collapse of multiculturalism in Germany and in parallel similar concerns were raised by the British Premier Cameron. If one adds the recent policies of Sarkozy in France and the Italian governmental coalition in Rome, as well as public and political sentiment in Austria, Netherlands, Belgium and Finland; one can easily comprehend that Islam as a religion and not only its radicalized segment will soon face tremendous challenges that can be easily summoned as "Integrate to the Western society or isolate yourselves". In that respect the issue of extremism in the Balkans of Islamic nature, will come about as a focal European issue.

For instance the recent veto by Netherlands and Austria against the inclusion of Bulgaria and Romania into the Schengen treaty was based on the assumption that the Balkans are the main gate under which Muslim illegal immigrants venture up to Central Europe. Due to reasons of political correctness in the Brussels, the terms "custom controls and organized crime " were mentioned although the hard truth was that certain European states are terrified that yet another free access corridor will open up for a large number of illegal aliens from Afghanistan-Pakistan and other countries that congregate in Turkey before trespassing the Balkans on their way to specific EU states.

In short, there are three main nucleus of power relating to Islamic affairs in the Balkans. The first one is the so-called "Neo Ottoman" one being directed by Ankara and from Istanbul in particular through the use of the Turkish ministry of foreign affairs and the myriads of supported government institutions and charities, aiming at creating a Turkish influenced Balkan territory mostly for nationalistic reasons and not exclusively related to religion per se. A second power block is the Middle Eastern-Wahhabi one, been supported by Saudi Arabia and Kuwait especially, aiming for the "Islamization" of the region en route for the Western European countries. A third and lesser player is Iran that still actively tries to gain footholds of influence mostly for

purposes of maintaining a global reach and as deterrence against its perceived enemies from the West.

The real issue here is the non-existent realistic approach by the Western countries and especially USA. Although the subversive nature of the activities of many groups and individuals across the Balkans has been noted, nevertheless the pervasive nature of political correctness, along with an irrational "cold war era" fear of the an impeding Russian (Soviet) "invasion" to the Mediterranean, has paralyzed the dynamic approach to the issue that in the long-term will neutralize NATO and will facilitate inter-ethnic competition in the whole of Europe. Unfortunately for many American policy makers, history is not understood as a dynamic all encompassing procedure and it is viewed rather from a mechanistic approach under which someone can actually both predict and change the course of events to its suit. The only certainty in history is that it does not favour lack of reason and that mistakes are due to be paid sooner or latter.

Note: Radicalism of Islamists in the Balkans is related directly to terrorist cells across the world and in turn those are indirectly connected with powerful criminal gangs of a translational level. Therefore, political mismanagement or overlook of the above regional issue has global consequences on security terms, a dynamic which is accelerated by the interconnection of all political-societal forces in the world nowadays due to the globalization process and the ease in communications and transport. In simple terms, the difficult years are ahead concerning the coming clash of civilizations which is gathering pace since the end of the bipolar world in the early 90's and it is reaching a climax, judging by the ethnic and religious based conflicts nowadays. Balkans seems to be an ideal ground where this clash has already been proven and it still remains a volatile region with tensions simmering just below the surface of political correct haziness.

FBI training elite deep-diving counterterrorism unit
Source: http://www.cnn.com/2011/09/28/us/fbi-dive-team/

To bolster its counterterrorism capabilities, the FBI has created an elite group of special agents trained to track terrorism underwater.

Next year the ten-member Technical Dive Team will begin searching for evidence left behind by international terrorists in waters contaminated by chemical, biological, radiological, or nuclear waste.

Pointing to the 2008 attack in Mumbai, India where terrorists entered the city by boat, supervisory special agent James Tullbane, a Technical Dive Team member, said, "There have been enough scenarios recently," to justify the creation of the special unit.

"If you look at Mumbai and you look at various international incidents that occurred where there's attacks on American civilians or attacks on American interests where water has been involved, … we determined that we really do need to expand our capabilities," he said.

The Technical Dive Team was created last year with the primary mission of gathering evidence following a terrorist attack to help find and prosecute those responsible.

Unlike existing FBI dive teams, the Technical Dive Team can operate in waters contaminated with

hazardous materials and investigate far deeper than others.

Instead of using air tanks, the divers use a hose

connected to a surface supply system.

"It not only provides the air, it collects the air that you exhale and brings it back to the surface," explained Michael Tyms, the team's program manager.

The divers are also equipped with special dive suits that come with a steel helmet so they can operate safely in contaminated water without being exposed to dangerous toxins. These suits also enable divers to reach depths of 300 feet, compared to 130 feet, which is considered safe for most recreational dives.

The team is currently in the midst of its two-year training program and will not be fully operational until next year when it completes all of its certifications, but this has not stopped the team from performing some less dangerous missions.

Most recently, the team was called in several weeks ago to retrieve a large shipment of drugs that had been stashed away in a sunk "narco sub." The U.S. Coast Guard had initially spotted the vessel off the coast of Honduras, and the crew quickly sank the semi-submersible vessel before they were apprehended.

"The thought was, 'Hey, somebody could go down and retrieve those narcotics,'" said Tyms. "So [the Coast Guard] called us and we said, 'Yep that's the type of mission we could do.'"

Using sonar and their special dive suits, the FBI dive team was able to successfully find and retrieve nearly 15,000 pounds of cocaine hidden in the sub's cargo hold eighty-feet below the surface.

"Once it sunk, diesel (fuel) was leaking out into the water, into the cargo hold," said Tyms.

It took eight divers twenty-four hours and fifteen dives to bring up all the cocaine which had an estimated street value of $180 million.

First responders learn to rescue large animals

Source: http://madison.patch.com/articles/local-first-responders-learn-large-animal-rescue

Last weekend first responders from Green Village, New Jersey and nearby New Vernon and

Madison gained a unique set of skills – rescuing large animals.

With an estimated 300 horses in the area, local first responders have been called in to rescue a horse at least once in the last eighteen months. Without the proper training or expertise, rescuing these large animals can result in injury to both first responders as well as the animals.

For instance last August , Mare Olsen, a resident of Green Village, called 911 after her and her husband failed in rescuing their horse that had fallen into a ditch and could not get out.

Madison, New Vernon, and Green Village fire departments all responded to the call as well as police, and they were all uncertain of how to free the horse. First responders first had the idea to enlarge the ditch and used a backhoe to dig dirt out from under the horse, but it was still unable to get up.

Eventually according to Olsen, rescue workers used inflatable pillows. "They put one under her hips and one under her chest. Those got her prone, and then she got up by herself and climbed out of that ditch."

Chip Del Coro, the vice president of the Green Village Fire Department, said the department had never been trained to perform a rescue like that.

"Nobody knew how to get a horse up with a sling," Choro said.

Following the rescue, Olsen contacted Days End Farm Horse Rescue, an organization in Maryland that specializes in training first responders how to deal with a horse, and they agreed to hold a seminar in New Jersey.

As part of the training held last weekend , first responders learned how to make an impromptu harness from rope and to lift a horse using a fire truck ladder.

New radar technology provides real-time video of what's going on behind solid walls

Source: http://www.physorg.com/news/2011-10-radar-technology-real-time-video-solid.html

The front of the phased array radar system developed by researchers at MIT's Lincoln Laboratory, which sends and receives signals of movement behind solid concrete walls. Photo provided by the researchers

The ability to see through walls is no longer the stuff of science fiction, thanks to new radar technology developed at MIT's Lincoln Laboratory.

Much as humans and other animals see via waves of visible light that bounce off objects and

then strike our eyes' retinas, radar "sees" by sending out radio waves that bounce off targets and return to the radar's receivers. But just as light can't pass through solid objects in quantities large enough for the eye to detect, it's hard to build radar that can penetrate walls well enough to show what's happening behind. Now, Lincoln Lab researchers have built a system that can see through walls from some distance away, giving an instantaneous picture of the activity on the other side.

The researchers' device is an unassuming array of antenna arranged into two rows — eight receiving elements on top, 13 transmitting ones below — and some computing equipment, all mounted onto a movable cart. But it has powerful

implications for military operations, especially "urban combat situations," says Gregory Charvat, technical staff at Lincoln Lab and the leader of the project.

Waves through walls

Walls, by definition, are solid, and that's certainly true of the four- and eight-inch-thick concrete walls on which the researchers tested their system.

At first, their radar functions as any other: Transmitters emit waves of a certain frequency in the direction of the target. But in this case, each time the waves hit the wall, the concrete blocks more than 99 percent of them from passing through. And that's only half the battle: Once the waves bounce off any targets, they must pass back through the wall to reach the radar's receivers — and again, 99 percent don't make it. By the time it hits the receivers, the signal is reduced to about 0.0025 percent of its original strength.

But according to Charvat, signal loss from the wall is not even the main challenge. "[Signal] amplifiers are cheap," he says. What has been difficult for through-wall radar systems is achieving the speed, resolution and range necessary to be useful in real time. "If you're in a high-risk combat situation, you don't want one image every 20 minutes, and you don't want to have to stand right next to a potentially dangerous building," Charvat says.

The Lincoln Lab team's system may be used at a range of up to 60 feet away from the wall. (Demos were done at 20 feet, which Charvat says is realistic for an urban combat situation.)

And, it gives a real-time picture of movement behind the wall in the form of a video at the rate of 10.8 frames per second.

Filtering for frequencies

One consideration for through-wall radar, Charvat says, is what radio wavelength to use. Longer wavelengths are better able to pass through the wall and back, which makes for a stronger signal; however, they also require a correspondingly larger radar apparatus to resolve individual human targets. The researchers settled on S-band waves, which have about the same wavelength as wireless Internet — that is, fairly short. That means more signal loss — hence the need for amplifiers — but the actual radar device can be kept to about eight and a half feet long. "This, we believe, was a sweet spot because we think it would be mounted on a vehicle of some kind," Charvat says.

Even when the signal-strength problem is

show up as a 30-kilohertz sine wave," Charvat says. The filter can be set to allow only waves in the range of 30 kilohertz to pass through to the receivers, effectively deleting the wall from the image so that it doesn't overpower the receiver.

"It's a very capable system mainly because of its real-time imaging capability," says Robert Burkholder, a research professor in Ohio State University's Department of Electrical and Computer Engineering who was not involved with this work. "It also gives very good resolution, due to digital processing and advanced algorithms for image processing. It's a little bit large and bulky for someone to take out in the field," he says, but agrees that mounting it on a truck would be appropriate and useful.

Monitoring movement

Taken with the through-wall ultrawideband radar system

Two humans in free space — Behind 4-inch solid concrete wall — Behind cinder-block wall — Behind 8-inch solid concrete wall

In a recent demonstration, Charvat and his colleagues, Lincoln Lab assistant staff John Peabody and former Lincoln Lab technical staff Tyler Ralston, showed how the radar was able to image two humans moving behind solid concrete and cinder-block walls, as well as a human swinging a metal pole in free space. The project won best paper at a recent conference, the 2010 Tri-Services Radar Symposium.
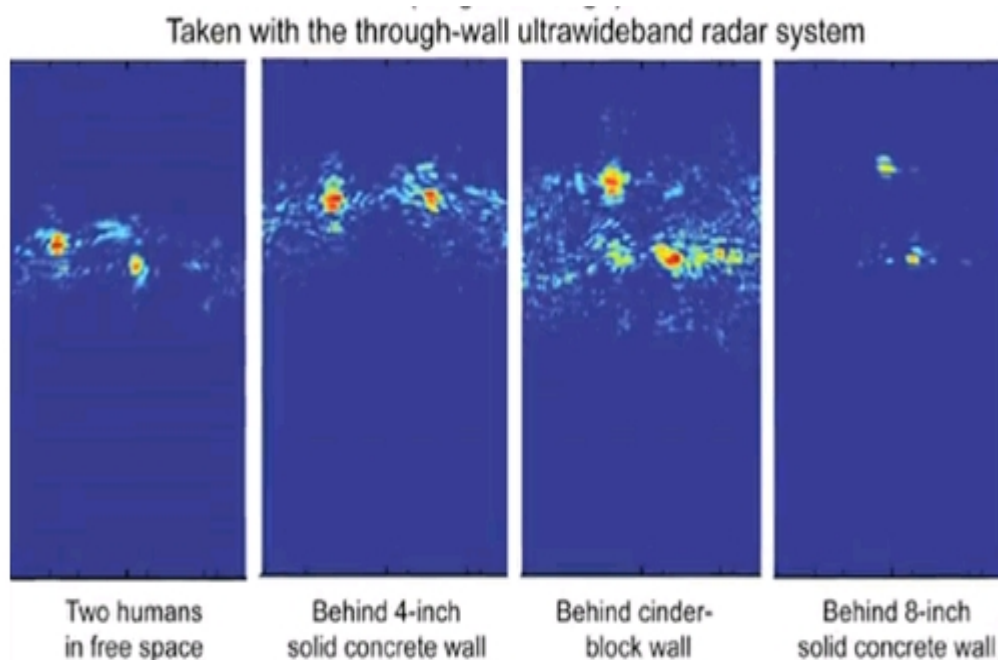
addressed with amplifiers, the wall — whether it's concrete, adobe or any other solid substance — will always show up as the brightest spot by far. To get around this problem, the researchers use an analog crystal filter, which exploits frequency differences between the modulated waves bouncing off the wall and those coming from the target. "So if the wall is 20 feet away, let's say, it shows up as a 20-kilohertz sine wave. If you, behind the wall, are 30 feet away, maybe you'll

Because the processor uses a subtraction method — comparing each new picture to the last, and seeing what's changed — the radar can only detect moving targets, not inanimate objects such as furniture. Still, even a human trying to stand still moves slightly, and the system can detect these small

movements to display that human's location.

The system digitizes the signals it receives into video. Currently, humans show up as "blobs" that move about the screen in a bird's-eye-view perspective, as if the viewer were standing on the wall and looking down at the scene behind. The researchers are currently working on algorithms that will automatically convert a blob into a clean symbol to make the system more end-user

friendly. "To understand the blobs requires a lot of extra training," Charvat says.

With further refinement, the radar could be used domestically by emergency-response teams and others, but the researchers say they developed the technology primarily with military applications in mind. Charvat says, "This is meant for the urban war fighter … those situations where it's very stressful and it'd be great to know what's behind that wall."

Terrorism in Africa: Kenyan troops invade Somalia

Source: http://www.homelandsecuritynewswire.com/bull20111021-terrorism-in-africa-kenyan-troops-invade-somalia

On Wednesday (Oct 19th), Kenya sent its troops some 100 miles inside Somalia to take the battle to the Islamic Al Shabaab organization, killing some 75 militants; yesterday, AU troops stormed a stronghold of Al Shabaab militant group on the outskirts of Mogadishu, while a militia backed by Kenyan troops simultaneously attacked another Shabaab stronghold along the Kenya-Somalia border, taking it over and forcing Shabab fighters to flee; Somalia's nominal government relies on Ethiopian and Kenyan troops to fight Islamic terrorists in Somalia

Four years ago the United States created a new military command – the Africa Command. For

nearly a decade now, Western military and intelligence services have been focusing on Africa as the source of a variety of problems threatening U.S. national interest and economic welfare.

Two main problems were of special concern:

- Terrorism: some African countries offer terrorists a hospitable environment because these countries are large and are poorly governed – if they are governed at all. Countries such as Somalia, Niger, Mauritania, and Chad, among others, are in this category. Other countries, like Nigeria, have a restive Muslim population in which terrorist groups find recruits.

- Climate change: the geography of Africa makes it vulnerable to climate change, as 70 percent of the continent's population relies on rain-fed agriculture for their livelihoods. The combination of desertification, longer and more intense droughts, and over-population has led intelligence and military services in the West to conclude that within a few short years, large groups of impoverished people will begin to move from their drying land to areas where water is more available, in the process plunging areas of the continent into bitter conflicts and war.

CBRNE Terrorism Newsletter – Winter 2011

At least when it comes to terrorism, more and more African governments have show willingness to take action. The latest example is the deployment of Kenyan troops inside Somalia.

On Wednesday, Kenya sent its troops some 100 miles inside Somalia to take the battle to the Islamic Al Shabaab organization, killing some 75 militants. The official reason given for the incursion was that it was meant to help find two kidnapped aid workers. In fact, the incursion was meant to inflict a heavy blow on the Islamic Al Shabaab and discourage it from conducting terrorist activities inside Kenya.

The incursion is similar to the one undertaken by Ethiopia five years ago. That incursion was similar to the none taken by Kenya in that both were motivated by growing Al Shabaab activity

The Ethiopians were promised that the AU would put together a force of 8,000 peace keepers to replace the Ethiopian troops in the city, but by 2009 the AU has been able to recruit on 3,400 troops for the peace keeping mission. Ethiopia had enough and pulled its forces to bases inside Ethiopia, from which they continue their policy of periodic raids against Islamists inside Somalia.

Kenya's military action is more modest than the ambitious Ethiopian invasion of 2006. The Kenyan army is well equipped and well trained, and there is little doubt that it can keep the border area quiet with periodic raids into Somali, the way the Ethiopians have managed to do in the past five years.

Moreover, the invasion was coordinated with Somalia's Transitional National Government

inside Ethiopia and Kenya, respectively.

Note that Ethiopia's action went further: at the urging of the United States and the African Union (AU), Ethiopian troops went beyond the border region and drove all the way to Somalia's capital Mogadishu, in order to drive the increasingly more powerful Islamic Court Union out of the city.

(TNG), the nominal ruling authority bin Somalia. Since the TNG controls no more than a few buildings in downtown Mogadishu, it relies on the Ethiopian and Kenyan militaries to engage the Islamists. The TNG has been reduced to providing intelligence information to

Ethiopia and Kenya about Al Shabaab concentrations in spots along Somalia's borders, then inviting those two countries to come in and engage the Islamists (officially, the TNG denies that it coordinates military action with its two

stronghold along the Kenya-Somalia border, taking it over and forcing Shabab fighters to flee. The Kenyan military has been coordinating its activities with clan-based militias in southern Somalia – especially with the Ras

© REUTERS/Thomas Mukoya

neighbors against Al Shabaab)
Yesterday, AU troops stormed a stronghold of Al

Kamboni Movement.
One interesting aspect of Kenya's military action is that, according to the New York Times, **the United States was not informed ahead of time of the incursion.** This is surprising, since "Kenya is one of the closest American allies in Africa," the Times reports, "frequently cooperating on military and intelligence issues, and American officials have branded Islamist militants in Somalia a serious threat to the United States."

Shabaab militant group on the outskirts of Mogadishu, while a militia backed by Kenyan troops simultaneously attacked another Shabaab

Grenade attack injures fourteen revelers in Nairobi night club

Source: http://www.coastweek.com/3442_security_07.htm

Fourteen people were wounded when a club in downtown Nairobi came under a grenade attack, local media reported early Monday. The blast happened shortly after 03.00 a.m. local time (0000 GMT – Oct 23rd) when a man entered the club and hurled a grenade into it before fleeing the scene, a witness told local media. The wounded have been sent to hospital, the reports said. According to local police, no one was killed. The wounded were receiving treatment, and most of their injuries were not serious, a doctor at Kenyatta National Hospital said. An investigation is under way. No one or group has claimed responsibility for the attack so far. The attack was suspected to be linked to Kenya's recent operations against Al-Shabaab militants in Somalia. Kenyan troops made further advances into Somali Al-Shabaab controlled territory on Saturday, with the support of heavy aerial bombardment. Somali militants have vowed to retaliate.

Indian Navy chief warns against piracy-terrorism nexus

Source:http://www.hindustantimes.com/News-Feed/newdelhi/Navy-chief-warns-against-piracy-terrorism-nexus/ Article1-760024.aspx

Navy chief Admiral Nirmal Verma has made a "relatively benign" problem of piracy forging links
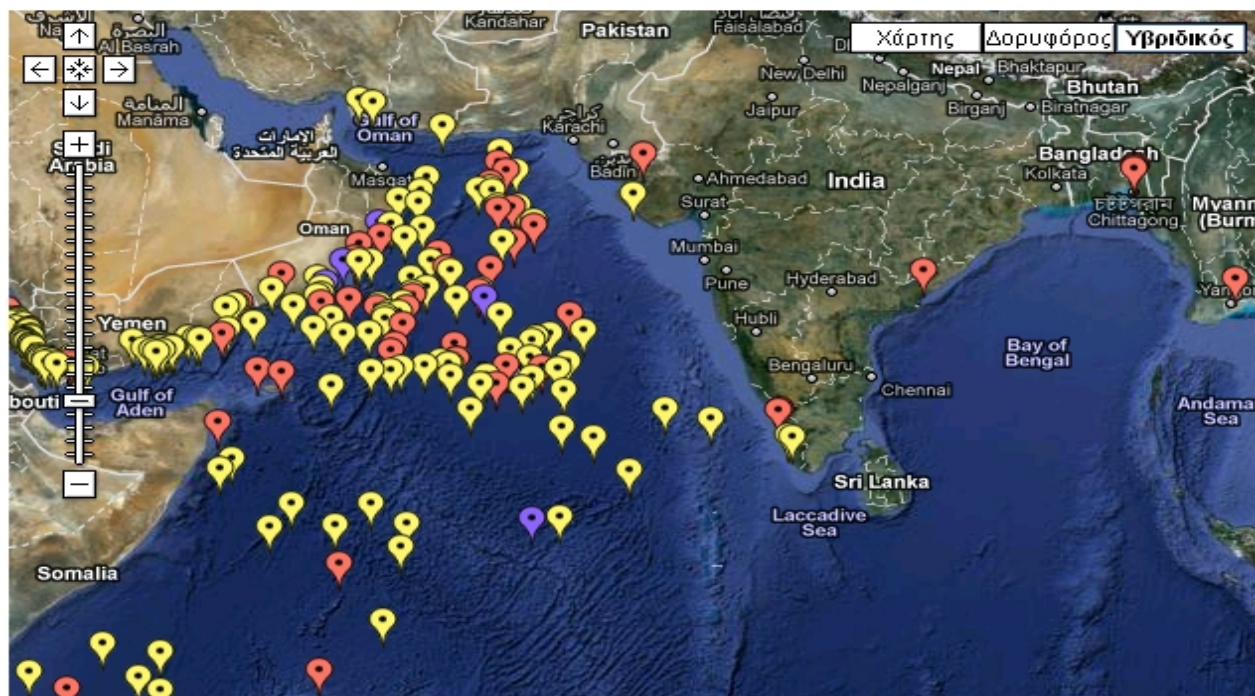
pitch for putting in place pre-emptive measures to scuttle pirates from developing a nexus with terror groups. Speaking at an international symposium at New Port, Rhode Island, Verma on Thursday cautioned against the possibility of the with terrorism, which has a "cancerous potential." The symposium themed, "Security and Prosperity through Maritime Partnerships," is being organized by the US Naval War College.

Verma highlighted the dilemma being faced by naval forces due to ineffective legal mechanisms to prosecute pirates apprehended by them. He said, "It is estimated that nine out of 10 apprehended pirates benefit from the 'catch and release' policy followed by most navies till now."

India is yet to prosecute more than 100 pirates apprehended by the navy. The country is working on a legislation to declare piracy as an offence under Indian law. In the absence of such a law, pirates apprehended by the navy and coast guard are currently prosecuted for offences such as attempt to murder, criminal trespass and damage to property.

Verma said piracy was no longer mere robbery but had morphed into an elaborate network of operations to extract enormous quantities of ransom. "Ransom amounts have increased to an average of $5.4 million per ship from just $150,000 five years ago," he said.

Verma said international efforts off the Gulf of Aden had resulted in pirates expanding their footprint in the Arabian Sea and prowling closer to Indian shores. He said, "Some of these areas have been not too far from India's Lakshadweep and Mincoy group of islands and this has been a cause of concern to us."

Saudi woman sentenced to 15 years for Qaida links

Source: http://www.wlox.com/story/15905242/saudi-woman-sentenced-to-15-years-for-qaida-links

Saudi Arabia says that a special tribunal has sentenced a Saudi woman to 15 years in prison on terrorism-linked charges including aiding al-Qaida cells and insurgents seeking to enter Iraq.

The official Saudi Press Agency says the woman sought to "commit terrorist attacks" in the kingdom, financed anti-state groups with more than 1 million riyals ($266,000 / 300,000€) and provided communications equipment. The woman also was convicted of helping issue forged IDs to people seeking to join the insurgency in Iraq.

The report did not identify the women sentenced Saturday or give other details. She also is banned from traveling for 15 years after completing her sentence.

Saudi authorities have cracked down periodically in recent years on groups inspired by al-Qaida.

NOTE: This is the first a woman goes on trial with terrorism charges in S. Arabia.

Terrorist incidents around the globe

Source: https://www.cimicweb.org/CounterIED/DaT-CoE%20Monthly%20report%20-%20September_2011.pdf

NATO's Defence against Terrorism Centre of Excellence (DaT-CoE) reported a total of 920 terrorist incidents across the globe during September, resulting in 1,449 people killed and 2,290 injured. IEDs, vehicle-borne IEDs, or suicide bombers were used in 319 (34.7%) of these attacks. IED-related attacks accounted for 493 deaths (34%) and 1,601 wounded (69.9%) from all terrorist incidents.

Attack type	Number of Instances	# Killed	# Injured
IED	251	282	743
VBIED	35	68	350
Suicide attack	33	143	508
All other attack types	601	956	689
Total terrorist attacks	920	1,449	2,290

NOTE: You can download the September report from the website hosting the Newsletter (CBRNE-CT Papers).

Counter-Terrorism Crisis Communication

Source: http://faculty.biu.ac.il/~sshpiro/index.html

The goal of the project is to help public authorities in Europe better reacting to terror crises by providing effective communication strategies for the aftermath of terror attacks. Such attacks take place when least expected, as terrorists search for vulnerable targets across Europe and seek to spread fear and panic. A terror attack instantly becomes breaking news in the media throughout the world. Effective recovery from such an attack depends also on a carefully planned and trained communication strategy which would restore public confidence and enable quick return to normality.
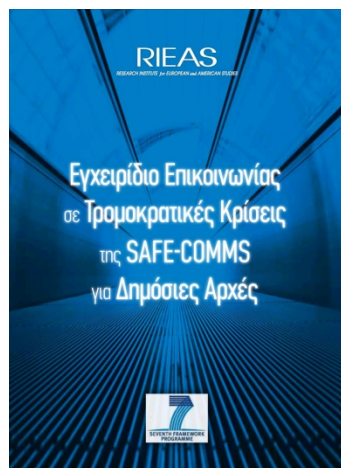
In order to effectively deal with the aftermath of terror attacks, public authorities need a counter-terrorism communication strategy comprised of activities aimed at the relevant audiences. This strategy needs to be trained and adapted before an attack takes place and forms an inherent part of crisis management and continuity plans. SAFE-COMMS aims to provide public authorities throughout Europe with an effective and modular communication strategy for terror crises.
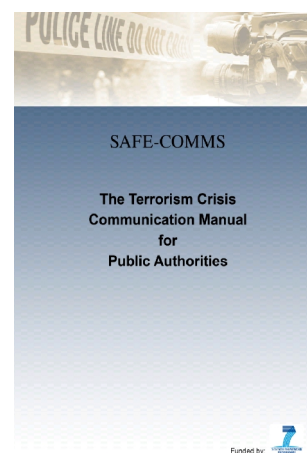
NOTE: Greek and English version of the manual can be downloaded from the website hosting the Newsletter (CBRN Response Tools section)

Alleged Plot to Attack U.S. Officials Was Inspired by Online Anti-Government Novel

Source: http://www.foxnews.com/us/2011/11/01/4-suspected-us-militia-members-charged-in-plot/

An alleged plot to attack federal and state officials by suspected members of a fringe north Georgia militia group was inspired by an online anti-government novel, authorities said.

Court documents state that 73-year-old Frederick Thomas, a suspected member of the group, told others that he intended to model their actions on the online novel "Absolved," which involves small groups of citizens attacking U.S. officials.

The four suspected members, who federal authorities arrested Tuesday, were expected to appear in court Wednesday.

They were part of a group that also tried to obtain an unregistered explosive device and sought out the complex formula to produce Ricin, a biological toxin that can be lethal in small doses, according to a federal complaint.

Authorities said the group intended to use the plot of the novel "Absolved," written by Mike Vanderboegh, a blogger who has closely followed the botched federal investigation known as "Fast and Furious." He also runs a whistleblower website called Sipsey Street Irregulars.

During a phone interview with FoxNews.com on Wednesday, Vanderboegh claimed he was not responsible for the alleged plot. "What kind of moron uses the phrase 'save the Constitution and then goes out to try and distribute Ricin?" Vanderboegh said. "This has got to be the Alzheimer's gang. What political point is made there? I don't understand what was going on in the minds of these Georgia idiots."

The four listed in the indictment are Thomas; Dan Roberts, 67; Ray Adams, 65; and Samuel Crump, 68. The men live in the north Georgia towns of Cleveland and Toccoa.

They had been talking about "covert" operations since at least March, according to court records, discussing murder, theft and using toxic agents and assassinations to undermine the state and federal government.

In one of the indictments obtained by FoxNews.com, authorities said Thomas is recorded saying, "Let's shoot the bastards that we discover are anti-American. And to me the best way to do that is to walk up behind them with a suppressed .22."

"I am of the, uh, old school, Mafia; one behind the ear with a .22 is all you need," Thomas allegedly said. "Of course a .40 Smith and Wesson or .45 ACP is just as good, even better, cause it makes the whole head explode."

Investigators also say Thomas openly discussed creating a "bucket list" of government employees, politicians, corporate leaders and members of the media he felt needed to be "taken out."

"I've been to war, and I've taken life before, and I can do it again," he told an undercover investigator, according to the records.

Thomas' wife, Charlotte, called the charges "baloney."

"He spent 30 years in the U.S. Navy. He would not do anything against his country," she said in a phone interview with The Associated Press.

Thomas and Roberts are accused of buying what they believed was a silencer and an unregistered explosive from an undercover informant in May and June. Prosecutors say he discussed using the weapons in attacks against federal buildings.

Prosecutors say Crump also discussed making 10 pounds of Ricin and dispersing it in Atlanta and various cities across the
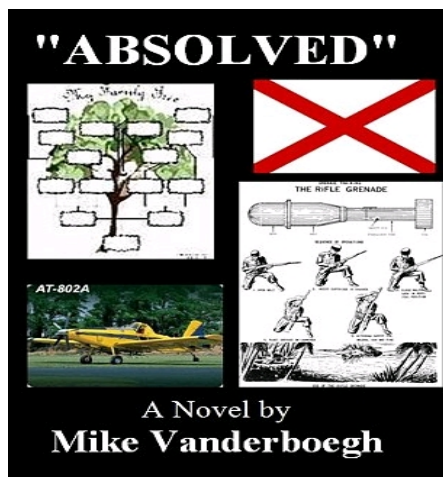
nation, suggesting it can be blown out of a car speeding down an interstate highway.

Adams, meanwhile, is accused of showing an informant the formula to make Ricin and identifying the ways to obtain the ingredients.

Thomas is accused of driving to Atlanta with a confidential informant on May 24 and scoping out an IRS building there and an ATF building "to plan and assess for possible attacks," the indictment states.

"We'd have to blow the whole building, like Timothy McVeigh," Thomas said during the trip to Atlanta, the indictment states.

Charlotte Thomas said her husband was arrested in a restaurant in Cornelia, Ga., and federal agents were at her home when she returned from the grocery store Tuesday afternoon. She said the agents wouldn't let her in her home.

"They tore up my house," Charlotte Thomas said. She said her husband doesn't have an attorney yet.

Margaret Roberts of Toccoa said FBI agents showed up with a search warrant and went through her home, handcuffing her and taking a computer and other items. She said her husband is retired from the sign business and lives on pensions.

"He's never been in trouble with the law. He's not anti-government. He would never hurt anybody," she said.

Listed numbers for the other two suspects could not be found.

Attorneys for the men were not identified, and the federal defender's office had no immediate comment.

U.S. Attorney Sally Quillian Yates said the case is a reminder that "we must also remain vigilant in protecting our country from citizens within our own borders who threaten our safety and security."

Book Review: Youth Violence

By Nancy Hartevelt Kobrin

Source:http://www.citizentimes.eu/2011/11/03/understanding-youth-who-become-radicalized-to-violent-extremism /#.TrOLAnLw1v0

Dr. Seifert's newest book Youth Violence: Theory, Prevention and Intervention, builds on more than thirty years of clinical experience working with the most violent and high risk youth imaginable. Two colleagues also contribute to this work – Dr. Karen Ray and Robert Schmidt. I was drawn to Dr. Seifert's first book How Children Become Violent: Keeping Your Kids Out of Gangs, Terrorist Organizations and Cults because she addresses the question "How" rather than the "Why". "How" stresses a dynamic process, where there are a series of factors which come into play such as genetics, biochemistry, nurturing environment, early trauma and so on. How Children Become

Violent did not disappoint for it specifically focused on disrupted attachment patterns in children and how such patterns can become detrimentally engrained in the character of a child early on lingering for the rest of his or her life as they mature. The author has also created and put into place an excellent evaluation methodology in CARE-2 (Child and Adolescent Risk/Needs Evaluation).

Kathryn Seifert (2011): Youth Violence. Theory, Prevention and Intervention. Springer. 256 p. 34.99 Euro.

Once again, Seifert deftly develops the contours of violence but this time in a more holistic, comprehensive way offering prevention and treatment modalities for adolescents in Youth Violence. The topic is perhaps one of the most pressing issues of our time when we stop to think about Columbine, Virginia Tech or even adolescent suicide bombers. Finally, someone has linked violence perpetrated by youth as a major red flag and concern for counter terrorist experts to pay more attention. Seifert understands the mind of the gang or group mentality and how youths are especially prone to and inclined to identify with paternal like charismatic leaders who offer some hope or give meaning to their lives in these cult like groups. Yet she stresses the early roots to this gang social bonding by raising the issue of maternal attachment and that of caregivers.

Even the allegedly self-radicalized terrorist is particularly susceptible to coming under the influence of violent ideologies to fend of personal impotence and vulnerability. While this aspect of radicalization is known, the devil is in the details and the willingness to explore the psychology of youth violence in a nuanced manner has not been well developed in terrorism studies. It is exciting to come across a practitioner of psychology who has taken the time to map out the tough terrain of adolescence and the potential for violence. It should be of great concern to all and especially to policy makers. Youths are at considerable risk to lose control over their mounting aggression if appropriate boundaries have not been set by authority figures. Otherwise like heat seeking missiles these youths who are full of rage gravitate to a leader who taps into this preexisting reservoir of rage to harness it and thereby enacts their aggression and rage. The leader does not have to even be "present", the very image or fantasy of what he represents is enough to empower these allegedly self radicalizing youth.

The book is divided into sections with an overview of the problem *vis a vis* prevention, trends, demographics, classification issues and theories. It then shifts into a discussion of dynamics of youth – both individual and environmental, followed by a section on special issues – bullying and suicide – with a final section on assessment, prevention and intervention.

It also serves as a most useful handbook or guide in conceptualizing youth violence from a multifaceted perspective. Dr. Seifert has done an admirable job integrating a wide range of theories, citing the pluses and minuses as well as pinpointing areas that need to be explored further through research. The section on special issues – bullying and suicide, are particularly applicable to the study of terrorism. Throughout the world there is growing concern about "self-radicalization." Seifert's work points to the need to delve deeper into the neuroscience, biology, educational and well as environmental stressors which prime the pump for youth to be swept up in murderous violence which is often categorized in a limited manner as political violence, thereby inadvertently permitting counter terrorist experts to dismiss
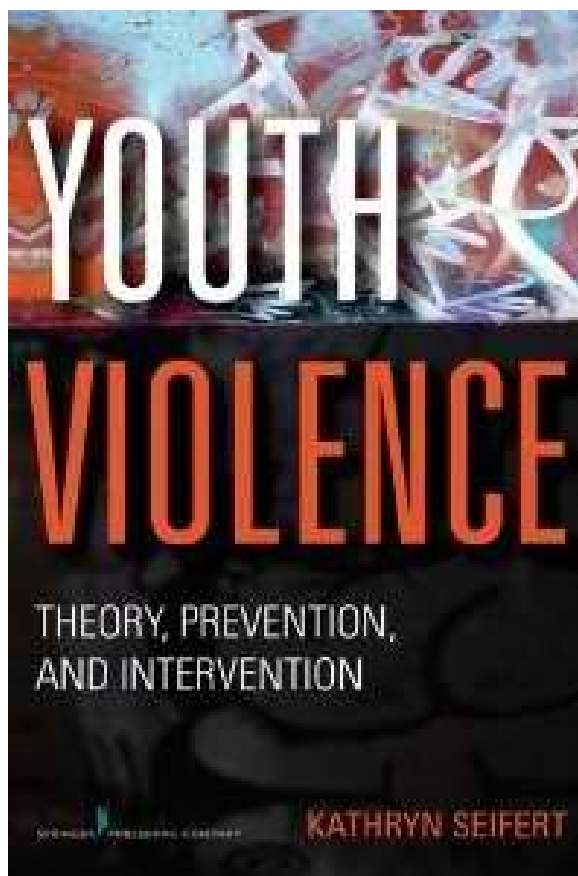
the nascent formation of the personality or what is referred to as characterological psychopathology, the armor of the personality so to speak which is used to protect the fragile traumatized self from what is perceived to be an inherently hostile world. Many psychiatrists and a wide range of mental health professionals' belief that serious violent psychiatric disorders are in place by age two. That is why this more covert period tends to be overlooked in counter terrorism work because it is multifaceted, complex, let alone the influence of the female caregiver.

Thus, while the book does not deal directly with Islamic suicide terrorism, it certainly has applicability by casting light on the escalation of youths involved in political violence linking it back to early childhood. The author notes in passing that Yassir Arafat is a good example of this. Besides being an abandoned orphan he was raised by terrorists and was forced to become a child soldier who in turn recruited other children into terrorism, tragically perpetuating the cycle of violence and its intergenerational transmission of trauma. In a way one can understand how Palestinian culture has developed a fixation and obsession with children shahids as Arafat became their venerated father. Seifert also cites the important and interesting recent research of Ez-Elarab Sabbour, Gadallah and Assad from Cairo (2007) in which they studied aggressive elementary school children. To quote Seifert:

"They found the following risk factors: absence of attachment figure, single parent, use of corporal punishment by caregivers, preference for violent video games, exposure to verbal aggression, aggressive peers, and victimization."

It is most impressive how she is of the few who stresses maternal attachment coupled with the paternal which sets a template for social attachment and bonding experiences later in life. Seifert reminds us of the crucial role that neuroscience plays in this attachment, interpersonal relationship bonding to people.

"There is a neurological component to secure attachment. A caregiver who smiles and coos at a baby, for example, supports the development of mirror neurons in the infant's brain, which are necessary for building the initial relationship…"

Mirror neurons are essential to the development of empathy. Children who do not feel safe in their early childhood will have difficult in their youth. Trauma plays a key role. This is not to say that everyone who experiences a parental deficit in the early attachment experience will become violent or a terrorist, yet there is much to learn about the linkage of these experiences for those who grow up and tragically inscribe their projected rage, envy and attacking written in blood, destruction, murder, etc. In my analysis this is the time frame which holds the key to early signals decoding violent mental states of terrorists.

Given how devastating and tiring such perpetrated violence becomes, this book is most inspiring. It left me with a feeling of wanting to create a subfield concerning early childhood development within terrorism studies. And if I had my druthers, I would invite Dr. Seifert to participate in such a project. With her newest endeavor, Youth Violence, she has succeeded to write an invaluable book which can be extrapolated specifically to understanding youth who become radicalized to violent extremism. While this was not her specific aim I am grateful to Dr. Seifert who unwittingly offered her insights in understanding the bare roots of such violence – it is a very precious gift.

Jihadi Terrorism and the Radicalisation Challenge - European and American Experiences
By Rik Coolsaet

- Published: October 2011
- Extent: 340 pages

Osama bin Laden's demise in May 2011 marked only the symbolic end of an era. By the time of his killing, he no longer represented the Robin Hood icon that once stirred global fascination. Ten years after the 11 September 2001 attacks, jihadi terrorism has largely lost its juggernaut luster. It now mostly resembles a patchwork of self-radicalising local groups with international contacts but without any central organisational design - akin to the radical left terrorism of the 1970s and the anarchist fin-de-siècle terrorism.

This volume addresses two issues that remain largely unexplored in contemporary terrorism studies. It rehabilitates the historical and comparative analysis as a way to grasp the
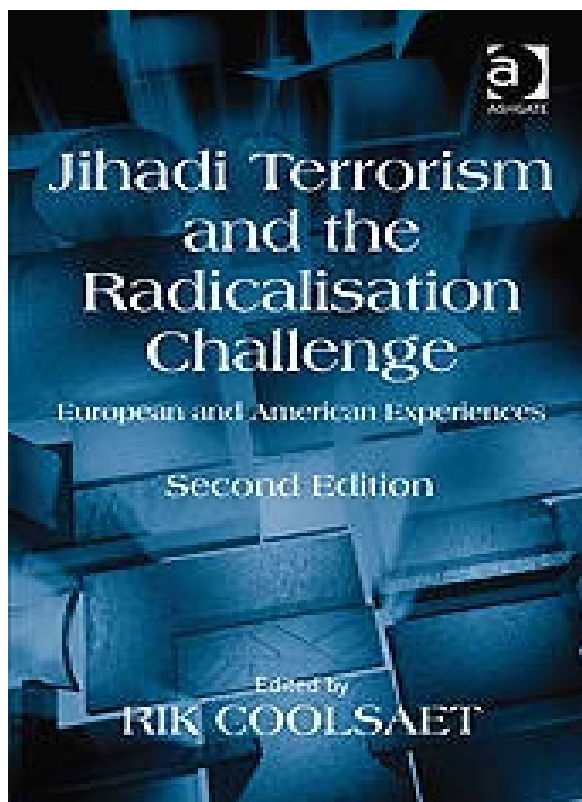
essence of terrorism, including its jihadi strand. Crucial similarities with earlier forms of radicalisation and terrorism abound and differences appear generally not fundamental.

Likewise, the very concept of radicalisation is seldom questioned anymore. Nevertheless it

often lacks conceptual clarity and empirical validation. Once considered a quintessential European phenomenon, the United States too experiences how some of its own citizens radicalise into terrorist violence. This collective work compares radicalisation in both continents and the strategies aimed at de-radicalisation. But it also assesses if the concept merits its reputation as the holy grail of terrorism studies.

The volume is aimed at an audience of decision makers, law enforcement officials, academia and think tanks, by its combination of novel thinking, practical experience and a theoretical approach.

Contents
Introduction, Rik Coolsaet; Part I The State of the Threat: Jihadi terrorism: a global assessment of the threat, Paul R. Pillar; Al-Qaeda: a true global movement, Olivier Roy; Logics of jihadi violence in North Africa, Hugh Roberts; 'Terrorism studies': a critical appraisal, Teun van de Voorde. Part II Cycles of Terrorism and Radicalisation: The debate over 'old' vs. 'new' terrorism, Martha Crenshaw; Radicalisation and terrorism in history: lessons from the radical left terrorist campaigns in Europe and the United States, Leena Malkki; Cycles of revolutionary terrorism, Rik Coolsaet. Part III Radicalisation in Europe and the US: Muslims in Europe and the US: a shared but overrated risk of radicalism, Jocelyne Cesari; The turn to political violence in the West, Marc Sageman; Characteristics of jihadi terrorists in Europe (2001–2009), Edwin Bakker; Dutch extremist Islamism: Van Gogh's murderer and his ideas, Rudolph Peters; The rise and demise of jihadi terrorism in Belgium, Rik Coolsaet. Part IV De-Radicalisation Experiences: Disengagement, de-radicalisation and the arc of terrorism: future directions for research, John Horgan and Max Taylor; Group desistence from terrorism: the dynamics of actors, actions and outcomes, Clark McCauley; (De-)escalating

radicalisation: the debate within immigrant communities in Europe, Tarik Fraihi; Competing counter-radicalisation models in the UK, Robert Lambert; Counterterrorism and counter-radicalisation in Europe: how much unity in diversity?, Rik Coolsaet; Counter-radicalization in the United States, Lorenzo Vidino. Epilogue: terrorism and radicalisation: what do we now know?, Rik Coolsaet; Appendix; Bibliography; Index.

About the Editor: Rik Coolsaet is Chair at the Department of Political Science, Ghent University, Ghent University, Belgium

Reviews

"Through its systematic engagement with a variety of ideas and cases, this collection of important work provides a central point of focus for scholars and practitioners seeking to engage with the questions and debates surrounding radicalisation and jihadi violence. Jihadi Terrorism and the Radicalisation Challenge represents the capstone to the current phase of research on this subject, and essential reading for all in this field."

Jonathan Githens-Mazer, Institute of Arab and Islamic Studies, University of Exeter, UK

'In the literature on Jihadism, Rik Coolsaet's contribution as the editor of the book Jihadi Terrorism and the Radicalization Challenge: European and American Experiences stands apart. Many outstanding scholars took part in its writing and they brought in new ideas not only on Jihadism and radicalization but also on the de-radicalization process and its intricacies. By reading this single book, one can surmise having read tens, the rich contribution of the scholars making almost each chapter unique. At the end, one comes out with a much deeper understanding of Jihadism. "

Farhad Khosrokhavar, École des hautes études en sciences sociales, France
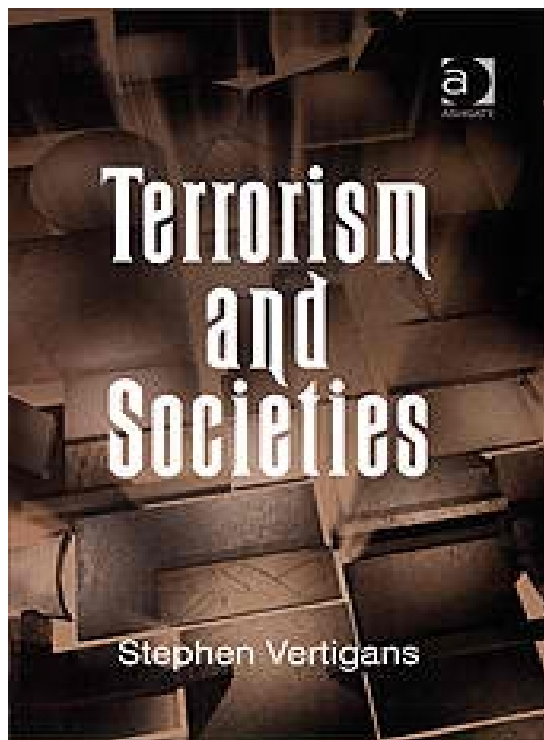
Terrorism and Societies
By Stephen Vertigans

- Published: April 2008
- Extent: 206 pages
- Price : £55.00

Which socializing agents are influential in people joining terror groups? What ideologies do terror groups hold? Which aspects of societies and social contexts contribute towards groups forming and people joining them?

This book considers a range of influential terror groups from the last 40 years, exploring relationships between people, local and global social processes, and activities that result in acts of terrorism. Examining Islamic groups alongside nationalist, 'red' and far right organizations, Stephen Vertigans identifies

important similarities in the social contexts, experiences of members and some of their demands.

Key questions are applied to a range of case studies of contemporary relevance. The groups studied originated from Europe, the United States, Asia and Africa and are associated with religion, nationalism, pro-state terrorism, militias and racism. Each chapter offers the reader a clear understanding about why particular terror groups form, while comparative analysis draws out commonalities and distinctions.

Contents

Reviews

"Stephen Vertigans has created a remarkable book about terrorism. From gun and talk shows to music, he extends the poignant case studies of Hamm and Stern in a sober, yet provocative manner. And, his theoretical insights on the societal breeding grounds of discontent help us explicate the ground-breaking research of internationally, acclaimed scholars such as Oliverio and Tilly. This book is especially useful for understanding conflict defined as terrorism from local to global settings.'"

Pat Lauderdale, Arizona State University, USA

"Written with clarity, and a superb balance of breadth that embraces several terrorist groups from across the globe and depth in the examination of each of them, this book addresses objectively the scourge of our age – terrorism. Stereotypes and popular misconceptions tumble under the weight of clear and well-informed analysis. This is essential reading for anyone who seeks insight into this fascinating and frightening phenomenon.'"

P.A.J. Waddington, University of Wolverhampton, UK

Terrorism yesterday and today: an introduction; National 'Islamic' terrorism: groups in the Palestinian territories; International 'Islamic' terrorism: al-Qa'ida and related groups; Republican and Loyalist terrorism in Northern Ireland; 'Red' urban terrorism: experiences in Italy, Germany and Japan; From Left to Right: terrorism within America from the 1960s to today; Conclusion: terrorism yesterday, today and tomorrow; Glossary; Bibliography; Index.

About the Author: Dr Stephen Vertigans is Reader in Sociology at the School of Applied Social Studies, Robert Gordon University, Aberdeen, UK

Top FARC rebel leader Alfonso Cano killed in Colombia

Source: http://www.bbc.co.uk/news/world-15604456

The leader of Colombia's left wing FARC rebel group, Alfonso Cano, has been killed in a military raid, President Juan Manuel Santos has confirmed.

He called it the most devastating blow to the group in its decades-long insurgency and urged it to disband.

Defence Minister Juan Carlos Pinzon said Cano was killed in an operation in mountains in Colombia's south-west.

Security forces have killed a number of Farc commanders and arrested many others in recent years.

Giving details of the operation, Mr Pinzon said

government forces first bombed a FARC jungle camp in Cauca state.

Alfonso Cano had a $4m prize tag on his head

Troops were then lowered from helicopters to search the area and killed Cano and several other Farc (Revolutionary Armed Forces of Colombia) members in a gun battle.
'Prison or a tomb'
Pictures of the dead leader, with his trademark bushy beard shaved off, were broadcast on Colombian television.
"It is the most devastating blow that this group has suffered in its history," President Santos said in a televised address. "I want to send a

Cano, 63, was reportedly tracked down to the jungle camp with the aid of telephone intercepts. Colombia had offered a reward of nearly $4m (£2.5m) for information leading to his capture.
Analysts say Cano's death deals a further blow to the rebel group's ability to co-ordinate attacks on security forces and other targets.
The Marxist-inspired FARC has already been weakened by a military offensive which began 10 years ago. Mr Cano, a former academic from Bogota, became the Farc's leader in 2008 after his predecessor, Manuel Marulanda died of a heart attack. His real name was Guillermo Leon Saenz.
In July, he narrowly escaped a raid on his camp, Colombian officials said. In September 2010, Mono Jojoy, another top Farc commander, was killed in a bombing raid. The Colombian army also said earlier this year that it had killed Mr Cano's head of security, Alirio Rojas Bocanegra.The military has been able to expand its operations against the rebels with the help of the US, which has provided billions of dollars in funding, training and intelligence-sharing.
However, the FARC - the oldest and largest among Colombia's left-wing rebel groups - retains the ability to mount hit-and-run attacks, partly owing to cash raised through its involvement in the illegal drugs trade and partly thanks to the country's thick jungles.
The FARC is on US and European lists of terrorist organisations.
Colombia's civil conflict has lasted more than four decades, drawing in

message to each and every member of that organization: demobilise... or otherwise you will end up in a prison or in a tomb. We will achieve peace."

left-wing rebels and right-wing paramilitaries.

Proliferation of drones raises alarms
Source: http://www.homelandsecuritynewswire.com/proliferation-drones-raises-alarms

Security analysts fear that with the increasing proliferation of unmanned aerial drone technology, terrorists could eventually begin using them to drop explosives or even biological weapons.

Technological developments have led to ever smaller, remote-controlled drones that are easily transported, increasing the potential for extremists to get their hands on one. Furthermore, drones have developed at such a rapid pace, analysts are uncertain of their future.

"I think of where the airplane was at the start of World War I: at first it was unarmed and limited to a handful

Yilong (Pterodactyl)

This medium-sized, propeller-driven drone is China's answer to the U.S. Predator and MQ-9 Reaper drones – with a similar V-tail configuration. Its manufacturer, Aviation Industry Corp., says the Yilong has undergone test flights and is now the only drone being freely sold on the international market that can be used for both reconnaissance and strikes.

Length: **29.5 feet**
Range: **2,485.5 miles**
Maximum speed: **174 mph**
Maximum altitude: **16,404 feet**

翼龙

Xianglong (Soaring Dragon)

Produced by Aviation Industry Corp., this is the Chinese version of the U.S. RQ-4 Global Hawk — an advanced, high-altitude, long-duration drone designed for reconnaissance. The main difference is that the Xianglong has only a fraction of the Global Hawk's range; its manufacturer says it is intended for operations limited to the Asia/Pacific region.

翔龙
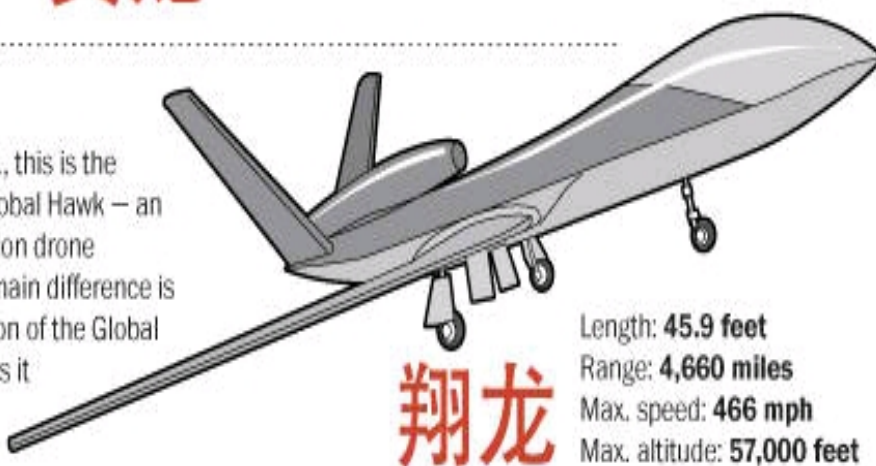
Length: **45.9 feet**
Range: **4,660 miles**
Max. speed: **466 mph**
Max. altitude: **57,000 feet**

暗剑
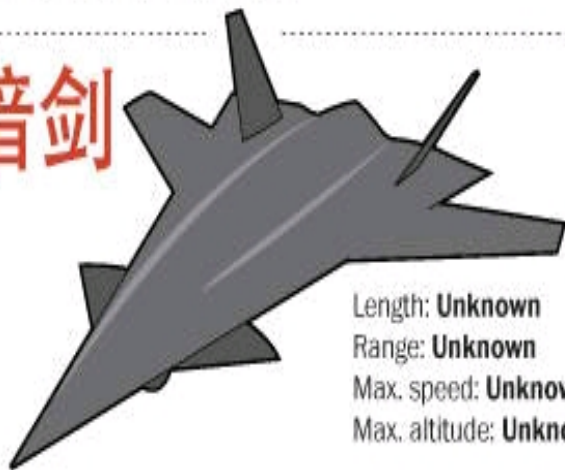
Length: **Unknown**
Range: **Unknown**
Max. speed: **Unknown**
Max. altitude: **Unknown**

Anjian (Dark Sword)

This conceptual model generated huge buzz when unveiled by Shenyang Aircraft Co. in 2006 because it represents the aspirations of the Chinese to design something even Western powers don't have yet — a supersonic drone capable of air-to-air combat as well as ground strikes. No one knows whether it can really be achieved and how far along in development the model is.

of countries," said P. W. Singer, a senior fellow at the Brookings Institute and the author of Wired for War. "Then it was armed and everywhere. That is the path we're on."

Analysts are particularly concerned as roughly fifty nations have purchased or are developing drones including India, Iran, Mexico, Pakistan, and Russia.

More troubling, China is now selling twenty-five different types of drones. During the drones' debut at an air-show last November, promotional video footage showed the Chinese drones attacking an American aircraft carrier and an armored vehicle.
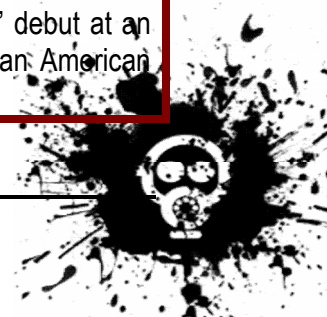
Clan and Conflict in Somalia: Al-Shabaab and the Myth of "Transcending Clan Politics"

By Ahren Schaefer and *Andrew Black*
Source: http://www.jamestown.org

Clan identity and Islam are central pillars of Somali society, with clan dynamics and inter-clan rivalries magnified by decades of state collapse. Al-Shabaab - the dominant Islamist militia controlling much of southern and central Somalia - claims to "transcend clan politics," yet reality on the ground belies this claim, revealing that al-Shabaab seeks to manipulate local clan alliances and remains deeply influenced by clan politics. This analysis shows that despite al-Shabaab's hard-line Islamist identity and pro-al-Qaeda rhetoric, many aspects of the group's past and current behavior remain deeply rooted in Somalia's local dynamics. Moreover, clan rules apply even to Somalia's most feared Islamists.

Somalia - All Politics are Local

Clan and sub-clan structures are central to Somali identity. From a young age, children are traditionally taught to memorize and recite their clan-based kinship genealogy, sometimes naming twenty or even thirty generations of their patrilineal ancestors. [1] When the Siad Barre regime collapsed in 1991 and with it the presence of centralized Mogadishu-based governance, inter-clan violence and power rivalries spiked as clan structures and identities filled the governance void. The destructiveness of this process contributed to a paradoxical perception of clans that remains palpable today. Though many Somalis often self-identify based on clan, they nevertheless blame "clannish" behavior for the fractionalization, violence, and the destruction of Somali stability. [2]

Nevertheless, Somali society continues to be defined by clan identities, and clan rivalries frame the balance of power across Somalia. Somali clans and sub-clans are geographically interwoven rather than clearly divided between homogeneous clan territories, although certain sub-clans exert significant power in specific regions. For example, the capital of Mogadishu is divided among Hawiye sub-clans while the Rahanweyn (also called the Digil-Mirifle) continue to play the key role in central Bay and Bakool regions. The Isaaq dominate Somaliland in the northwest, and various Darod sub-clans reside mainly in Puntland, the north-central provinces, and the southern Juba region. [3] These geographic divisions often correspond to battle lines, as clans vie for influence and resources.

This complex and interlocking system establishes the rules by which Somali politicians, warlords, and even terrorists must abide. As al-Shabaab has developed in recent years and sought to balance domestic priorities with international jihadi ideals, the role of clan has continued to plague and shape the organization.

Al-Shabaab - Avoiding the Stigma of "Clannish Behavior"

Al-Shabaab rose to prominence in 2006 as a militia subordinate to the Islamic Courts Union (ICU) and was typically criticized as being a Hawiye militia. [4] The Habr Gedir/Ayr sub-clan factions of the powerful Hawiye clan were noted as being particularly influential within the Islamic Courts at the time. Under the leadership of Aden Hashi Ayro, al-Shabaab became known for its Takfiri-Salafi worldview and links with al-Qaeda. [5]

With the dissolution of the ICU following the invasion of Somalia by the locally-reviled Ethiopian military, al-Shabaab arose as the most competent and capable resistance force against the Ethiopian occupation, even drawing on members of Somalia's minority clans ("looma ooyan") and building a multi-clan leadership structure (*Suna Times*, November 10, 2010). [6] Dr. Andre Le Sage notes that Ahmad Abdi Godane, Fu'ad Shongole, and Ibrahim Haji Jama, along with al-Shabaab's foreign fighter cadre, are the more radical leaders favoring the ideology of al-Qaeda's global jihad. In contrast, other Shabaab leaders and many of the groups rank-and-file have little loyalty to this trans-national cause. [7]

Al-Shabaab's protracted campaign against the deeply resented Ethiopians allowed the group's more jihad-oriented leadership to equate their radical agenda with nationalist sentiment and gain more cross-clan support than would have been possible absent a "common enemy." [8] In an effort to galvanize cross-clan support, al-Shabaab highlighted its Islamist and nationalist credentials, and in the face of the Ethiopian occupation, al-Shabaab succeeded in

establishing hegemony in south-central Somalia. In a pattern that has recurred throughout Somali history, the presence of an outside invader was able - albeit only temporarily - to rally otherwise disparate Somali factions. [9]

Since the Ethiopian withdrawal from Somalia, al-Shabaab has maintained that it "transcends clan," based on Islamist beliefs and the goal of Shari'a law. Al-Shabaab's determination to distance itself from clannish behavior stems from a) the belief that strength comes through unity; b) the belief by some of the group's more hard-line leadership in the universalism of al-Qaeda's Salafi-Jihad worldview; and c) the aforementioned sentiment that the fractionalization of Somali society is largely the result of clan-based power struggles. Therefore, this

However utilitarian this narrative may seem, al-Shabaab's clannish behaviors in Somalia belie the universality of this narrative, and show the organization to be fighting clan-based struggles internally and with other key players in Somalia.

The Rise of al-Shabaab—Still Fighting Clan Battles
Al-Shabaab's strategy and its inability to avoid clan influence has affected the way the group projects force, recruits fighters, and influences the Somali population. In these ways, al-Shabaab has evolved drastically over the past five years. Initially a relatively small militia, al-Shabaab gained local support as the only effective fighting force against the Ethiopian intervention in Somalia from late 2006 through early

transcendent narrative provides al-Shabaab with the flexibility to negotiate and mobilize support across clan lines, while simultaneously providing the common ideological link across segments of Somali society, the diaspora, and even the global jihadi movement.

2009. [10] As noted before, this strong position bolstered al-Shabaab's numbers and reinforced its universal narrative. Today, al-Shabaab is estimated to field roughly 2,500-3,000 fighters, likely augmented by an additional 3,000 or so loosely aligned militia. However, much of this façade

began falling apart with the Ethiopian withdrawal in 2009 as clan disputes surfaced immediately affecting al-Shabaab's leadership and conflicts with other Somali actors.

While al-Shabaab's multi-clan leadership has been beneficial to the movement, disagreements between key leaders like Amir Ahmad Abdi Godane "Abu Zubayr" (Isaaq/Arap) from the north and Commander Mukhtar Robow "Abu Mansur" (Rahanweyn/ Mirifle/Laysan) have created friction within the group. Al-Shabaab's Ramadan offensive in 2010 ended with numerous reports in the Somali press of a major leadership rift within al-Shabaab - a reaction to the failed offensive and the grievances of clan constituents. Specifically, Mukhtar Robow allegedly withdrew his Rahanweyn forces from Mogadishu because he and Rahanweyn elders were angry that their clan fighters bore a disproportionate share of the casualties (Garowe Online, January 9; *East African* [Nairobi] January 24; see also *Terrorism Monitor*,

allowing humanitarian aid because it benefited Robow's clan constituents in the Bay and Bakool regions. [11] These clan-based leadership disagreements have increased in 2011; particularly over contentious issues such as allowing humanitarian aid and the integration of Hizb al-Islam into al-Shabaab (see *Terrorism Monitor*, August 12).

Al-Shabaab's cross-clan narrative helps to mask the relative weakness of its leaders, Amir Ahmed Abdi Godane and Ibrahim Haji Jama al-Afghani, both of whom are members of the Isaaq clan of Somaliland, an autonomous region far from al-Shabaab's normal region of operations in southern Somalia. Consequently, these leaders lack a natural power base in areas of southern Somalia where al-Shabaab dominates. In contrast, many al-Shabaab leaders with Hawiye, Darod, or Rahanweyn clan affiliations, like Mukhtar Robow, are typically better able to tap into clan-derived power bases across southern Somalia - often leading them to strike a balance between more

October 21, 2010). This incident highlights longstanding grievances between Robow and Abdi Godane dating back to 2008. Robow incurred Abdi Godane's wrath by giving safe passage to Somali government officials who were his clansmen and

pragmatic local interests and al-Shabaab's ideological hard-liners. [12]

Fighting Clan Battles

A review of al-Shabaab's battles in recent years reveals clear clan dynamics. Fighting between al-Shabaab, allied Islamist militia around Mogadishu, and Somalia's feeble Transitional Federal Government (TFG) surged in May 2009 and again during al-Shabaab's Ramadan offensive of 2010 (see *Terrorism Monitor*, October 21, 2010). In both cases, the presence of the roughly 7,000 peacekeepers of the African Union Mission in Somalia (AMISOM) prevented al-Shabaab from toppling the TFG. Fighting in central Somalia continues to ebb and flow, with AMISOM holding the initiative in Mogadishu in 2011 until taking substantial losses in al-Shabaab ambushes in October (see *Terrorism Monitor*, October 28). Sub-clan divisions are a significant factor in this violent stalemate. Within Mogadishu, the powerful Hawiye sub-clans of the Abgal, Haber Gedir, and Murosade are internally split between the government and the al-Shabaab insurgents. [13]

South of Mogadishu, al-Shabaab has engaged in clan-based fighting to control the strategically important port of Kismayo. In Fall 2009, al-Shabaab seized full control of Kismayo, consolidating power by ousting its former ally, an Islamist militia known as Hizb al-Islam. The group began as an umbrella organization comprised of various clan/sub-clan factions with alliances intended to reflect a clan-based balance of power. These included the Alliance for the Re-Liberation of Somalia-Asmara, the Somali Islamic Front, the Ras Kamboni militia, and the Anole militia. Alliances in the fighting broke down along sub-clan lines, with al-Shabaab fighters affiliated with the Marehan sub-clan ultimately defeating the Ras Kamboni militia (Ogadeni sub-clan power base) and the Harti sub-clan fighters called the Anole faction. [14] Al-Shabaab's success in taking the port represented a major strategic victory, providing access to port revenue and taxation fees. Research suggests that al-Shabaab leadership in the Kismayo area, led by Ibrahim Haji Jama al-Afghani, continues to manage al-Shabaab's interests by manipulating a network of clan allies to maintain local control. [15]

Emergence of Ahlu Sunna wa'l-Jama'a

Farther north, al-Shabaab has fought against a loosely structured alliance called Ahlu Sunna wa'l-Jama'a (ASWJ). Although nominally a Sufi conglomeration that armed itself in reaction to al-Shabaab's desecration of Sufi tombs, ASWJ is largely formed along clan lines in the Galguduud, Hiraan and Gedo regions. ASWJ's strength stems in part from clan-based support, as elements of the Habir Gedir, Dir, and Marehan sub-clans elected to support ASWJ against al-Shabaab (Shabelle Media Network, January 24; Garowe Online, January 25). [16]

Even beyond southern and central Somalia, al-Shabaab factions are tied to clans. Al-Shabaab exerts considerably less influence in Somalia's northern Puntland and Somaliland areas, but the group has conducted bombings and assassinations and is known to have active networks there. Puntland-based militia leader Shaykh Muhammad Sa'id "Atam" has fought sporadically against the Puntland government in the mountainous Galgala district of Puntland's Bari Region. [17] Atam has also been described by UN experts as "essentially a Warsengeli clan warlord," although he and his network in Puntland are known to be sympathetic to al-Shabaab and its aims. There remains some debate as to whether Atam's network has direct ties with al-Shabaab, as Atam and senior al-Shabaab members have denied the links. The UN in 2011 noted that Atam sought financial and medical assistance in Mogadishu and Kismayo, and his networks in Sool and Sanaag have "effectively merged with Al-Shabaab." [18] Much of the fighting breaks down along sub-clan lines, pitting Atam's Darod/Harti/Warsengeli sub-clan against the Darod/Majarteen clan which forms the foundation of President Farole's government. [19]

Even recruitment of foreign fighters - at least those of ethnic Somali origin - may have a clan-based component. A March 2010 report by the United Nations noted that more than half of the initial twenty Somalis who left Minneapolis to fight in Somalia had a parent from the Harti sub-clan, and several American Somalis killed in Somalia were discovered to have Harti familial ties, supporting the conclusion that recruitment has occurred along clan-linked peer networks. [20]

It is worth noting the unique challenges clan dynamics impose on al-Shabaab as the organization attempts to recruit foreign fighters. Somalia's strong clan identities, prevailing instability, and wariness of foreign influence make the country inhospitable to individuals of non-Somali origin. [21] Al-Qaeda learned this lesson in the early 1990s, when Osama bin Laden - then based in Sudan - dispatched a deputy, Abu Hafs al-Misri, to develop terrorist networks and training camps in Somalia. Abu-Hafs and his colleagues ultimately

failed, complaining that Somalis lacked commitment to jihad. According to Abu-Hafs, the al-Qaeda operatives had to pay tribal expenses, but could only buy - or more accurately rent - temporary sub-clan "loyalty" and were constantly plagued by shifting alliances. [22]

Conclusion: Clan Influence and Countering al-Shabaab
The foregoing has shown the inconsistencies between al-Shabaab's narrative and the group's clannish behaviors. Though attempting to position itself as transcending clan rivalries in pursuit of a pan-Somali and Islamist agenda, evidence shows al-Shabaab to be embroiled in local clan-based disputes.

For policy-makers, this presents multiple strategic opportunities. In terms of al-Shabaab's placement as an adherent to al-Qaeda's worldview, the organization is caught between proving its Salafi-Jihadi credentials to core al-Qaeda and affiliated movements while attempting to establish power among a Somali population that focuses internally on parochial clan interests. Any disruption to this careful balance risks either undermining al-Shabaab's carefully built power-base in Somalia or losing the support of international Salafi-Jihadis.

Partly in recognition of this opportunity, Assistant Secretary of State for African Affairs Johnnie Carson announced a new "Dual Track" policy for Somalia in October 2010 designed to support not only the TFG, but also promote local civil society and stability efforts across Somalia. [23] Success for this dual track initiative would almost certainly require greater clan involvement and therefore would challenge al-Shabaab's local power-base and potentially disrupt the group's internal leadership balance. For the strategy to succeed, Somalia's TFG will need to foster clan alliances, both militarily and politically, and show greater strength independence from AMISOM (Reuters, August 6). Some experts point to nascent indicators of an Iraqi-style "Awakening movement," however, such efforts have not yet materialized in a systemic manner (*East African*, January 24). New clan-based groups opposed to al-Shabaab have emerged, but their sustainability remains uncertain. [24]

This review of al-Shabaab's evolution and Somalia's ongoing conflict leaves little doubt that clan politics continue to influence al-Shabaab to a substantial degree. Looking ahead, the group's ability to forge and maintain clan alliances will be fundamental to al-Shabaab's trajectory and viability in the long term.

Notes:

1. "Somali Social Structure: A System of Kinship and Clan," Library of Congress, July 2010,
p. 2.
2. Andrea Levy, "Looking Toward the Future: Citizen Attitudes about Peace, Governance and the Future of Somalia," National Democratic Institute, December 6, 2010; "Somali Social Structure," *op cit*, p. 4.
3. Matt Bryden, "New Hope for Somalia? The Building Block Approach." *Review of African Political Economy* 26(79), March1999, p. 136.
4. Andrew McGregor, *Who's Who in the Somali Insurgency: A Reference Guide*, Jamestown Foundation, Washington D.C., September 2009, p. 8.
5. For a description of this term, see: Quintan Wiktorowicz," Anatomy of the Salafi Movement," *Studies in Conflict & Terrorism* 29, 2006, pp. 207-239.
6. See: Angel Rabasa, "Radical Islam in East Africa," RAND, Project Air Force, 2009; "Somalia's Divided Islamists," ICG Africa Briefing 74, May 18, 2010, p. 6; Report of the Monitoring Group on Somalia Pursuant to Security Council Resolution 1853. United Nations Security Council. March 10, 2010, p. 14.
For information about Somalia's minority clans, refer to: *Report on Minority Groups in Somalia*, Joint British, Danish and Dutch Fact-Finding Mission to Nairobi, Kenya, September 17-24, 2000, http://www.somraf.org/research%20Matrerials/joint%20british%20danish%20dutch%20fact%20finding%20mission%20in%20Nairobi%20-%202001.pdf;
7. Andre Le Sage, *Somalia's Endless Transition: Breaking the Deadlock*, *Strategic Forum* 257, Institute for National Strategic Studies, National Defense University, June 2010, http://www.ndu.edu/inss/docuploaded/SF%20257.pdf .
8. David Shinn, "Somalia's New Government and the Challenge of al-Shabaab," CTC Sentinel, March 2009.
9. Ken Menkhaus, "Violent Islamic Extremism: Al-Shabaab Recruitment in America," Testimony before the Committee on Homeland Security and Governmental Affairs, United States Senate. March 11, 2009; Georg-Sebastian Holzer. Political Islam in Somalia: A Fertile Ground for Radical Islamic Groups? Geopolitics of the

CBRNE Terrorism Newsletter – Winter 2011

Middle East 1(1), June 2008, p. 24; "Al-Qaeda's Misadventures in the Horn of Africa," Harmony Project, Combating Terrorism Center at West Point, p. 29.

10. "Somalia's Divided Islamists," *op cit.* ; Le Sage, *op cit*; Report of the United Nations Monitoring Group on Somalia, *op cit.*; "Somalia's Islamists," ICG Africa Report 100, December 12, 2005, p. 14.

11. McGregor, *op cit*, p. 15; "Somalia's Divided Islamists," *op cit*, pp. 5-7, 11; Report of the Monitoring Group on Somalia 2010, p. 27.

12. Le Sage, *op cit*.

13. *Ibid*.

14. *Ibid*; Report of the Monitoring Group on Somalia 2010, pp. 11, 17.

15. "Somalia's Divided Islamists," *op cit*, p. 9; Le Sage, *op cit*.

16. Report of the Monitoring Group on Somalia 2010, p. 11; Abdulahi Hassan, "Inside Look at the Fighting Between al-Shabaab and Ahlu-Sunna wal-Jama," CTC Sentinel, March 2009.

17. See Andrew McGregor, "Puntland's Shaykh Muhammad Atam: Clan Militia Leader or al-Qaeda Terrorist?" *Militant Leadership Monitor*, September 29, 2010, http://mlm.jamestown.org/single/?tx_ttnews[swords]=8fd5893941d69d0be3f378576261ae3e&tx_ttnews[any_of_the_words]=ata m&tx_ttnews[tt_news]=36982&tx_ttnews[backPid]=539&cHash=fa328428d5b609a8f08dc9e4994e3535 .

18. Report of the Monitoring Group on Somalia 2010, pp. 16, 20-22, 45; *Somalia Online*, "Atom denies Al-Shabaab links," May 18, 2011.

19. "Somalia's Divided Islamists," *op cit*, p. 11; Matt Bryden. New Hope for Somalia? The Building Block Approach. *Review of African Political Economy* 26(79), March 1999, p. 138; Le Sage, *op cit*.

20. Report of the Monitoring Group on Somalia 2010, p. 33.

21. "Al Qaeda in Yemen and Somalia: A Ticking Time Bomb," Report to the Committee on Foreign Relations, United States Senate, January 21, 2010, pp. 4, 14.; Andrew Black, "Recruitment Drive: Can Somalia Attract Foreign Fighters?" Jane's Intelligence Review, 19(6), 2007, pp. 12–17.

22. "Al-Qaeda's Misadventures in the Horn of Africa," *op cit*.

23. U.S. State Department: A Dual-Track Approach to Somalia. Statement by Assistant Secretary of State for African Affairs, Ambassador Johnnie Carson at the Center for Strategic and International Studies (CSIS). October 20, 2010. http://csis.org/event/state-department-dual-track-approach-somalia

24. Le Sage, *op cit*.

Ahren Schaefer is a Foreign Affairs Research Analyst at the U.S. Department of State, Bureau of Intelligence and Research.

Andrew Black is the CEO of Navanti Group, LLC.

The views expressed in this article are those of the authors, and do not necessarily reflect the views of the U.S. Department of State or the U.S. Government.

Osama bin Laden 'was dead in 90 seconds'

Source:http://www.telegraph.co.uk/news/worldnews/al-qaeda/8868328/Osama-bin-Laden-was-dead-in-90-seconds.html

A controversial new account of the killing of Osama bin Laden has challenged the official story of the how the al-Qaeda leader died during the raid on his Pakistani hideout in May.

Wreckage in the Bin Laden compound after the US raid Photo: REUTERS

Chuck Pfarrer, a former commander of US Navy SEAL Team Six, whose

members carried out the assault, claims bin Laden was shot dead almost instantly rather than killed in a 45-minute firefight.

Claiming to have interviewed several men involved in the raid, Pfarrer also contradicted the official account of how the SEAL team landed and how one of their Black Hawk helicopters crashed. "The SEALs entered the building after being deposited on the roof by the lead helicopter, not from the ground," Pfarrer said in a statement about the book. "Only minutes after bin Laden was dead did the lead helicopter, heading for a landing spot, lose altitude and sink, tail-first, into the large walled enclosure east of the main house." Pfarrer explains that if the SEALs had been forced to climb stairs to reach bin Laden, as has been officially claimed, he would have had enough warning to arm and effectively defend himself. "Bin Laden was dead within 90 seconds of the beginning of the raid, not after an extended firefight," Pfrarrer said. "Four suppressed rounds were fired".

Pfarrer adds that Amal bin Laden, the al-Qaeda chief's youngest wife, was wounded in the calf during the second round of fire, as she was shoved her in the way of the shooters. This chimes more with an account that was originally

stated by US officials in the immediate aftermath of the attack, before later being withdrawn.

Pfarrer describes his book as an "explosive story of unparallelled valour, clockwork military precision, and deadly accuracy". But it was dismissed as "plain wrong" by US officials.

The book also argues that bin Laden's long-time deputy, Ayman Zawahiri, may have been ultimately responsible for leading the US to his boss because he repeatedly sent a courier, whose cover he must have known had already been blown, in and out of the compound.

A trusted Kuwaiti courier, Abu Ahmad, is believed to have been followed by US officials for several months before the raid after his name emerged in interrogations of other al-Qaeda suspects and he was tracked down to Abbottabad.

The book, which is due to be released later this month, is said to have been delayed for several weeks while being cleared by government officials. Its British edition is being revised due to concerns that individuals named may sue the author for libel.

Balkan Wahhabis threaten Europe

Source:http://glassrbije.org/E/index.php?option=com_content&task=view&id=16533&Itemid=32

After the U.S. embassy attack in Sarajevo, new and more aggressive acts of terrorism should be expected in the region that will target not only diplomatic missions and facilities of the U.S. and Western European countries, but also the military bases of NATO, member of the Southeastern European Counter Terrorism Expert Team Dzevad Galijasevic warns in an interview for International Radio Serbia. He argues that the expansion and strengthening of the Wahhabi movement in B-H and the Balkans were enabled by Bosnian political and religious leadership in Sarajevo, and the West, especially Washington,

who based their policies in the region on the political myth of Serbian guilt. In the shadow of such a political mythology a powerful radical Islamist movement came into being, having over 100.000 members in B-H, many of them ready to act at all times, says Galijasevic.

The attack in Sarajevo shows that the Wahhabi movement intensifies actions and shortens the time between terrorist acts, while giving hints on directions of the future action, says Galijasevic. " Up to the terrorist attack in Bugojno

of June 27, 2010, when one policeman was killed, Wahhabi attacks were mainly directed at the so-called unprotected targets - mostly civilians-returnees and members of other religious communities. The attack on the U.S. embassy building, which is the most protected building in B-H, suggests that future Wahhabis' targets will be western diplomatic missions, NATO military bases in B-H, as well as the B-H armed forces participating in NATO peacekeeping operations in Afghanistan and Iraq. On the other hand, the selection of protected targets shows their power, force of their structure and strength of their religious beliefs. With that in mind, future attacks could be far more damaging, with more material damage and even victims, Galijasevic says.

According to our collocutor, the political and security situation in the region was most favorable for the emergence and spread of the Wahhabi movement in B-H. Having insisted on the myth of a regulated Bosnian society, based on the premise of Serbian guilt, Western diplomacy also contributed to their stronger position. In the shadow of such political mythology, they have grown into a powerful radical Islamist movement. The Wahhabi movement in B-H today includes more than 100.000 people, and therefore it can not be seen as a marginal phenomenon, Galijasevic says. Thus, he continues, it is clear that the center of Wahhabism in the Balkans is neither in Sandzak, nor Kosovo or Montenegro, but in Sarajevo. "The case of Mevlid Jasarevic is only an indication that

the West has created a "security monster" that they can no longer control. Do not forget, Galijasevic reminds, that during the Bosnian war, Vienna was the center of organizations that financed militant Islamists, whom they still finance today. The "Washington Post" once wrote that the assistance to "third countries' in the amount of 400 million dollars and some 240 million Deutsche marks was wired into the account of the TVRA agency which is owned by Fatih Al Hassanein. The Wahhabi movement is still financed from Vienna, the seat of Wahhabi leader Mohammed Effendi Porca, Galijasevic reminds.

Successful opposition to radical religious movements requires broader social activity. This primarily means, our collocutor explains, that the political elites have to adopt such laws that will ban the operation of movements based on hatred and promotion of violence, regardless of whether these are formally registered or not. At the same time, the religious elites have to deprive such movements of the so-called religious immunity and make it clear that it is not based on the postulate of faith. And finally, countering extremism successfully involves monitoring relocation of such movements' members and the flow of money financing these movements, prohibition of financing terrorist organizations and the functioning of banks participating in it. Only in this way can we successfully confront the extremist movements, such as the Wahhabism, concludes Dzevad Galijasevic.

Myths of the Bin Laden Raid

Source:http://www.thedailybeast.com/articles/2011/11/06/new-book-details-seals-raid-that-killed-osama-bin-laden. html

There was no running gunfight. And the SEALs did not have a kill order. Richard Miniter on the new book detailing the night al Qaeda's chief died—and the headaches it could cause Obama. Osama bin Laden did not hear the SEALs' stealthy helicopter until it hovered over the roof of

his three-story home and the chopper's spinning blades smashed his plastic patio chairs against his bedroom window.

In less than 10 seconds, the SEALs had jumped onto the roof, crawled across the rain-stained tiles, and descended onto bin Laden's patio. The bearded terror leader sleepily opened his bedroom door and then, spotting two armed men with night-vision gear coming down the hall toward him, quickly slammed it. They were right behind him.

Navy Seals photographed during a drill at the John C. Stennis Space Center in Mississippi on October 25, 2010., John Scorza / U.S. Navy via Getty Images

As the SEALs forced open the bedroom door, they heard bin Laden's youngest wife screaming in Arabic while raising a blanket to block their view. Behind the rising blanket, they saw bin Laden scrambling for an AKSU machine pistol.

As she tried to shield him, bin Laden shoved his wife into the line of fire. It was the last thing he did.

The first round went into the mattress behind bin Laden. The other three rounds found their mark as the two SEALs fired as one.

Bin Laden's pistol now hangs on the wall of SEAL Team Six's Virginia base, beside the photos of comrades killed in action.

These are the kinds of inside details that emerge from Chuck Pfarrer's new book **SEAL Target Geronimo.**

Pfarrer certainly had access. A SEAL Team Six assault-element commander in the 1980s, he is known inside the intelligence community for his well-regarded first book, Warrior Soul, and inside Hollywood for writing and producing movies including Navy SEALs, Hard Target, and Virus. He clearly had detailed conversations with senior officers in the SEALs' chain of command (especially Adm. William McRaven and then–SEAL Team Six commander Scott Kerr) and understands the vocabulary and the culture very well.

But some details in his book could complicate the 2012 presidential race. Pfarrer reports that the White House overruled the Navy plan to have two F-18 Hornets provide air support for SEALs helicopters, which would have been easily shot down if found by Pakistan's Air Force. Also scrubbed were the latest-generation stealth helicopters, known as "ghost hawks." The SEALs would have to make do with the older Stealth Hawks, which had mechanical problems. Ultimately, one crash-landed due to faulty electronics and had to be
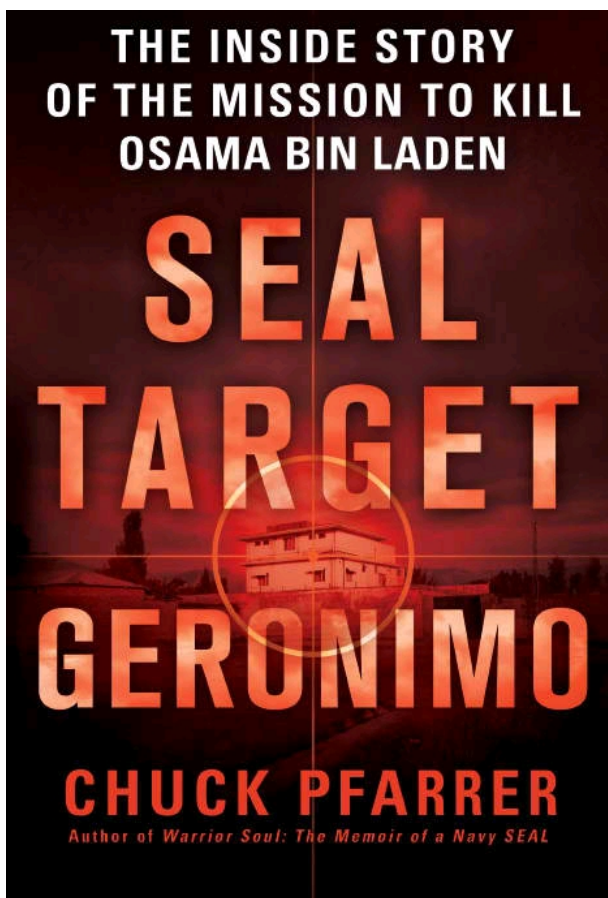
demolished on the site. Each of these decisions—to deny fighter support and to use older helicopters—may have been sound. Putting fighters in Pakistani airspace or allowing the Pakistanis to see the latest technology might have complicated relations between America and its Janus-faced ally, Pakistan. Republicans may have been reluctant to attack the president over an achievement that even Dick Cheney applauded. Still, Pfarrer's findings could fuel critics of the president who think he was quick to take personal credit and play politics with the SEALs' successful mission.

Obama may also have trouble explaining why he publicly announced bin Laden's death just hours after it occurred. The SEALs captured 12 garbage bags worth of notebooks, hard drives, satellite phones, and other digital devices. The data could have been used to launch surprise raids on all the senior members of the al Qaeda network, while the leaders turned on each other and wondered who the traitor was. For the SEALs and other special operators I've spoken with, that was the natural next move. Al Qaeda could have been rolled up in six months. Pfarrer captures the SEALs' resentment of the president, whom they see as publicity-seeking. He ignores the White House's concerns: the nation had waited almost 10 years for bin Laden to be brought to justice, and that news might have leaked.

Pfarrer also does his best to poke the CIA in the eye. He points out that the agency insisted on having one of its officers in on the raid. While we are repeatedly told that the CIA man had little experience "fast-roping" down for helicopters and doesn't have the training that the SEALs do (who does?), only in an aside are we informed that he was the only one who could speak Arabic and other local languages. He was the only man who could interview the prisoners or quiet the women

and children in the compound. Also, the CIA's role in locating bin Laden is dismissed in a throwaway paragraph. That's unfair. The CIA took a few clues from the interrogation of Khalid Sheikh Mohammed, the operational planner of the 9/11 attacks, and located bin Laden's trusted courier, Abu Ahmed al-Kuwaiti. Then the agency persuaded a colonel in Pakistan's feared intelligence agency, the ISI, to provide key documents, including the plans for bin Laden's Abbottabad compound. CIA officers rented apartments and surveilled the bin Laden compound for months, until they could persuade their superiors to deploy satellites. And so on. The CIA's role in the operation remains an exciting, but untold, story.

SEAL Target Geronimo explodes a number of media myths about the raid to kill bin Laden.

It was not a "kill mission" from the start. The SEALs had no explicit orders to kill the archterrorist and would have captured him if possible.

Pfarrer captures the SEALs' resentment of the president, whom they see as publicity-seeking.

There was no "45-minute" running gun battle. The SEAL team fired only 12 bullets, and the whole operation lasted only 38 minutes.

The most provocative part of the book is pure speculation: by killing bin Laden, did the SEALs accidentally do Zawahiri's dirty work? Ayman al-Zawahiri is al Qaeda's No. 2 and wanted to be No. 1. Maybe Zawahiri used couriers he knew were known to America's spies, hoping they would find bin Laden and dispatch him. Also, Zawahiri, a physician, never apparently treated bin Laden for Addison's disease, a condition that was suggested by bin Laden's autopsy results aboard the USS Carl Vinson. So maybe bin Laden was set up by his deputy. As the British Foreign Office used to famously say: "Interesting, if true."

Highly-trained Indian K-9s join counter-terror forces
Source: http://www.homelandsecuritynewswire.com/dr20111108-highlytrained-indian-k9s-join-counterterror-forces

CBRNE Terrorism Newsletter – Winter 2011

The Indo-Tibetan Border Police (ITBP) has a highly-trained unit in its force unlike any other in the world.

Police handlers have taught six Labradors to carry explosives in their teeth, sneak into terrorist lairs, plant remote-controlled bombs, hide secret cameras, interpret body language, and understand English and Hindi.

"It's the first time in India such a dog squad has been successfully trained in dropping of bombs, video and audio devices and other equipment inside enemy hideouts. They will be carrying them in their mouth and drop it inside the suspected hideout and when they report back to their handler and commander, then only the next step will be taken – triggering the blast through remote control," said DK Pandey, an ITBP spokesman.

ITBP's Labrador's can plant explosives, listening devices // Source: bleacherreport.com

In addition, the dogs have been taught to snatch and retrieve weapons from enemy suspects and determine whether they are alive or dead following an attack.

The Labradors have even been trained to understand the scope of the mission. "If there are five enemies inside a hideout the trainer will say 'three plus two' and the dog will bark five times," Pandey said.

Dilip Trivedi, ITBP's additional director general, said the dogs would be deployed in situations where it was too dangerous to send officers.

"During an encounter with an enemy, if our soldiers are under fire and unable to reach the enemy's hideout, say a building, these dogs can approach the target and secretly plant explosives. When it goes off, the terrorists would be exposed and thus easily targeted. As they are smaller in size to men, these canines are not easily spotted by the enemy. According to the situations, they further lower themselves and approach targets by crawling," Trivedi explained.

"Using these dogs would minimize casualties of our soldiers during a confrontation with an enemy. These canines are specially trained to target terrorist hideouts with deadly precision," he added.

Animal rights activists have voiced concerns over the use of dogs in the battlefield, but Pandey said the team works to ensure that the dogs are safe and well-protected.

"The safety of the dogs will be ensured before setting them off from a mission," he said. "They are great assets for the force and it takes around one year to train them. Apart from healthy diet the dogs have to wear specialized jackets for safety."

So far only six Labradors have been trained to complete these types of special missions, but Trivedi hopes that more will join their ranks soon.

"This is just the beginning of an experiment to make our forces more efficient and stronger. Presently, it is a small squad of six Labradors only. Dogs of other breeds can also be trained for this purpose," Trivedi said.

Israel rushes airliner defenses as Libya leaks SAMs
Source: http://english.alarabiya.net/articles/2011/11/11/176548.html

Israel has accelerated the installation of anti-missile defenses on its airliners, a security official said on Friday, seeing an enhanced risk of attack by militants using looted Libyan arms. Jets flown by El Al and two other Israeli carriers are being equipped with a locally made system known as C-Music that uses a laser to "blind" heat-seeking missiles, the official said, giving a 2013 target for fitting most of the fleet. As a stop-gap, Israel is adapting air force counter-measures for use aboard civilian planes, said the official, who declined to elaborate on the technologies involved, or to be identified.

"We have long been aware of the threat and were ahead of the rest of the world in preparing for it. Libya has meant government orders to step things up even further," the official said, citing intelligence assessments that chaos during the North African nation's uprising against Muammar Qaddafi allowed trafficking of Libyan shoulder-fired missiles to Palestinians and al-Qaeda-linked groups in the Egyptian Sinai.

Israel began deploying another system, "Flight Guard", on El Al after al-Qaeda tried to shoot down a planeload of Israeli tourists in Kenya in 2002. Flight Guard's use of diversionary flares set off safety concerns abroad and the Israelis turned to C-Music, manufactured by Elbit Systems Ltd.

CBRNE Terrorism Newsletter – Winter 2011

According to the Israeli official, Prime Minister Benjamin Netanyahu's government is covering the $1 million to $1.5 million that it costs to fit C-Music to each plane.

The bathtub-sized pods, built into the planes' bodies, increase drag in flight, meaning "a few million (dollars) a year" in extra fuel expenses, the official said, adding that this, too, would be borne by the government. Israel's main international gateway, Ben-Gurion Airport, is 10 km (6 miles) from the occupied West Bank where, along with the Islamist-ruled Gaza Strip, Palestinians want a state.

The Israeli official said he had no information indicating the presence of anti-aircraft missiles in the West Bank — unlike in Gaza, which has seen an influx of smuggled weaponry from Egypt since Israel withdrew settlers and soldiers in 2005.

The official said Netanyahu had, in closed-door discussions, described C-Music as a way to help reassure the Israeli public about security should the government one day return occupied land to the Palestinians under a peace agreement. Asked for confirmation, Netanyahu's spokesman, Mark Regev, quoted him as saying that "in any possible peace deal there have to be effective security arrangements that can deal with a range of security threats, including shoulder-fired missiles".

Israel also wants to protect traffic to its small airport in the Red Sea resort of Eilat, which abuts Jordan and Egypt, where Islamist militants have operated in the past. Armed infiltrators killed eight Israelis on the Egyptian border on Aug.18.

Olympic HQ built in secret for SAS

Source: http://www.thesun.co.uk/sol/homepage/news/3911459/Olympic-HQ-built-in-secret-for-SAS.html

A TOP secret new SAS base is under construction — at the Olympics.

It means the elite troops can combat any terrorists at next year's London Games in an instant, The Sun can reveal.

A source said last night: "It reflects the gravity of the threat."

Chinook helicopters have been in action over the capital for months ferrying special gear to the new East London HQ.

Underground bunkers will house even more crack troops.

Crests ... SAS and SBS badge

The SAS will have a key role in massive security at the Olympics — using "black ops" BOATS to swoop via the Thames if terrorists attack.

A secret new riverside base being built for the Who Dares Wins heroes in East London will be home to a fleet of the high-powered rigid inflatables.

It means elite units can speed there "in seconds" using the network of waterways around the Olympic site that make it an island — with no fears about being held up in London's notorious traffic.

The plan to enlist Old Father Thames as an ally was hatched as part of a ring of steel that will be thrown around the London Games next year.

A source said last night: "All scenarios are being anticipated. London will be protected like never before — and the message is clear.

"If anyone is fool enough to try to endanger the public at these Games they will be met with the swiftest retribution by the best-equipped troops of our most elite fighting units."

Fearsome ... arsenal at SAS base

A fearsome arsenal of weapons will be housed at the new SAS HQ along with the boats. Firepower will include sub-machine guns, assault and sniper rifles, stun grenades — like those famously used in the Iranian Embassy siege — and teargas launchers.

The SAS will also have biochemical suits on standby in case of a "dirty bomb" attack.

Anti-terror chiefs believe the biggest threat is from al-Qaeda.

Brit star ... Jessica Ennis

With the eyes of the world on the London Games — and Brits cheering on athletes such as Sheffield's

heptathlon ace Jessica Ennis, 25 — bloodthirsty fanatics would glory in staging a Mumbai-style massacre.

CBRNE Terrorism Newsletter – Winter 2011

To combat the threat, a network of underground bunkers housing even more Special Forces will have been constructed in time for the opening ceremony.

Helicopters will also be at the ready to fly in reinforcements. Our source said of the SAS's task at the Olympics: "They've been preparing for months. It's a huge mission and reflects the gravity of the threat."

The £486million Olympic stadium sits on former industrial land between the Old River Lea and the City Mill River. Other waterways including St Thomas' Creek mean it is surrounded. People injured in any attack could also be swiftly evacuated by river.

The source said: "Troops can deploy by air and water and be on site in moments. Then you've got force on the ground while the situation is monitored by the air.

"Major evacuation plans are still being revised in case of a terrorist attack. But the most important thing is having the access and ability to strike back at terrorists.

"That will be achieved and those plans are in place."

Fire and water ... heavily-armed troops in high-speed rigid inflatable

The Sun told in May how the SAS fired off live ammo at the Olympics Village — as they practised tackling a hostage crisis like the one at the 1972 Munich Games that saw 11 Israeli athletes and coaches massacred.

In July we revealed the Special Boat Service — sister force of the SAS — was in training to thwart suicide bombers off Weymouth in Dorset, where 60,000 sailing fans will flock to Olympic events.

Yachts there will also be guarded during the Games by Chinook helicopters operating out of RAF Odiham, Hants.

Last night the MoD refused to comment on the latest anti-terror plans.

► A MINI "Olympics" to road-test the new stadium ahead of the Games — involving hundreds of charity fundraisers who will be cheered on by up to 20,000 spectators — will be held on April 1.

Better hospital responses to terrorist attacks

Source: http://www.homelandsecuritynewswire.com/better-hospital-responses-terrorist-attacks

Research and Markets has a new offering: "Hospital Planning For Terrorist Disasters: A Community-Wide Program."

Terrorist attacks are less likely to occur than other disasters, but they can have greater impact on hospital operations. Hospital emergency preparedness programs had not included provisions for terrorism events, but the 9/11 attacks was the catalyst that convinced many emergency management officials of the need for such plans.

Following the anthrax bioterrorism attacks in late September 2001, the U.S. Centers for Disease Control and Prevention (CDC) began focusing on emergency operations systems for public health facilities. Despite the limited number of direct victims in those attacks (twenty-two people), the public health effects were widespread, with large numbers of people receiving antibiotic prophylaxis. Psychological effects were also considerable.

Research and Markets note that in order to develop an effective emergency preparedness plan, hospital leaders should build on previous experiences with disaster management, especially with respect to human behavior, as well as on published research. The book is intended to complement resources such as the U.S. Department of Health and Human Services' Public Health Emergency Response Guide and assist hospital planners in preparing for terrorism events and other disasters
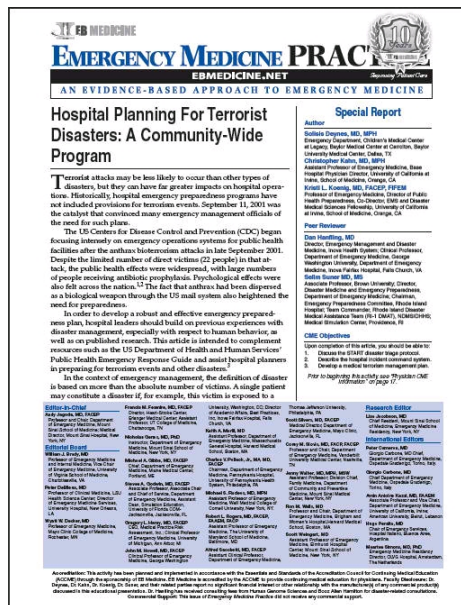
NOTE: More details about the book at:
http://www.ebmedicine.net/store.php?paction=showProduct&pid=163

Death by remote
By Anshel Pfeffer
Source: http://www.haaretz.com/weekend/week-s-end/death-by-remote-1.394968

Lieutenant Colonel Ido doesn't wait for the question. He takes up the question of morality at his own initiative, almost at the start of the interview.

"It's far from simple, when someone is in an air-conditioned trailer eating yogurt under fluorescent lighting, and within 30 seconds, with his help, another person dozens of

kilometers away is dead," he says. To him, that sums up the dilemma facing operators of unmanned aerial vehicles (UAVs, also referred to as "drones") in the Israel Defense Forces. It is one of the major issues Ido must address as commander of the school for UAV operators at the Palmahim air force base.

"This profession, of UAV operator, has brought new aspects to the army experience," Ido continues. "These fighters participate very intensively on the battlefield, decide fates in seconds, but are not themselves in any sort of danger. This would seem to make things easier for the Jewish mother, but the soldier himself faces far more acute conflicts.

The UAV base. Photo by: Nir Kafri

"A soldier on the battlefield needs primarily to survive. He doesn't have to think very much when he opens fire; he is exempt from considering all kinds of issues. For UAV operators, survival is not part of the equation; all that remains are operational and moral considerations."

Lt. Col. Ido (censor's restrictions permit use of only his first name) has been on the job for three years. Over that period, he greatly expanded the extent to which he addresses moral issues while teaching a course for "inside operators" - officers who operate airborne UAVs and command unmanned missions. ("Outside operators" are in charge of the drones takeoff and landing; once the craft enter a flight path, they are taken over by "inside operators.")

As part of the course, Ido leads the "Morality and Combat" workshop. He starts with the Kibiyeh operation in 1953, in which Israeli soldiers killed 60 civilians in the Jordanian village of Kibiyeh in retaliation for a terrorist attack in Yehud. The course participants read the seminal essay "After Kibiyeh" by philosopher Prof. Yeshayahu Leibowitz, who wrote, "Only the decision of one who is capable of acting and on whom rests the responsibility for acting or refraining from action can pass the genuine test of morality. We, the bearers of a morality which abominates the spilling of innocent blood, face our acid test only now that we have become capable of defending ourselves and responsible for our own security. Defense and security often appear to require the spilling of innocent blood." (Translated by Eliezer Goldman, the editor of "Judaism, Human Values, and the Jewish State," a collection of essays by Yeshayahu Leibowitz, published by Harvard University Press, 1995.)

"When people are killed by mistake, we are tormented, and that's how it should be," Ido says. "I've met some people who had a very hard time with it. Some coped, and others wanted to leave. I told them, 'This is dirty work. Who would you like to have do it? We would all like to be professors.'"

Legitimacy debate

The use of UAVs has also given rise to moral dilemmas in the U.S. military, especially in the past two years, since President Barack Obama decided to use them extensively in the war on Al-Qaida in Afghanistan, Iraq, Pakistan, Yemen, Somalia and Sudan.

Fierce debates are underway in the American media and academia over the legitimacy of such attacks. Are they not actually extrajudicial executions? This dispute was exacerbated in September after the U.S. military assassinated an Al-Qaida cleric - and American citizen - Anwar al-Awlaki, in a drone attack in Yemen. The Obama administration has no doubts: Sending armed drones into

confrontation zones is far preferable to sending in ground troops. They are far cheaper, American soldiers aren't killed, and they cause fewer diplomatic rows.

The Americans are developing and acquiring hundreds of new UAVs capable of carrying advanced missiles. The British, too, have recently begun to use them in Afghanistan, and there is no doubt that they will become increasingly prevalent, as other countries acquire them for assault missions.

Whereas in the West there is a lively public debate over the "robot wars," in Israel there is almost no discussion of the subject. There are various reasons for this. The debate over "targeted assassinations" was already conducted during the second intifada, and even reached the High Court of Justice.

The American drones can launch attacks on the other side of the world, where soldiers cannot go. In contrast, the use of unmanned aerial vehicles by the IDF takes place largely across the border, in the Gaza Strip and Lebanon, places where Israeli ground forces recently operated and where they will almost certainly return in the future. And there is also the military censorship that turns every report about armed drones - as opposed to those used for observation and intelligence gathering - into one based on "foreign sources."

This situation changed somewhat two months ago, when WikiLeaks released two U.S. State Department documents describing conversations between IDF generals and American diplomats. The former military advocate general, Maj. Gen. Avichai Mendelblit, told the Americans about an IDF investigation into the killing of 16 Palestinians in a Gaza mosque.

"Mendelblit said the facts were known," the diplomat wrote in his summary to Washington. "A UAV fired at two Hamas fighters who were standing in front of the mosque and the result was 16 casualties inside the mosque - due to an open door through which shrapnel penetrated during a prayer service," Mendelblit reportedly continued."

In June 2009, Human Rights Watch published a report based on testimonies of Palestinians in the Gaza Strip. According to the report, Israeli drones wounded and killed at least 29 Palestinian civilians during Operation Cast Lead, a half year earlier. This, the report said, was a violation of the laws of war, because the operator can see civilians are being targeted and alter the missile's trajectory accordingly. At the time, the IDF Spokesman refused to respond to the report, but a senior officer in the UAV unit says, "It grieved me, because I know how hard we work to avoid cases like that. Sometimes, there is a UAV in the sky whose whole mission is to search and check that there are no noncombatants in the attack zone."

Says Lt. Col. Ido: "The asymmetrical confrontation against terrorist organizations in urban areas, the territories and Gaza takes us to the extremes. We operate in those places, and the key, above all, is professionalism. A professional generally does not make moral errors and achieves the goal with minimal collateral damage. When the terrorists send children to collect a missile tripod after an attack, it is professionalism to see that it is a child and not an adult, and to recognize this before someone attacks."

Triple D

Earlier this fall, the air force's first UAV squadron marked its 40th anniversary. The event was attended by air force commander Maj. Gen. Ido Nechushtan and senior figures from Israel Aerospace Industries, the manufacturer of the Shoval (Heron), the main UAV used in intelligence-gathering missions.

The Shoval lifts off and lands two days later, and in that time executes a large number of missions in different regions. Operational orders come nonstop from a variety of "clients" within the IDF and the intelligence community. In the course of one such sortie, the Shoval might be sent to perform four or five tasks that were not planned before the liftoff. The operators in the control trailer are rotated every four hours.

"Many people are surprised that we have been around for 40 years already," says the squadron commander, Lt. Col. Zviki. "Originally, the UAV was intended for high-intensity warfare and less for routine security. Nowadays, the UAV accompanies every military mission from above." This means everything from gathering intelligence in what the air force calls the "third circle" - namely, the Iranian sector and its satellites - to assisting firefighters in the Mount Carmel forest fire and guarding worshipers at Joseph's Tomb in Nablus. It was also recently decided that drones would be a major part of the protection afforded the offshore natural gas rigs in the Mediterranean.

Lt. Col. Zviki, an F-16 combat navigator by training, says the term "unmanned" is not a good description. "It's just that the cockpit is on the ground," he says. "The aircraft is technically manned, even though we don't really fly a plane but rather operate an aircraft in flight. Instead of a stick and throttle, we have a mouse and a keyboard."

The range of the missions flown by the squadron and the two other, younger UAV squadrons reflects the transformation of the threats facing the IDF. The first, American-made UAVs, which were introduced into service in 1971, were quite awkward and took only stills. After the Yom Kippur War, it was decided to expand the use of drones, mainly to support manned warplanes, in order to address the threat of the Arab armies' surface-to-air missiles, which downed dozens of Israeli planes in the 1973 war. The first extensive use of UAVs was in the Lebanon War of 1982, in the form of smaller drones.

"These days it's no longer a drone - a model plane with a camera," says Col. Eli Ankori, head of the air force's UAV, Space and Intelligence Branch. "We are now talking about a very extensive portfolio, and there is a broad understanding these days that wherever we can execute a mission unmanned, we will do so. It is clear that this means every mission in which you don't want to risk lives and can execute without risking human life. There is a tremendous advantage to UAVs. They are also significantly less costly, as the per-hour cost of flight is far lower."

Col. Eli switches to English to sum up the missions where UAVs can take the place of manned aircraft: "Triple D: dirty, dull, dangerous."

How the War on Terror Has Militarized the Police

By Arthur Rizer and Joseph Hartman

Source: http://www.theatlantic.com/national/archive/2011/11/how-the-war-on-terror-has-militarized-the-police/248047/

At around 9:00 a.m. on May 5, 2011, officers with the Pima County, Arizona, Sheriff's Department's Special Weapons and Tactics (S.W.A.T.) team surrounded the home of 26-year-old José Guerena, a former U.S. Marine and veteran of two tours of duty in Iraq, to serve a search warrant for narcotics. As the officers approached, Guerena lay sleeping in his bedroom after working the graveyard shift at a local mine. When his wife Vanessa woke him up, screaming that she had seen a man outside the window pointing a gun at her, Guerena grabbed his AR-15 rifle, instructed Vanessa to hide in the closet with their four-year old son, and left the bedroom to investigate.

Over the past 10 years, law enforcement officials have begun to look and act more and more like soldiers. Here's why we should be alarmed.

Within moments, and without Guerena firing a shot–or even switching his rifle off of "safety"–he lay dying, his body riddled with 60 bullets. A subsequent investigation revealed that the initial shot that prompted the S.W.A.T. team barrage came from a S.W.A.T. team gun, not Guerena's. Guerena, reports later revealed,

had no criminal record, and no narcotics were found at his home.

Sadly, the Guerenas are not alone; in recent years we have witnessed a proliferation in incidents of excessive, military-style force by police S.W.A.T. teams, which often make national headlines due to their sheer brutality.

Why has it become routine for police departments to deploy black-garbed, body-armored S.W.A.T. teams for routine domestic police work? The answer to this question requires a closer examination of post-9/11 U.S. foreign policy and the War on Terror.

Ever since September 14, 2001, when President Bush declared war on terrorism, there has been a crucial, yet often unrecognized, shift in United States policy. Before 9/11, law enforcement possessed the primary responsibility for combating terrorism in the United States. Today, the military is at the tip of the anti-terrorism spear. This shift appears to be permanent: in 2006, the White House's National Strategy for Combating Terrorism confidently announced that the United States had "broken old orthodoxies that once confined our counterterrorism efforts primarily to the criminal justice domain."

In an effort to remedy their relative inadequacy in dealing with terrorism on U.S. soil, police forces throughout the country have purchased military equipment, adopted military training, and sought to inculcate a "soldier's mentality" among their ranks. Though the reasons for this increasing militarization of American police forces seem obvious, the dangerous side effects are somewhat less apparent.

Undoubtedly, American police departments have substantially increased their use of military-grade equipment and weaponry to perform their counterterrorism duties, adopting everything from body armor to, in some cases, attack helicopters. The logic behind this is understandable. If superior, military-grade equipment helps the police catch more criminals and avert, or at least reduce, the threat of a domestic terror attack, then we ought deem it an instance of positive sharing of technology — right? Not necessarily. Indeed, experts in the legal community have raised serious concerns that allowing civilian law enforcement to use military technology runs the risk of blurring the distinction between soldiers and peace officers.

CBRNE Terrorism Newsletter – Winter 2011

This is especially true in cases where, much to the chagrin of civil liberty advocates, police departments have employed their newly acquired military weaponry not only to combat terrorism but also for everyday patrolling. Before 9/11, the usual heavy weaponry available to a small-town police officer consisted of a standard pump-action shot gun, perhaps a high power rifle, and possibly a surplus M-16, which would usually have been kept in the trunk of the supervising officer's vehicle. Now, police officers routinely walk the beat armed with assault rifles and garbed in black full-battle uniforms. When one of

have acquired bazookas, machine guns, and even armored vehicles (mini-tanks) for use in domestic police work.

To assist them in deploying this new weaponry, police departments have also sought and received extensive military training and tactical instruction. Originally, only the largest of America's big-city police departments maintained S.W.A.T. teams, and they were called upon only when no other peaceful option was available and a truly military-level response was necessary. Today, virtually every police department in the nation has one or more

us, Arthur Rizer, returned from active duty in Iraq, he saw a police officer at the Minneapolis airport armed with a M4 carbine assault rifle — the very same rifle Arthur carried during his combat tour in Fallujah.

The extent of this weapon "inflation" does not stop with high-powered rifles, either. In recent years, police departments both large and small

S.W.A.T. teams, the members of whom are often trained by and with United States special operations commandos. Furthermore, with the safety of their officers in mind, these departments now habitually deploy their S.W.A.T. teams for minor

operations such as serving warrants. In short, "special" has quietly become "routine."

The most serious consequence of the rapid militarization of American police forces, however, is the subtle evolution in the mentality of the "men in blue" from "peace officer" to soldier. This development is absolutely critical and represents a fundamental change in the nature of law enforcement. The primary mission of a police officer traditionally has been to "keep the peace." Those whom an officer suspects to have committed a crime are treated as just that - suspects. Police officers are expected, under the rule of law, to protect the civil liberties of all citizens, even the "bad guys." For domestic law enforcement, a suspect in custody remains innocent until proven guilty. Moreover, police officers operate among a largely friendly population and have traditionally been trained to solve problems using a complex legal system; the deployment of lethal violence is an absolute last resort.

Soldiers, by contrast, are trained to identify people they encounter as belonging to one of two groups — the enemy and the non-enemy — and they often reach this decision while surrounded by a population that considers the soldier an occupying force. Once this identification is made,

a soldier's mission is stark and simple: kill the enemy, "try" not to kill the non-enemy. Indeed, the Soldier's Creed declares, "I stand ready to deploy, engage, and destroy the enemies of the United States of America in close combat." This is a far cry from the peace officer's creed that expects its adherents "to protect and serve."

The point here is not to suggest that police officers in the field should not take advantage of every tactic or piece of equipment that makes them safer as they carry out their often challenging and strenuous duties. Nor do I mean to suggest that a police officer, once trained in military tactics, will now seek to kill civilians. It is far too easy for Monday-morning quarterbacks to unfairly second-guess the way police officers perform their jobs while they are out on the streets waging what must, at times, feel like a war.

Notwithstanding this concern, however, Americans should remain mindful bringing military-style training to domestic law enforcement has real consequences. When police officers are dressed like soldiers, armed like soldiers, and trained like soldiers, it's not surprising that they are beginning to act like soldiers. And remember: a soldier's main objective is to kill the enemy.

Arthur Rizer, a former Washington state peace officer who deployed to Iraq as a member of the U.S. Army Reserves, currently works at the U.S. Department of Justice. (His views do not necessarily represent the views of the Department of Justice.)

Joseph Hartman, a Ph.D. candidate in government at Georgetown University, practices law in Arlington, Virginia.

Al-Qaeda and Algiers Struggle to Cope with the Implications of the Arab Spring

By Dario Cristiani
Source: http://www.jamestown.org

Al-Qaeda's media arm released a video from Dr. Ayman al-Zawhiri in October that focused mainly on American "defeats," but also offered the al-Qaeda leader's views on Algeria. Al-Zawahiri called upon the people of Algeria to rise up against their government, which he claimed was

guilty, among other things, of fighting the imposition of Shari'a in Algeria and serving the interests of America and France in the Mediterranean. Al-Zawahiri also called on the soldiers of Islam in the region (i.e. al-Qaeda in the

Islamic Maghreb - AQIM) to offer an example of jihad and resistance (as-Sahab Media, October 11). [1] On October 17, al-Qaeda's media wing posted another video entitled "Algeria and the Battle of Patience" by senior al-Qaeda commander Abu Yahya al-Libi. This message called upon Algerians to depose President Bouteflika and his regime (as-Sahab Media, October 18):

"Rise up with your sons and bring back your uprising against a fragile, shaky regime, as life is chances, and the winds are winds of change, and relenting and settling won't work with it. Should your winds blow, take advantage of them, as after each storm there will be calm… So, revolt O defiant people in the face of injustice and tyranny with higher determination and stronger challenge in order to overthrow this moldy regime that stole your revolution, wasted your wealth and enriched your enemy with your money, and caused you poverty and forbade you to have the best of your resources, and opened your country for the bastards of the West to enjoy your resources, and made your honorable sons displaced around the world asking for peoples' help. [2]"

Why then, has al-Qaeda Central turned its focus to Algeria at this time?

A Contextual Assessment

These statements must be contextualized in a wider political and strategic framework and in light of the dynamics of change working in the region and interacting with global and long-term trends. There are three main contexts, which can be divided in three geopolitical circles:

- Global Dynamics: These statements are an attempt by al-Qaeda Central to retain the political initiative. The capture and death of Bin Laden represented a great symbolic blow to the organization, whose operational capabilities were already in decline. For al-Qaeda/jihadist elements, Algeria has a strong importance for historical reasons but several current trends and developments have attracted al-Qaeda's attention: Algeria is in the midst of a vast year-old regional turmoil, it has good relations (more or less) with all the main "far enemies" of al-

Qaeda (the United States, the United Kingdom, France and Spain); it supported, although not very vocally, Mu'ammar Qaddafi until the end of his regime and its political balance is currently considered fragile. These messages are likely also a signal to AQIM to become more resolute in its fight against the Algerian government. AQIM suffers from the same problems as al-Qaeda Central: It has lost the political initiative over the past few years and despite some recent signs of survival, the group's ability to attack the Algerian government has decreased progressively.

- Regional Troubles: One of the novelties of the Arab Spring revolts was that, from the very beginning, they were not characterized by a resolute Islamist rhetoric. However, the lack of a radical Islamist discourse in the uprisings does not entail the end of Islamist forces as main political players in the region. The increasing prominence of Islamist groups in Libya, the victory of Ennahada in Tunisian elections and the role of the Muslim Brotherhood in the Egyptian political transition show that Islamist-oriented groups still remain among the region's most organized political and social groups. Al-Qaeda is ideologically and politically remote from many of these players. However, this broadly considered Islamist awakening is seen as an opportunity for the movement to re-enter the political and ideological window of the Arab Spring, in which Al Qaeda has had trouble finding a place since the earliest days of the revolts.

- The National Arena: In the early weeks of the Arab Spring, Algeria was considered a serious candidate to follow the same path as Tunisia, Egypt and Libya. However, this did not happen, although there were reports of demonstrations, strikes and clashes in Algeria. The nation's domestic political picture is becoming more and more complicated as social and political cleavages emerge, but

that does not automatically entail that the regime will be destroyed. There is strong potential for an increasing destabilization of the Algerian institutional and political landscape due to questions over the health of President Abdelaziz Bouteflika and intelligence chief General Mohamed "Toufik" Mediène, housing shortages, sustained inflation in food prices, structural corruption and tensions over the distribution of wealth. With parliamentary elections upcoming in 2012 and presidential elections following in 2014, these elements likely entered into the calculations of al-Qaeda's leaders when deciding to release these statements.

The Fragile Status Quo

Paradoxically, there is a convergence of views between al-Qaeda and some Western views on the inevitability of the domino effect in considering the Arab Spring. Algeria was for some time considered to be the next in line for a national uprising. However, when the Arab Spring is discussed in the context of Algeria, the discussion must take into account developments in Algeria since 1988. Unlike Tunisia, Egypt and Libya, Algeria has already experienced a large-scale insurgency since the thorny elections of 1991. Although this did not end in regime change, its enormous impact on the political scene in Algeria is the major factor in understanding whether there is room in Algeria for another huge uprising that would provide an opportunity for AQIM to exploit it.

Currently, the elements supporting the political status quo seem stronger than those against, at least in the short term. Whether these balances are sustainable in the longer run remain to be seen; indeed, some developments – demographic pressure, persisting youth unemployment, an economy still too much dependent on oil revenues and the likely drop in gas production starting in 2012 - will likely reduce the sustainability of the current Algerian political balance. However, there are significant elements supporting a fragile and unstable status quo. In decreasing order of importance, these are:

- The memory of the civil war of the 1990s: Together with the enormous violence of the war of independence against the French colonizer, this represents an enormous psychological burden for Algerians, without distinction between social classes and geographical origins. This is by far the most important element in understanding why Algerians are so hesitant to experience another round of large-scale political violence.

- A more consistent government paternalism: As a rentier state, a paternal use of economic resources was common in Algeria. In the wake of the Arab Spring, the political power structure has been able to use money to reduce political tensions. This situation is different from the late 1980s, when Algeria was in a far more difficult economic situation given the crisis in global oil prices and the failure of its socialist economic model. Since the beginning of the general regional uprising, Algerian authorities have increased public sector wages, provide more generous food subsidies to face food inflation and given handouts to unemployed youth (Reuters, October 20). Moreover, huge infrastructure projects focused on reducing the impact of housing shortage are ongoing. The levels of Algeria's foreign currency reserves, currently estimated at about $150 billion, can allow Algerian authorities to keep working on this track.

- The losing appeal of radical Islamist messages: In the late 1980s, Islamist narratives were the only catalyst of discontent in an ideological and political landscape dominated by socialist ideology and rhetoric, which were identified by Islamists with the existing power structure and therefore considered illegitimate. Now, however, radical Islamist messages have lost their appeal given the violence of the past 20 years and the presence of moderate Islamist parties in the political mainstream of the country, a significant difference from the one party system of the 1980s dominated by the Front de Libération Nationale (FLN).

- The interests of the external players in stability: In the case of Libya, some of the main external players had an interest in getting rid of Qaddafi, including France, the UK, the United States and eventually Italy. However, this convergence of aims is unlikely to be replicated and their stances on Syria, apart from some rhetorical peaks, demonstrate a lack of interest in providing open and resolute support for other revolts. In the case of Algeria, this element is important as Algiers is a fundamental actor for the overall security of the Maghrebi/Saharan/Sahelian region as well as the Mediterranean region. Washington and Paris have a strong interest in the stability provided by Algeria. Moreover, Algerian energy supplies are key to the energy needs of Italy, which is now in financial crisis. No external government, even among those rhetorically committed to supporting democracy, has any interest in supporting a possible destabilization of Algeria.

- The strange openness of the political system: Although it remains an authoritarian country, the political system of Algeria is now more open than it was 20 to 25 years ago. Debates and clashes between political factions and players are frequent and the press openly criticizes political personalities and factions in a rather open fashion compared to the standards of the wider Middle East and North Africa area.

- On the other hand, this openness helps avoid any unexpected explosion of political and social conflict, as happened in the nations more affected by the Arab Spring.

- The "normality" of discontent: Demonstrations, strikes and protests are a common features of the Algerian the political landscape, giving Algiers more experience than its neighbors in handling political and social turbulence. The opposition, moreover, is fragmented, with none of its main leaders able to present an ideological alternative appealing to a large segment of the population.

- The lack of Tahrir Square-style mass protests. This absence is explained by the peculiar geographical features of the Algerian urban landscape: for instance, Algiers is characterized by a lack of large open spaces, with very few wide boulevards and squares, thus discouraging huge gatherings of people (Jadaliyya.com, September 16; Daily Star, [Beirut], February 8).

Conclusion

Al-Qaeda, in general, was incapable of asserting its influence over the events of the Arab Spring, suffering from a general inability to impose its ideological imprint on the narratives of discontent in the Arab and wider Islamic world over the past decade. Though the movement can exploit development to gain greater room to maneuver, as in the Egyptian Sinai and the Sahel following the Libyan war, politically and ideologically, al-Qaeda has remained removed from development.

Placed in a situation of weakness on a global scale following Bin Laden's death, al-Qaeda is now trying to retain some political significance. In its current perceptions, Algeria is now the weak link in the wider Middle East-North Africa region and one in which, given the presence of a clear and active franchise, al-Qaeda would try to integrate itself into the dynamics of the Arab Spring by pushing for demonstrations and regime change. The operational links between al-Qaeda Central and AQIM remain weak but it is likely that these statements were a suggestion for AQIM to take action.

The strategic picture for AQIM has improved over the past few months amid the implosion of Qaddafi's regime and the more general increase in regional instability, with weapons and veteran fighters spreading through the Sahel.

As confirmed recently by an AQIM commander, AQIM acquired weapons from Libya during the collapse of the Qaddafi regime and is trying to stress its ideological connection with the Libyan Islamists (Agence Nouakchott d'Information, November 9; Jeune Afrique, November 10). The strategic developments of the Arab Spring could help AQIM to increase

its operational profile and refocus its attention on opposing the Algerian regime rather than smuggling activities in the Sahel, an outcome more likely if the Kabylia-based AQIM leadership can retain control over its autonomous and quasi-independent units in the Sahel. AQIM will also benefit if the process of state-building in Libya proves more complicated than hoped and the main focus of the Algerian security services remains domestic stability rather than counter-insurgency operations directed at AQIM.

However, it is not very likely that AQIM, as we know it today, could succeed in exploiting and at the same time reinforcing discontent against the Algerian government as it lacks the ideological depth and political flexibility to attract other segments of the opposition galaxy. Moreover, AQIM suffers from a strong unpopularity among ordinary citizens because of its kidnappings and its status as the latest incarnation of the groups fighting in the 1990s. AQIM, and consequently al-Qaeda Central, could benefit from the Arab Spring's impact on Algeria more from a strictly operational than broadly political point of view.

Notes:
1. See http://www.youtube.com/watch?NR=1&v=5qdFOTI-Kc4.
2. See http://aljahad.com/vb/showthread.php?t=12879.

Dario Cristiani is a PhD Candidate in Middle East and Mediterranean Studies at King's College London. Previously, he has been a teaching fellow in Political Science and Comparative Politics at the University of Naples "L'Orientale" and a political analyst with the Power and Interest News Report (PINR).

DHS warns terrorists targeting buses

Source:http://www.dailymail.co.uk/news/article-2060717/Newest-threat-TSA-warns-terrorists-targeting-buses-holiday-travel-season.html?ito=feeds-newsxml

In a recent Transportation Security Administration (TSA) security bulletin, officials warned state and local authorities that terrorists are increasingly targeting bus networks.

John Pistole, the head of the TSA, explained that bus networks are attractive targets for attacks because of their "accessibility" and their "open architecture."

"It's something that we've seen in reporting over time that terrorists around the world clearly are interested," Pistole said.

Officials were careful to note that the warning did not come in regards to a specific threat or that there was credible intelligence indicating that terrorist were plotting an immediate attack, instead the bulletin sought to warn local law enforcement agencies of the growing risk to buses.

The bulletin, titled "Terrorist Concerns Regarding Mass Transit Bus Systems," noted that attacks on buses are far more common than on airlines and terrorist groups could try to recruit employees who work in the bus industry.

Between 2004 and 2009, there were more than 725 attacks on buses. Most notably, in 2005 during the coordinated attacks on the London transportation system, a suicide bomber blew himself up on a double-decker bus killing two.

Soft target: The federal government believes American bus systems are easier for terrorists to attack than airlines

In addition al Qaeda's magazine Inspire suggested using buses to ram into crowds, buildings, and other vehicles, while intelligence gathered from Osama bin Laden's compound indicated that he preferred using buses to carry out attacks. "He always felt that he wanted to

leverage his targets. Both to use a soft target, one that he had access to, and one that was spectacular because you know terrorism it has to resonate within the world of ideas. It's political theatre, and he had a really good grasp of that," explained Chuck Pfarrer, the author of "Seal Target Geronimo."

Railroad authority investigates threat of unattended trains

Source: http://www.homelandsecuritynewswire.com/railroad-authority-investigates-threat-unattended-trains

The Federal Railroad Administration (FRA) is currently investigating the dangers of unattended freight trains, especially those that carry hazardous materials, following a report by a Seattle, Washington television station.

In a segment called "Problem Solvers," KOMO News investigators boarded several freight trains throughout the state without encountering security personnel or crew members. In one instance, the news team was able to enter the unlocked lead locomotive of a train which was found idling just thirty miles north of Spokane. The train, which was left unattended for six hours, was carrying sulfuric acid, a highly corrosive liquid that would be extremely dangerous if released. Burlington Northern Santa Fe (BNSF), the train's operator, strongly denied that its trains were unsafe and called the report "sensationalized accusations and exaggerated hypotheticals." The company allows trains to go unguarded to give crews operating on twelve hour shifts time to rest as well as to keep air in the compression brake systems. BNSF also said the KOMO team "failed to recognize that there are numerous ways to immobilize a parked train such as removing essential equipment, tying down hand brakes, or isolating electrical fields on the locomotive." "Joe," a BNSF employee interviewed for the story, claimedthat leaving trains unattended is company policy and that safeguards such as setting the handbrake would not be able to halt a train if its engines were fully throttled. "It wouldn't be hard for anyone to move one of these trains in the path of an oncoming train, and not only kill the crew but the community, too." In 1990 a homeless man hijacked an unattended, idling Burlington Northern train, taking it for a seventy-mile joyride from Seattle to Tukwila. The Problem Solvers report also contained a videotaped deposition from an unrelated lawsuit in which Burlington Northern's senior trainmaster Doug Kayser states that the company has never tested whether or not a trespasser could operate an idling train. Following the report, Senator Maria Cantwell (D-Washington) raised the issue with Transportation Security Administration (TSA) chief John Pistole during a hearing on Capitol Hill on 9 November, asking him what TSA could do to make sure these security gaps are closed. "We will work with the FRA to make sure

these types of situations do not repeat," Pistole responded. "I think it's an issue that needs to be addressed both from a safety and security perspective." Senator Cantwell also expressed disbelief at TSA regulations which limit its authority to fifteen miles outside of the high-

threat urban area of Seattle. "There's a lot of rail traffic that goes through there [Spokane], and I think people would say, 'Wait a minute, we're not part of this protection.'" Pistole promised to review the regulations and make any changes deemed necessary.

Britain's 'most wanted' killed in drone attack

Source: http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/8900443/Britains-most-wanted-killed-in-drone-attack.html

An international alert was issued last year warning that Ibrahim Adam was trying to secure a passport and might be trying to return to Britain to launch attacks. He was killed in the tribal region of Waziristan alongside Mohammed Azmir Khan, 37.

Both men and their brothers were believed to be part of an established network of radicals from Ilford, East London with connections to al-Qaeda.

Adam's father confirmed that his son had been killed and a close friend of Khan's family, who did not want to be named, said: "They have taken it very badly - this is the second son who has been killed in a drone strike."

Adam, 24, was the younger brother of Anthony Garcia, 28, one of the men jailed for life for plotting to blow up the Ministry of Sound night club or the Bluewater Shopping Centre with a fertiliser bomb in 2004.

Adam disappeared along with his older brother

Lamine, 30, in May 2007 despite being put under a control order after previously being stopped while en route to Syria.

Lamine, who had a job as a tube driver had allegedly wanted to carry out an attack on a nightclub in Britain. He appears to have survived the drone attack.

Garcia wrote a letter to Adam from an al-Qaeda training camp in 2003, when he was still a teenager, telling him: "You have been gifted OK with the people you know but never think you are OK, always think you are nothing. "Only when you believe this will you be able to sell your life….We will meet either in this life or the hereafter.

"Study hard in Islamic matters, don't let them know you have future plans, better that they think you are a fool than someone good."

His passport photographs were found in an al-Qaeda safe house in Oslo showing Adam with four different hairstyles and clothing and were circulated to law enforcement agencies across the world.

The photographs were discovered after MI5 and MI6 unraveled a global network controlled by Rashid Rauf, a British al-Qaeda commander behind the July 7, July 21 and trans-Atlantic airlines plots.

The Adam brothers had been part of a group of militants in Ilford, East London that also included the other dead man, Mohammed Azmir Khan, 37, a father of three.

Khan's brother, Mohammed Jabar Ahmed, 34, also known as Abdul Jabber, was killed by a missile from an unmanned drone in Datta Khel, near Miranshah in North Waziristan on September 8 last year.

CBRNE Terrorism Newsletter – Winter 2011

The whereabouts of a third brother, Mohammed Tunveer Ahmed, 39, is unknown. All three were born in Sheffield and moved to London.

Tunveer and Jabar were members of the radical group al-Muhajiroun and travelled to Afghanistan around the time of the September 11 attacks to fight with the Taliban.

Like their associates in the fertiliser gang, the brothers returned to Britain but were not arrested and at some point returned to Pakistan to rejoin the militants.

Sources told the Daily Telegraph that two individuals associated with the group tried to travel to Pakistan said.

through Cairo and Dubai but were turned back at Heathrow airport and put under control orders.

Another associate, tube driver Amir Ali, was acquitted of trying to travel to Pakistan after telling a jury he was set up by MI5.

The Adam brothers' father, Elias, told the Daily Telegraph last year that he feared he would never see his other two sons alive again. "I am heartbroken. I am worried that I will never see them again. I just want them to come back home," he

Overview of terrorist incidents worldwide – October 2011

Source: http://www.coedat.nato.int/

Country	Number of attacks	K	W	A
Iraq	177	189	505	3
Pakistan	154	184	186	14
Afghanistan	126	172	259	4
India	104	55	69	16
Thailand	33	34	46	0
Colombia	27	43	53	7
Philippines	26	40	59	3
Mexico	25	125	6	0
Yemen	22	15	67	12
Turkey	19	46	70	0
Somalia	18	110	63	2
Syria	14	45	32	1
Russia	11	6	4	0
Nepal	9	3	2	1
Nigeria	8	59	21	0
Kenya	6	1	16	5
UK	6	0	0	0
Algeria	5	1	8	3
Peru	3	19	22	0
Indonesia	3	9	5	0
Israel	3	0	0	0
Sudan	2	6	13	0
Germany	2	0	0	0
Kazakhstan	2	0	0	0
Congo	1	10	0	0
Honduras	1	6	4	0
Burundi	1	4	0	0
Kosovo	1	1	1	0
Iran	1	1	0	0
Denmark	1	0	0	0
Bulgaria	1	0	0	0
Kyrgyzstan	1	0	0	0
Japan	1	0	0	0
Total	**814**	**1,185**	**1,511**	**71**

Table 1- Attacks in October 2011 throughout the World

There were **814** reported terrorist incidents in **33** different countries in October 2011, versus **920** in the preceding month. These incidents claimed **1,1851** lives, caused **1,511** injuries and included **71** abductions. The incidents decreased roughly 12% in the world compared to previous month. Incidents in Iraq, Afghanistan and Pakistan consist of 56% of all total incidents in the world. Iraq was in the first place by the total number of casualties in the world in October 2011.

[1] All figures mentioned in the report come from

CBRNE Terrorism Newsletter – Winter 2011

publicly available sources, and any discrepancy in figures cited in similar works is the result of varying consultation of these sources. Neither NATO nor COE-DAT is responsible for such discrepancies.

Attack type	Number of Instances	K	W	A
IED	252	215	602	0
Armed Attack	215	354	236	0
Clash	115	190	224	0
IDF	64	46	173	0
Execution	48	141	0	0
VBIED	35	39	125	0
Abduction	25	0	0	59
Suicide Attack	22	137	131	0
Raid	20	62	20	12
Arson	14	0	0	0
Cyber Attack	3	0	0	0
Hoax	1	0	0	0
Total	814	1,185	1,511	71

Table 2- Types of Terrorist Attacks in October 2011

The attack types in the world in October are shown above in the table. Improvised explosive device (IED) attacks, armed attacks and clashes consist of 71% of the total attacks in the world in October. According to attack types, IED attack was the most prevalent methodology during the month. **"The deadliest attack was a suicide attack in Mogadishu in Somalia on October 4 and claimed 70 lives and 20 injuries. The incident happened when a suicide attacker blew himself off near a government compound in the capital."**

MAP OF TERRORIST INCIDENTS OF THE MOST HIT 10 COUNTRIES IN THE WORLD DURING OCTOBER 2011[2]

Pakistan : 154 attacks
Colombia : 27 attacks
Iraq : 177 attacks
Turkey : 19 attacks
Yemen : 22 attacks
Afghanistan : 126 attacks
Philippines : 26 attacks
Mexico : 25 attacks
Thailand : 33 attacks
India : 104 attacks

[2] This map shown here is taken from www.presentationmagazine.com
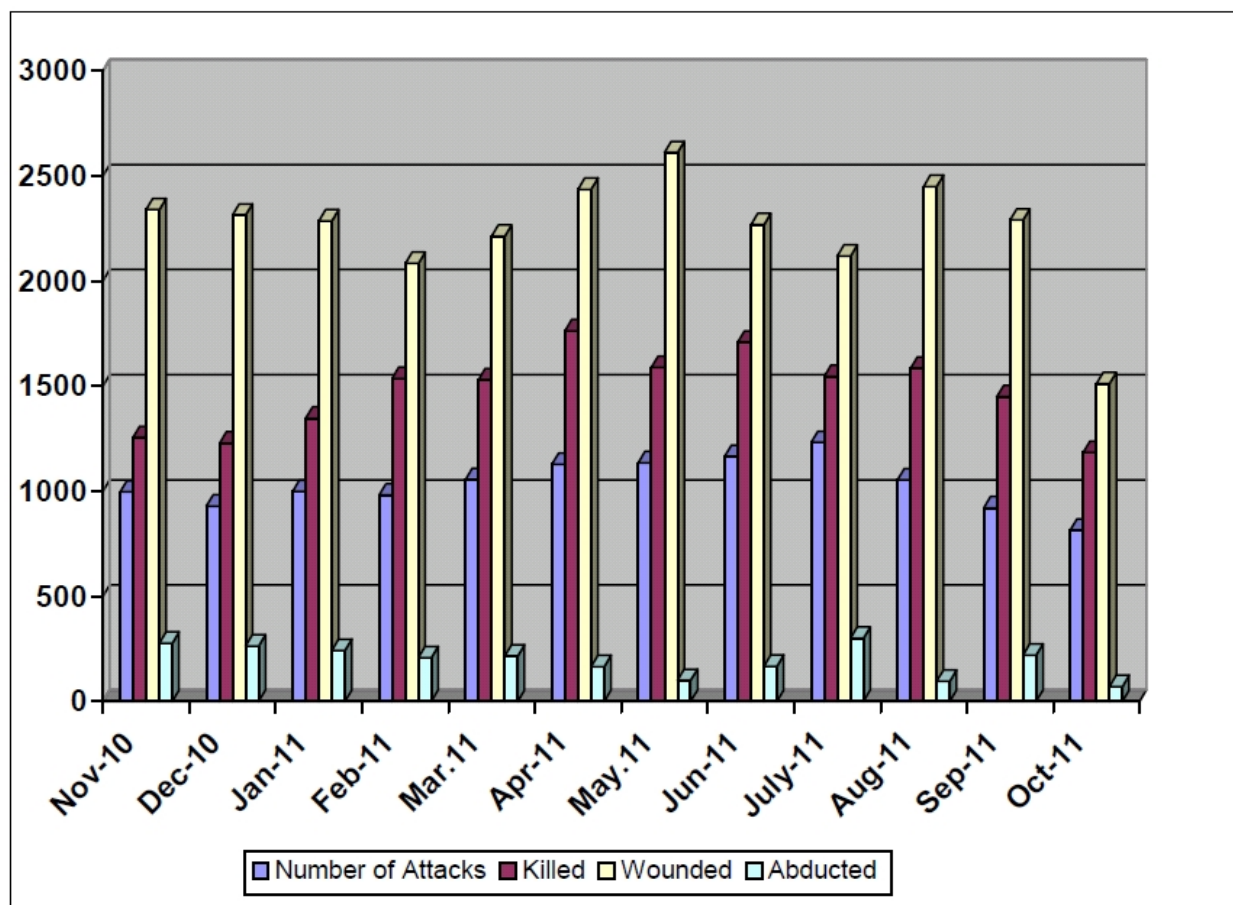
Chart 1 – Some World Security Trends

The Mystery of Invisible Terrorists

By Victor Grossman

Source: http://mrzine.monthlyreview.org/2011/grossman191111.html

"Ten murders traced to neo-Nazi terrorists!" More and more ugly facts splashed through the German media, with echoes around the world. Politicians from the "respectable" parties expressed shock and surprise. In 2007 a German policewoman had been shot to death and her colleague badly wounded. The murder weapon was now found in a partly burned-out building in the East German town of Zwickau. Nearby lay the corpses of two men, probably suicides, both guilty of a recent bank robbery and mostly likely of killing the policewoman. Nine retail merchants, eight of Turkish, one of Greek,

background had also been murdered as far back as 2000, often with the same weapon.

The two men and a woman accomplice who has since given herself up to police belonged to a "National Socialist Underground" with a brutal Nazi program. Why did it take years to find the culprits? Another group member, arrested on November 12th in Hanover, was arrested in 2006 for mailing phony explosives -- and then freed. Why was there no checkup on him? Was the group responsible for 14 bank robberies all over Germany, at least as far back as

1998, for a bombing in Cologne in 2004 which wounded 22 people in an immigrant neighborhood, and perhaps for other acts of violence, sometimes fatal, against people with immigrant origins? While the list of mysteries grew, one question kept recurring: what took the police so long?

Some answers are breaking through the fog. It is no secret that the Nazi movement, both its legal component, the National Democratic Party (NPD), and its illegal thug element are riddled with secret agents of the "Constitution Protection Agency" ("Verfassungsschütz"), the German FBI. Their number and because they themselves often wrote Nazi propaganda, even holding leadership positions, had stymied an attempt to outlaw the NPD in 2003. The court found that the indictment was partly based on texts written by the agents and stated that: "A governmental presence at the leadership level of a party renders its influence on decisions and activities inevitable." So it threw the case out. The winner was the NPD.

Those agents are still in there, preventing new attempts to ban the organization, at least without risk of exposing, or having to withdraw, the agents. The government would not know what the Nazis planned if they were removed, it was asserted, while a second mishap in the courts would give the Nazis a big new propaganda advantage. Remaining legal not only guarantees the NPD large sums of badly-needed government money for election purposes and gives it the chance to elect legislators (now in two states and three Berlin boroughs), but gives it police protection for weekly, threateningly reminiscent anti-foreigner marches all around Germany, which feature fearsome-looking gangs of thugs they are closely connected with.

But now their murderous menace has dramatically come to light. A video film was found, using the jolly "pink panther" film and TV cartoon figure to boast of the crimes already committed and those to come. Once again: Did the Constitution Protectors, especially in Saxony and Thuringia, where these three had been hiding out, know nothing about them?

Now an upsetting new fact has come to light. At the murder of one of the young Turkish merchants in his shop in 2006, an agent of the "Protectors" from the West German state of Hesse was present, holding a heavy object in a paper bag, quite probably a gun. He was found and arrested. But 24 hours later he was freed. Some believe they saw the same man at some of the other murder sites. Who was he, why was he hired -- and paid -- by the forces of law and order in Hesse?

New connections have also come to light between the former chief of the Constitution Protectors in the state of Thuringia, an extremely right-wing historian, and a pro-Nazi who was paid as a secret agent while vice-president of one such fascist group.

Leading politicians, with worried voices and furrowed foreheads, are now demanding a "total investigation"! No stone must be left unturned. Coalition party leaders, always opposed to a ban on the NPD, now, in dramatic tones, call for a reevaluation of the question.

What hypocrisy! What would a true reevaluation reveal? Historical studies, known for decades but recently reinforced, supply countless facts on how former Nazis dominated police, secret police, and intelligence-gathering institutions in the Federal Republic from the start. The police apparatus was built up by and with SS officers and Gestapo men with the bloodiest of hands. At least a thousand ex-Nazi judges and prosecutors dominated the courts, many of them guilty of death sentences against opponents of fascism. The same held true of the military general staff, the diplomatic corps, and the political scene. It has recently been disclosed that until 1966, in Hesse, a quarter to a third of Christian Democratic deputies and 60 to 70 percent of their Free Democratic partners had been in the Nazi Party, some in high positions. In charge of personnel questions nationally was Adenauer buddy Hans Globke, in great measure responsible for the criminalization and easy identification of German Jews.

Worst of all was the espionage apparatus directed against the Soviet bloc. Nazi spy General Reinhard Gehlen, first used by US intelligence after 1945 to build up its secret network, was then switched to the new West German government. A study by historian Martin A. Lee described how "Gehlen proceeded to enlist thousands of Gestapo, Wehrmacht, and SS veterans. Even the vilest of the vile -- the senior bureaucrats who ran the central administrative apparatus of the Holocaust -- were welcome in the 'Gehlen Org,' as it was called, including Alois Brunner, Adolf Eichmann's chief deputy. SS major Emil Augsburg and Gestapo captain Klaus Barbie, otherwise known as the 'Butcher of Lyon,' were among those who did double duty for Gehlen and U.S. intelligence (San Francisco Bay Guardian, May 7, 2001). Lee also quoted the Frankfurter Rundschau: "It seems that in the Gehlen headquarters one SS man paved the way for the next and Himmler's elite were having happy reunion ceremonies."

Nearly all these men have died. But their disciples remained, and so did their inclinations. The Gehlen gang and their friends in top army and government offices used the Cold War to justify their return to strong positions. In the twenty-one years since Germany was unified, the main device has been a constant stress on the "totalitarianism" theory: one nasty dictatorship in Germany was replaced, in the East, by another one, equally bad or, to judge by the amount of propaganda, really far worse. The constant attacks on the system in the GDR and anyone who can be linked with it as being as bad as or worse than Nazis, and similar denunciations of "both right-wing and left-wing terrorism," again stressing the latter, have permitted most politicians and Constitution Protectors to concentrate on attacking those on the left.

This reflects fears that uncertain economic conditions, like a recession or worse, might cause Germans, especially in the East, to reflect that despite the bad features in the old German Democratic Republic, the limits on travel, far fewer high-quality consumer goods, and the other pressures and defects, there were good features

as well, like job security, women's rights, no financial burdens with child care, medical care, or education. Maybe socialism. . .?

Faced by fears of any such reflection (and possible growth of The Left), some leaders felt that Nazis, though not pleasant folk, are good to have around as a preferable, perhaps useful means of channeling dissatisfaction if things get rough. This was the same philosophy which led their grandfathers in politics and the economy to support Hitler.

Is such a stand really possible in today's Germany? Luckily, neither the NPD nor other openly racist (usually anti-Muslim) parties win nearly as many votes as similar parties in many other countries -- most dangerously in Hungary, Austria and possibly even France. And while there is always potential support among racists, nationalists, and economically hopeless groups, wherever Nazis demonstrate there is almost always a rally of anti-fascists to stop and usually to outnumber them. "No Nazis in Our Town" is a simple but common statement. But while there are still many good exceptions, all too frequently it is the city governments or the courts which not only protect the Nazis but harass and often arrest their opponents.

Last February, like every year, the Nazis wanted to misuse for their own purposes ceremonies in Dresden mourning those killed in the air raid of February 1945, largely to counterbalance recollections of the Holocaust. 18,000 anti-fascists gathered to prevent their march and their rally for the second year in a row and, with no violence, sent them home in helpless rage. But after most Nazis and anti-Nazis had left the city, one group of "anti-fascist" youngsters, their faces covered and almost certainly led by provocateurs, as on past occasions, skirmished with the police. This is always meat for the mass media; it has been tried recently against Occupy groups. During the day thousands of cell phones were hacked by the police. At night the skirmish was used to justify a brutal, fully illegal raid on The Left headquarters and to remove the legal immunity as legislators of the

leaders of The Left in Saxony, Dresden's state, and neighboring Thuringia. They are to be brought to court for sponsoring "illegal blockades." Voting against them were the Christian Democrats, Free Democrats, and the neo-Nazi NPD. Once again it was: "When in doubt support the far right."

Until last week the media was full of angry articles about "right-wing terrorism and left-wing terrorism," with Angela Merkel joining the chorus. As ever, it was hinted, both were much the same but the latter were possibly worse, as proved by the burning of luxury cars in Berlin, blamed on "left-wing terrorists." Even when an unemployed, very distressed young man with no political ties was caught in the act, the chorus hardly let up. Now, with increasingly frightening details about genuine right-wing terror, strong indications that government spies were involved, and the mysterious failure of Constitution Protectors to find the culprits in fifteen long years, they may decide to be just a little quieter, at least for a while.

Victor Grossman, American journalist and author, is a resident of East Berlin for many years. He is the author of Crossing the River: A Memoir of the American Left, the Cold War, and Life in East Germany (University of Massachusetts Press, 2003).

Olympic Heli-snipers: Sharpshooters to patrol the skies during London 2012

By Christopher Leake
Source:http://www.dailymail.co.uk/sport/olympics/article-2063920/London-2012-Olympics-Snipers-helicopters-Games.html

The Olympic Games in London will be protected from above by snipers on board military helicopter.

Sources say the military crackshots will fly above the capital in case terrorists attempt an atrocity at the event in Stratford, in the east of the city.

The RAF snipers are understood to have been training recently at the restricted Lydd military live-firing range near the Kent coast to sharpen their skills.

Taking aim: RAF snipers will be deployed in London to target potential threats to the 2012 Olympic Games

One source told The Mail on Sunday that the training had been designed specifically to prepare for an Olympic Games deployment to protect stadium sites in East London and elsewhere.

Flying in Merlin or Lynx helicopters, the snipers are capable of killing an attacker at a range of more than a mile using a Barrett 'Light Fifty' rifle, which fires a powerful .50-calibre half-inch bullet at 2,799 feet per second.

Even at night, the flying snipers can kill an enemy 1,000 yards away using night sights

and infra-red lasers for target-marking as they keep in touch with commanders on the ground using encrypted military radio frequencies.

Death from above: The snipers will hover above Olympic sites in Lynx MK7 helicopters, like this one, which have been used in Iraq and Afghanistan

Their rifles have the power to destroy engine blocks and fire through concrete from long range, making it difficult for a terrorist to take cover.

Bird's eye view: The snipers will be able to kill suspected terrorists from up to a mile away - even at night

© ODA 2008

The airborne sharpshooters were deployed in Iraq, where they were described by the Ministry of Defence as a 'special weapon' against the insurgent threat.

In Iraq, the snipers were on standby around the clock to provide protection from the air and carried out sniping and surveillance duties on the ground.

Now, they could find themselves on operational duty in the UK for the first time, helping to protect

© Alamy

prime venues such as the 80,000-seat Olympic Stadium and the Aquatic Centre.

Airborne threats: Surface-to-air missiles may also be part of the armoury available to Olympics security forces

© PA

Last week, Defence Secretary Philip Hammond revealed in the Commons after a question from his predecessor, Dr Liam Fox, that ground-to-air missiles were part of the armoury that may be used during the Olympics if required.

Mr Hammond's statement was interpreted as an attempt to show how seriously the UK is taking the terror threat after it was revealed that the US is preparing to send 1,000 armed agents, including 500 from the FBI, to protect its competitors.

High security: Left, police officers take part in a search exercise at the Olympic Stadium. Right, Mail cartoonist Pugh imagines the scene at the start of an event

A Ministry of Defence spokesman said last night: 'The MoD has been fully involved in Olympic security planning work and it is anticipated that the Armed Forces, at the request of the civilian authorities, will provide some specialist support including the use of assets where appropriate. However, this will be a police-led operation and any military involvement will be in a supporting role.

PUGH

'Drop the gun, buddy!'

'It is too early to talk about the numbers of personnel who may be involved or further details around precisely what support the MoD might provide – but ongoing planning to meet a range of contingencies is sensible.'

The spokesman added: 'This work is not in response to any specific threat but, as the Defence Secretary said in Parliament, all necessary measures to ensure the security and safety of the London Olympic Games will be taken.'

The banality of suicide terrorism

Radio interview of Prof Nancy Hartevelt Kobrin author of "The Banality of Suicide Terrorism" to Candace Salima for her radio program "Turning the Tide". Candace Salima at the end of the program stated that Nancy's book should be required reading for everyone living in the West.

View the two hours interview (Parts 1-4) at:

http://www.youtube.com/watch?v=M_KiA7nCdWg

Candace Salima commented:

When I sat down to read this book, I was decidedly unsure of what I would be getting into, but since I was interviewing Dr. Kobrin the next day, I wanted to have a full list of questions and comments ready to go.

Dr. Nancy Kobrin is a psychoanalyst with a Ph.D. in romance and semitic languages, specializing in Aljamía and Old Spanish in Arabic script. She is an expert on the Minnesota Somali diaspora and a graduate of the Human Terrain System program at Leavenworth Kansas. And yes, I had my dictionary pulled up and used it often as I read the book, and I'm a well-read, educated woman.

I had quite the visceral reaction to Dr. Kobrin's approach to suicide terrorism. I forced myself to keep reading, as horrifying as I found the entire subject and her theories on the matter, until I finished the book. I made myself take a good hard look at my response to the information, and realized because I am an American, and a westerner to boot, there was simply no way I would ever understand, let alone accept, the motivation behind suicide terrorism.

With that being said, I believe this is a book every single person in the western world should read. Dr. Kobrin looks at the treatment of women in the Arabic world, the treatment of children, boys vs. girls, and how they are brought up within the interpretations of the teachings of Islam. She compares, and quite well, suicide terrorism to domestic violence, and draws the parallels across the board.

As she outlined how children are raised, the self-hatred Arabic women have, because they are devalued and abused from birth, and the children's reaction to this abuse before their very eyes, it is easy to see how the added element of a genetic disposition toward violence, would easily grow to serial killer status and the perfect patsy for jihadists and Al Qaeda. Add, what I already know about *unattachment disorder* and I can easily understand how this is the perfect breeding ground for terrorists and suicide bombers in all forms.
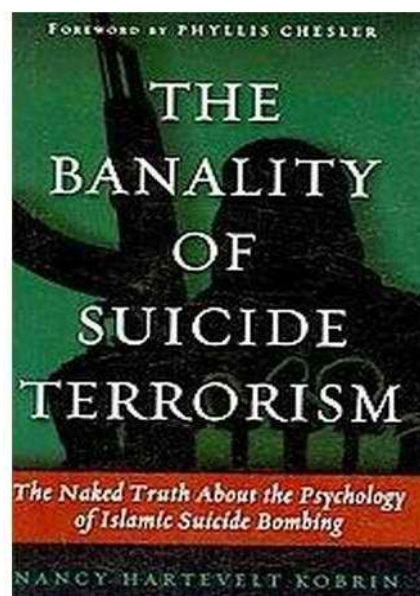
She writes of the "Early Mother" and the mother/child relationship between the terrorist, suicide bomber, and his/her mother. And, this is where I run into a little trouble. But she outlines it well, and explains her hypothesis well. So well, in fact, that the U.S. Army uses this book to help its soldiers understand the psychology of suicide bombers and terrorists.

So although I was highly disturbed by what I read, I'm glad I read it and understand better what goes on in the families and culture which produce this type of individual. With that being said, I have no sympathy for terrorists or suicide bombers, nor will I ever, regardless of their upbringing.

It is stated that 1% of the almost 1.5 billion Muslims worldwide are terrorists. That's 15,000,000 terrorists running around, in case you were wondering. But that leaves the rest of them who DON'T become terrorists. Read *The Banality of Suicide Terrorism* to understand how those 15,000,000 think.

The Banality of Suicide Terrorism could have used the benefit of a top notch editor, and the flow of information better organized, but it is packed with good information and leaves the reader with a greater understanding of what we are facing with suicide bombers and terrorists in the world today.

Israel to assist Kenya in battle against al Shabaab

Source: http://www.jamestown.org

Kenyan reports say Israeli personnel will help secure potential targets in Kenya from terrorist attacks. The Israeli security experts are expected to start work in the next few weeks. According to Israeli ambassador Gil Haskel: "Israel is willing to send consultants to Kenya to help Kenya secure its cities from terrorist threats and share experience with Kenya because the operation in Somalia is very similar to Israel's operations in the past, first in Lebanon and then in Gaza Strip" (*Daily Nation* [Nairobi], November 18). Since the Kenyan operation in Somalia began in mid-October, terrorists have struck the Kenyan cities of Nairobi, Garissa and Mandera. More attacks are feared as the operation progresses; al-Shabaab leaders continue to call for major terrorist attacks within Kenya.

A statement from the office of Kenyan Prime Minister Raila Odinga said that Israel had agreed to help "rid its territory of fundamentalist elements," with Israeli Prime Minister Benjamin Netanyahu asserting that "Kenya's enemies are Israel's enemies." The statement also said that the Israeli prime minister had pledged to help create a "coalition against fundamentalism" in East Africa together with Kenya, Ethiopia, South Sudan and Tanzania (BBC, November 4). The Kenyan prime minister's four-day visit to Jerusalem concluded with the signing of a memorandum of understanding on internal security issues (*Jerusalem Post*, November 15). Various arms deals are expected to follow, with Kenya seeking patrol vehicles and maritime surveillance equipment. The latest meetings follow up on a Kenyan mission to

Jerusalem last year to request Israeli military assistance in countering al-Shabaab threats (Shabelle Media Network, February 14; see also *Terrorism Monitor* Brief, March 11, 2010).

Al-Shabaab is reported to have responded to the initiative by sending agents from mosque to mosque to announce Israel had now joined the Christian Crusaders in destroying Islam in Somalia (*Daily Nation*, November 18). Referring to the terrorist strikes already carried out inside Kenya, al-Shabaab spokesman Ali Mahmud Raage warned Kenya that "things have not begun in earnest yet and it is now a month on. You still have a chance to go back to your border (*Nairobi Star*, November 17). Al-Shabaab spokesmen also insisted the world's Muslims had a responsibility to aid the Somali Islamists now that Israel was joining the struggle against them.

Israel has lately intensified its diplomatic efforts in sub-Saharan Africa. A recent meeting between Netanyahu and South Sudan president Salva Kiir was soon followed by visits from Kenyan Prime Minister Odinga and Ugandan president Yoweri Museveni, who actually bumped into each other in Jerusalem unaware of each other's presence (*Nairobi Star*, November 18). Israel indicated last year that it was prepared to recognize the breakaway territory of Somaliland as an independent nation (Golis News, February 11, 2010). It is believed that Israel has an interest in establishing a military outpost in the Somaliland port of Berbera (Shabelle Media Network, February 14, 2010). However, new

complications in Israeli naval access to the Suez Canal since the Egyptian Revolution may put such plans on hold.

The question now is whether the Israeli-Kenyan agreement will provide the necessary fuel to sustain a successful al-Shabaab recruitment campaign in Somalia at a time it is hard pressed on several fronts and awaiting yet another potential military intervention by Ethiopia. TFG cooperation with the Kenyan offensive will also be easily interpreted by Somalis as cooperation with Israel, a development that would present a major setback for international efforts to restore security in the Horn of Africa region. Discussions regarding Kenya joining the existing African Union Mission in Somalia (AMISOM) could further complicate the local credibility of American-backed African Union efforts to destroy al-Shabaab.

Military a Growing Terrorist Target, Lawmakers Warn

By Catherine Herridge
Source: http://www.foxnews.com/politics/2011/12/06/military-growing-terrorist-target-lawmakers-warn/

There is growing evidence that homegrown terrorists see military personnel and bases as legitimate, high-value targets, lawmakers said ahead of a joint session of the House and Senate Homeland Security Committees on Wednesday,.

"People in uniform are symbols of the United States. They're symbols of America power, symbols of America might," Rep. Peter King of New York, the Republican chairman of the House Homeland Security Committee, told Fox News. "And if they (military personnel) can be killed, then that is a great propaganda victory for Al Qaeda."

King said there is also evidence that extremists have joined the services. "There is a serious threat within the military from people who have enlisted who are radical jihadists," King stated. "The Defense Department is very concerned about them. They feel they're a threat to the military both for what they can do within the military itself and also because of the

weapons skills they acquire while they're in the military."

The chairman of the Senate Homeland Security Committee, Connecticut independent Joe Lieberman, agreed.

"The records show that the United States military has become a direct target of violent Islamist extremism here in the U.S., and that means soldiers and perhaps their families are potentially vulnerable at work and at rest, in a military setting or a civilian one," he told Fox News.

Since the Fort Hood massacre in 2009 that left 13 killed and dozens more wounded, the number of alleged plots targeting the military has grown significantly. In June, two men allegedly plotted to attack a Seattle, Wash., military installation using guns and grenades. In July, Army Pvt. Naser Abdo was accused of planning a second attack on Fort Hood. And in November, New York police arrested Jose Pimentel, who alleged sought to kill service members returning from Iraq and Afghanistan.

Both Pimentel and Abdo allegedly drew inspiration from the American cleric Anwar al-Awlaki and the online jihadist magazine Inspire, which includes a spread on how to "Make a Bomb in the Kitchen of Your Mom."

"The stark reality is that the American service member is increasingly in the terrorists' scope and not just overseas in a traditional war setting," Lieberman said.

The witnesses scheduled to testify before the joint session on Wednesday, include Paul N. Stockton, assistant secretary of defense for homeland defense; Jim Stuteville, U.S. Army senior adviser for counterintelligence operations and liaison to the FBI; Lt. Col. Reid L. Sawyer, director of the Combating Terrorism Center at West Point, and Daris Long, whose son, Army Pvt. William Andrew Long, was shot and killed at an Arkansas military recruitment center in 2009. The shooter, Carlos Bledsoe,

pleaded guilty to the crime earlier this year. In a letter to the court, Bledsoe said he carried out the attack on behalf of Al Qaeda in Yemen -- the group that was behind the last two major plots targeting the U.S. airline industry.

Rep. King said the Web is the driver of the new digital jihad.

"It enables people -- rather than having to travel to Afghanistan to learn about jihad or to be trained, they can do it right over the Internet," he said. "And this is a growing role."

And while al-Awlaki and his colleague Samir Khan, who was behind the magazine Inspire, were killed in a CIA-led operation in September, King warned against overconfidence that Al Qaeda in Yemen was done.

"This is a definite short-term victory for us. There's no doubt they are going to regroup, that there will be others who will be providing Internet data, inspiration to jihadists in this country, instructions on how to make bombs," he said.

While King was heavily criticized, in some quarters, for launching his hearings 10 months ago on homegrown terrorism, the congressman said Wednesday's joint session showed that the threat is legitimate, and recognized as such by other members of Congress.

"To me it's a validation of what I've been trying to do all year," King emphasized. "There's a definite threat from Islamic radicalization in various parts of our society, including within the military, and we can't allow political correctness to keep us from exposing this threat for what it is."

Fox News chief intelligence correspondent Catherine Herridge's bestselling book "The Next Wave: On the Hunt for al Qaeda's American Recruits," published by Crown, draws on her reporting for Fox News into al-Awlaki and his new generation of recruits

A Chronology of Attacks on and Unlawful Interferences with, Offshore Oil and Gas Installations, 1975 – 2010

By Mikhail Kashubsky

Source: http://www.terrorismanalysts.com/pt/index.php/pot/article/view/offshore-gas-and-oil-attacks/html

Abstract

Throughout its history, the oil and gas industry has been a subject of environmental protests, labour disputes, tensions with local communities, and it has also been a target of various violent activities ranging from vandalism to political violence, which have impinged on the security of oil industry workers and interfered with operational activities of oil companies on numerous occasions. Although a considerable number of attacks on oil and gas infrastructure occurred over the course of the industry's existence, most of those attacks were directed against onshore petroleum targets. Compared to onshore petroleum infrastructure, attacks on offshore oil and gas installations are relatively rare. The following chronology provides details of attacks, unlawful interferences, and security incidents involving offshore oil and gas installations that happened between 1975 and 2010.

Introduction

This chronology [1] lists some 60 events. [2] The chronology was compiled from publically available data on past attacks against maritime and petroleum infrastructure collected from various sources including databases, policy documents and reports of national and international government and non-government organisations, scholarly commentaries, journal articles, books, and previous studies done by academics and security analysts, as well as media reports, newspapers, and online news. [3] It should be noted that sometimes different sources report different details of offshore attacks and incidents. In some cases, inconsistent and conflicting facts are reported. Where possible, all reasonable effort has been made to ensure the accuracy of information contained in this chronology.

It is recognised that this chronology probably does not list all incidents that happened during that period and it does not reflect the frequency at which they are happening. Therefore, it does

not necessarily provide a reliable base for quantitative analysis. Nevertheless, some interesting observations can be made.

General Observations

It is apparent that attacks on, and interferences with, offshore petroleum installations have generally increased in recent years. The majority of attacks/interferences have occurred since the beginning of 2004. In particular, 41 of 60 incidents (almost 70 percent) have occurred since 1 January 2004. Prior to the beginning of this chronology, we found only one security incident/attack, namely the 1899 'Montecito Mob' incident which is also listed. However, there must have been more in the intervening 75 years. The majority of security incidents involved violence (whether actual use of violence or threat of violence), but 15 of 60 incidents (25 per cent) were non-violent.

The types of installations that had been victims of attacks/interferences include fixed offshore production platforms, mobile offshore drilling rigs, floating production storage and offloading units (FPSOs), floating storage and offloading units (FSOs), offshore oil export terminals, and other types of offshore installations such as oil derricks, wellhead platforms, and flow stations. In some cases, the type of facilities attacked was not specified, but incidents involving offshore drilling rigs are the most common. [4]
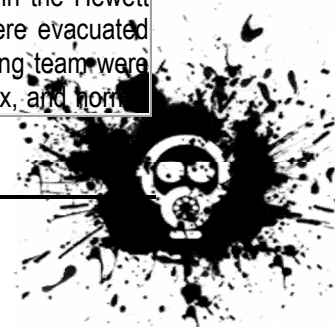
Attacks and security incidents involving offshore oil and gas installations have taken place in practically all regions of the world. [5] The analysis of offshore security incidents by location shows that most of the incidents occurred in economically and politically unstable countries [6] and some occurred in stable countries, but the incidents listed in this chronology are limited to the following countries: the United States, the United Kingdom, Angola, Iran, United Arab Emirates, Nigeria, Guyana/Suriname, Iraq, Yemen, Indonesia/Malaysia (Malacca Strait), India, Malaysia, Denmark (Greenland), Cameroon, and Mexico. The majority of offshore incidents (more than 60 percent) took place in Nigeria.

The attacks/interferences have been committed by various types of adversaries including terrorists, insurgents, pirates, hostile nation States, environmental activists, anti-oil activists and other protesters, and sometimes unknown perpetrators. The analysis indicates that insurgent groups are responsible for at least one-third of all incidents. [7] There are five bomb threats and threats of attack (rather than the actual attacks) among the incidents recorded in this chronology. Other incident scenarios include abduction of workers, armed intrusion, hostage-taking, bombing and use of explosives, military strikes, and unauthorised boarding. The most common scenario is armed intrusion and abduction of offshore workers. [8]

In at least 13 of 60 incidents there was some kind of damage caused to platforms and 8 of 60 attacks resulted in human casualties. Almost all incidents caused interruption or shutdown of platform operations. The means of transport that assailants use to reach offshore platforms is often not reported, but in most cases perpetrators used motorboats. In some cases, small fishing vessels and vessels that look similar to offshore supply vessels were used.
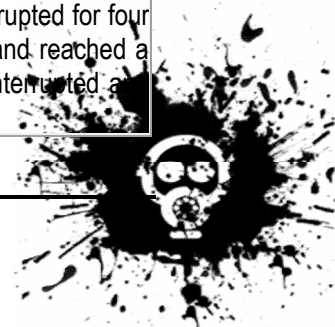
Date	Location	Details of Attack/Incident
2 Aug 1899	USA	When an oil company began to construct an oil derrick off the shores of Montecito, a highly affluent suburb of Santa Barbara in the State of California, a local mob took direct action. They attacked the rig and demolished it. [9] The next day these activists were described approvingly on the front page of the local newspaperas 'a party of the best known society men of Santa Barbara armed to meet any resistance'. [10] The local 'society men' responsible for the attack did not suffer any noteworthy legal repercussions for their actions, despite having been so well known. [11] The incident had become known as 'Montecito Mob'.
25 Aug 1975	UK	Philips Petroleum Company in Yarmouth, England, received three anonymous telephone calls with callers announcing that underwater charges with delayed-action fuses had been attached to the legs of offshore production platforms in the Hewett field, some 20 miles to the east off Norfolk coast. Three platforms were evacuated immediately. [12] A Royal Navy vessel, helicopters, and an expert diving team were dispatched. Two days later, it was concluded that the threat was a hoax, and non

		production operations were resumed. The incident cost to the British taxpayers about USD $500,000. [13]
16 May 1977	Angola	An African guerrilla movement, the Cabinda Enclave Liberation Front (CELF), said that it plans to blow up the offshore drilling complex of the Gulf Oil Company (GOC) in the Cabinda enclave of Angola and warned the company to evacuate its 200 British and American employees within three days. A spokesman for the guerrilla group said the warning must be taken seriously because the movement had acquired ground-to-ground missiles in exchange for coffee and uncut diamonds. [14] The guerrilla spokesman said the guerrillas were opposed to GOC because it was giving the ruling pro-Marxist Angolan Popular Liberation Movement $2 million a day in oil royalties. [15]
25 Jul 1981	USA	Greenpeace activists attempted to board an oil rig operated by Shell 177 miles off the coast of Cape Cod, Massachusetts, to express their opposition to drilling during a Shell news conference on the rig. Shell denied the group access to the drilling rig. Greenpeace officials sought to explain their fear that the drilling (which had been delayed for six years) would result in oil spills endangering the nearby Georges Bank, home for much of the world's supply of cod, haddock and food fish. [16] Shell denied the group access to the drilling rig and Shell spokesman said Georges Bank is a relatively low-risk geological formation for oil spills.
Oct 1981	USA	An anonymous caller said that a bomb had been placed on one of several attending vessels at *Habitat* Texaco platform located 9 miles offshore, southeast of Santa Barbara, California. No bomb was found after platform and vessel searches. [17]
Mar 1983	Iran	Iraqi planes attacked the Iranian offshore platform at the Nowruz oil field; the damaged platform collapsed, and the oil slick caught fire. [18] The platform burned and spilled oil at an initial rate of approximately 5,000 barrels per day (bpd). The rate slowed to about 1,500 bpd in the two years before the well was capped in May 1985. Overall, approximately 1.9 million barrels of oil spilled into the sea as a result of this incident. [19]
19 Oct 1987	Iran	The US Navy attacked Iranian *R-7* and *R-4* oil platforms in *Reshadat* (also known as *Rostam*)offshore complex blaming Iran for a missile strike on the US-flagged Kuwaiti oil tanker *Sea Isle City* near Kuwait Harbour three days earlier. [20] The Navy destroyers opened fire on *R-7* platform and subsequently detonated explosives on it, completely destroying it; and *R-4* platform was attacked in a similar fashion and severely damaged. [21] As a result of the attack, one platform was almost completely destroyed and another was severely damaged and, according to Iran, production from the *Reshadat* and *Resalat* offshore complexes was interrupted for several years. [22] The attacks caused damage to the nearby *Resalat* offshore complex, connected by underwater pipelines to *Reshadat*. [23]
Apr 1988	UAE	In response to the US attack on the Iranian *Joshan* missile boat, Iranian patrol boats attacked the neighbouring United Arab Emirates's Mubarak oil field. The Iranian boats sprayed several ships and a mobile drilling rig with machine-gun fire and grenades but caused no casualties. [24]
18 Apr 1988	Iran	The US military attacked and destroyed Iranian offshore oil complexes, *Salman* (aka *Sassan*) and *Nasr* (aka *Sirri*), shortly after the US frigate, *Samuel B Roberts* was damaged by a mine, allegedly belonging to Iran, in international waters near Bahrain. [25] According to Iran, the attacks caused severe damage to the production facilities of the platforms and the activities of the *Salman* complex were totally interrupted for four years, its regular production being resumed only in September 1992, and reached a normal level in 1993; and activities in the whole *Nasr* complex were interrupted and did not resume until nearly four years later. [26]

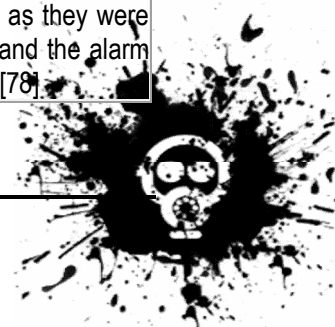|		
30 Apr 1995	UK	Greenpeace activists occupied *Brent Spar* facility in the North Sea for more than three weeks thereby interfering with Shell's decommissioning operations. [27] Shell subsequently obtained legal permission to evict the protesters from the platform and the protesters were removed from *Brent Spar* on 23 June 1995. [28]
13 Dec 1997	Nigeria	Employees and villagers kidnapped one US citizen, one Australian, and two British oil workers, and at least nine Nigerian staff members of Western Geophysical, a US-owned oil exploration company off the coast of Nigeria. The victims were released in stages on 17 and 18 December 1997. [29]
25 May 1998	Nigeria	Over 100 unarmed and peaceful Ilaje protestors went to the Chevron's Parabe oil production platform about nine miles offshore. Nigerian Navy and Mobile Police stationed at the platform, who were armed, allowed the protestors aboard. [30] The protestors occupied the platform to protest environmental and distribution issues, and to demand monetary compensation for environmental and economic grievances and jobs. [31] After two days of negotiations, Chevron used its contracted helicopters to fly Nigerian security forces to the platform. Security forces opened fire at the protesters which resulted in the death of two protesters and several others were wounded. [32]
27 Jun 1999	Nigeria	Armed youth militants (local anti-oil industry activists) stormed a Shell oil platform in Port Harcourt, Nigeria. The attackers caused damage to the platform and kidnapped three foreign platform workers, including an Australian. [33] The attackers then hijacked a helicopter and forced the hostages to fly them to a village near Warri. [34] The hostages were released unharmed on or about 16 July 1999 for an undisclosed ransom. A group calling itself *Enough is Enough* in the Niger River (EENR) claimed responsibility. [35]
20 Jul 1999	Nigeria	Armed men stormed a Royal Dutch Shell operated oil rig in Osoko and held seven British nationals and 57 Nigerians hostage. On 22 July 1999, the youths released the hostages unharmed. [36]
10 Aug 1999	Nigeria	Three British nationals were kidnapped by armed youths from a US operated oil platform in the Niger Delta region. [37] No one was injured, and no one claimed responsibility. On 11 August the youths released the hostages unharmed. [38]
3 Jun 2000	Guyana/ Suriname	The gunboats of the Suriname Navy approached an American owned and operated offshore oil drilling rig, *CE Thornton*, retained by the Canadian corporation CGX Energy. [39] The Canadian company had received a license from the Guyanese government to conduct exploratory drilling in a disputed area of the continental shelf claimed by both Guyana and Suriname. [40] The Surinamese Navy advised that the rig was in Surinamese waters and ordered it to stop unauthorised drilling immediately and clear the area within 12 hours. Fearing that the Surinamese Navy would use force against it, the oil rig decided to follow the orders to withdraw. [41]
31 Jul 2000	Nigeria	About thirty-five armed young men from a village in Bayela State used a rowboat to reach two oil platforms off the coast. They boarded the rig and took 165 oil workers hostage, including 20 foreigners. They demanded that Shell employ more Nigerian nationals and that it pay a fee to the local community for exploiting its petroleum resources. Shell made a deal with the hostage-takers and the employees were released four days later. [42]
23 Aug 2001	Nigeria	The local community group of anti-oil activists boarded a Shell's production platform and the nearby *Trident VIII* jack-up drilling rig. The rig's crew was safely evacuated to Port Harcourt and the activists had withdrawn. [43]

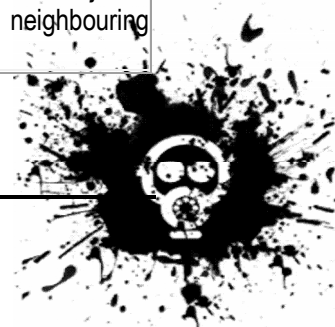| Apr 2003	Nigeria	About 100 oil workers were held hostage aboard offshore installations off the coast of Nigeria by striking Nigerian workers complaining about redundancies and unfair dismissal of Nigerian employees. The hostages included over twenty Americans and over thirty British nationals. [44]
24 Apr 2004	Iraq	Terrorists carried out a suicide boat attack on offshore Al-Basra Oil Terminal (ABOT) in the Persian Gulf. [45] Two zodiac type speedboats piloted by suicide bombers approached the terminal at high speed. The lead boat aimed at the platform and was fired upon, after which it detonated before it could hit the platform. The second boat was also fired upon, killing attackers but the boat still rammed *MV Takasuza* oil tanker, yet it failed to detonate/explode. [46] The Al-Basra terminal, capable of exporting up to 900,000 bpd, was shut down for two days, which (combined with a closure of KAAOT) cost nearly $28 million in lost revenues due to oil not being exported during that time. [47] This consequently led to the spike in oil prices on the world markets which resulted in a further loss of approximately US$6 billion to the global economy. [48] The attack was allegedly carried out by Zarqawi network based in Iraq. In addition, the initial security zone of 2 nautical miles around ABOT was supplemented with a 3000 metre warning zone and a 2000 metre exclusion zone. [49]
24 Apr 2004	Iraq	Terrorists carried out a suicide boat attack against offshore Khawr Al-Amaya Oil Terminal (KAAOT) in the Persian Gulf using a dhow. [50] The dhow was intercepted by a coalition forces vessel as it approached the exclusion zone around the platform. Soon after it was boarded by Navy personnel, the boat exploded. Two US Navy sailors and one member of the US Coastguard were killed in the attack, and four others were injured. [51] No damage was reported, but the terminal was immediately shut down by the authorities. [52] KAAOT, which exports about 700,000 bpd, reopened the next day following the attacks. [53] The attack was allegedly carried out by Zarqawi network based in Iraq. The initial security zone of 2 nautical miles around KAAOT was supplemented with a 3000 metre warning zone and a 2000 metre exclusion zone. [54]
Sep 2004	Yemen	Yemeni insurgents abducted several Western nationals based on offshore oil facilities off the coast of the Red Sea. After several hours, the workers were released. Yemeni authorities have increased security at all sea ports and oil terminals in response to the attacks and information 'about the intention of a foreign terrorist group to carry out sabotage acts on vital oil facilities on Yemeni shores'. The security effort included the deployment of helicopters around two oil terminals on the Arabian Sea and the Red Sea. [55]
3 Nov 2004	Malacca Strait	In the Malacca Strait, outside Malaysia's and Indonesia's territorial seas, several lookalike fishing boats followed a tug towing the oil rig *Ocean Sovereign*, while underway. [56] The duty officer alerted Master who came to the bridge and observed a boat heading for tug. Crew mustered and as the pirates came within 250 metres of tug, they started shooting, causing extensive damage to navigation equipment, bridge windows and the superstructure. Crew switched on lights, activated fire hoses and fired rocket flares but the pirates continued to shoot with automatic weapons. When they were within 50 metres, the crew took evasive manoeuvres and the pirate boat moved away. The crew suffered no physical injuries but was shaken after the incident. [57]
12 Jun 2005	Nigeria	A group of armed men boarded FPSO *Jamestown* in Warri Region and took hostage all 45 crew members. After lengthy negotiations, the gunmen released all hostages unharmed three days later. [58]

22 Sep 2005	Nigeria	More than 100 armed militants stormed a Chevron-operated *Idama* oil production platform in the southern Niger Delta in response to the arrest of an ethnic militia leader on treason charges and forced it to shut down operations. [59] Armed with assault rifles, militants attacked the platform using about eight boats, each carrying 15 gunmen, and occupied the *Idama* flow station. Six government security forces had their weapons taken from them. Production of 8,000 bpd shut down. [60]
10 Jan 2006 / 11 Jan 2006 [61]	Nigeria	Movement for the Emancipation of Niger Delta (MEND) rebels attacked Shell's *EA* offshore oil platform located about 15 km offshore and kidnapped four foreign oil workers from a support vessel anchored at the platform. [62] The company shut down 115,000 bpd *EA* platform. MEND demanded the immediate and unconditional release of Dokubo-Asari and Governor D.S.P. Alamieyeseigha. [63] Insurgents also blew up crude oil pipelines, cutting supplies to *Forcados* offshore export terminal by 100,000 bpd. [64] Some sources claim that *EA* platform was not attacked, but a support vessel in the vicinity of the platform was attacked. [65] Hostages were released on or about 30 January 2006.
15 Jan 2006	Nigeria	MEND insurgents, travelling in speedboats, attacked Shell's *Benisede* flow station. They burned down staff accommodation and damaged the processing facilities, [66] killing at least 16 people in the process, including fourteen soldiers and two civilians. [67] Shell's operations were reduced by about 106,000 bpd as a result of the attack and the company was forced to consider evacuating. [68]
18 Feb 2006	Nigeria	MEND insurgents in speedboats bombed the *Forcados* offshore oil loading terminal and abducted nine workers from the nearby offshore barge at the Escravos coast, [69] and they also damaged oil platform equipment. [70] Six workers were released on 1 March and the remaining three on 27 March. [71]
2 Jun 2006	Nigeria	About 30 armed militants boarded a semi-submersible rig, the *Bulford Dolphin,* about 65 km offshore and abducted eight offshore workers. [72] Hostages were released a couple of days later. [73] About 20 non-essential personnel were evacuated to shore and the rest of the rig crew was safe, but operations were temporarily halted. The attack also contributed to the rise of oil prices by about $1 to $71.50 per barrel. [74]
22 Aug 2006	Iran	Iranian Navy attacked and seized control of *Orizont* offshore drilling rig, owned by the Romanian oil company Grup Servicii Petroliere (GSP), in the Salman field. There were 26 Romanian offshore workers on board the platform at the time of the incident. Iranian troops had seized and occupied the rig after firing on it with machine guns from a ship. The rig was operated under a deal signed between Petrom, GSP and Dubai-based Oriental Oil Co, and the shooting reportedly happened as the rig was being taken outside Iranian waters for a mandatory overhaul. Iranian armed forces kept the crew on the rig's heliport for several hours without food and water, but later they allowed the crew to return to their quarters after cutting off all communications between the workers and the company. The incident arose due to a commercial dispute. [75]
22 Nov 2006	Nigeria	FPSO *Mystras* was attacked by armed men while anchored off Port Harcourt. Ten gunmen boarded the facility and kidnapped seven workers. Their boat was intercepted by the authorities and engaged in a shoot-out during which one worker was killed, one injured, and five others were rescued. [76]
22 Mar 2007	India	Mobile offshore drilling unit *Aban VII* (jack-up rig) was attacked by pirates in speedboats near the south west coast of India, outside India's territorial sea. [77] The rig was boarded by three pirates while under tow. Pirates were noticed as they were preparing to transfer some equipment from the rig to their speedboats and the alarm was raised. Pirates jumped overboard and escaped in their speedboats. [78]

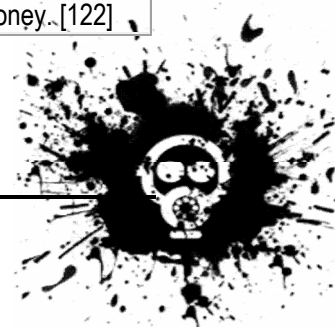| 31 Mar 2007 / 1 Apr 2007 [79]	Nigeria	*Bulford Dolphin* mobile offshore drilling rig was attacked again by gunmen about 65 km off the coast of Nigeria. One British expatriate worker was abducted and taken ashore from the platform. The attackers, believed to be pirates, boarded the rig via an offshore support vessel, which was secured alongside the platform at the time of the incident. [80] Hostage was released on 4 April 2007. [81]
19 Apr 2007	Nigeria	An offshore security vessel that was supporting *Trident VIII* drilling rig, was attacked and three Nigerian sailors were abducted and another six were injured. The gunmen also seized weapons and equipment. *Trident VIII* rig was later shut down as a result of this incident and the staff of *Don Walker* oil rig, which was within a 10 minute boat ride from the incident, had requested security reinforcements from the nearest naval base. [82]
1 May 2007	Nigeria	Chevron's *Oloibiri* floating storage and offloading (FSO) unit was reportedly attacked by MEND at offshore Pennington field off southern Bayelsa state. One Nigerian sailor was killed during the attack and six other foreign oil workers were abducted, but later released on 2 June 2007. [83] The FSO was moored near *Funiwa* platform. The production at the 15,000 bpd Funiwa field and other fields supported by this vessel was shut down to avoid any additional security or safety incidents. [84]
3 May 2007	Nigeria	FPSO *Mystras* was attacked by gunmen believed to be pirates they boarded via the anchor chain. The intruders kidnapped eight foreign workers, including an Australian, from FPSO and an offshore support vessel. The workers were released the following day. [85] FPSO was moored about 55 km off Port Harcourt (however, some sources report that it was 55 miles offshore). Force majeure was declared at a field capable of producing 50,000 bpd, and the production was shut down for several days. [86] Some sources report that this attack was carried out by MEND, not pirates; and that six foreign workers were kidnapped, not eight. [87]
5 May 2007	Nigeria	*Trident VIII* offshore drilling rig was attacked and boarded by gunmen, believed to be pirates, near Brass oil export terminal. One crew member was kidnapped. [88] The attack triggered a security lockdown of the Brass crude oil export terminal. [89]
22 Jun 2007	Nigeria	In the early hours three gunmen armed with AK-47s boarded the 159,000-dwt *Cape Brindisi* moored at Pennington Oil Terminal (also known as FSO *Oloibiri*) and proceeded to shoot up the vessel. No injuries to the crew were reported as they succeeded in going into lock-down mode, after which the gunmen left the ship. The militants reportedly took control of the FSO *Oloibiri*, where the *Cape Brindisi* had been loading. [90]
20 Oct 2007	Nigeria	Seven workers were kidnapped at the EA field (possibly from FPSO *Sea Eagle*) about 15 km off the coast of Bayelsa state by gunmen in speedboats including four Nigerians, a Russian, a British, and a Croatian. All workers were released two days later. [91]
26 Oct 2007	Nigeria	Gunmen in speedboats attacked FPSO *Mystras* about 85 km offshore at an oil production facility operated by Saipem, taking hostage six oil workers. MEND had claimed responsibility for the attack. [92]
10 Feb 2008	UK	*Safe Scandinavia* oil rig in the North Sea issued a security alert which resulted in one of the biggest evacuations in the history of the North Sea offshore industry. It was reported that a catering worker on the rig screamed 'Bomb!' in her sleep and apparently was 'convinced that her nightmare was about to come true'. The authorities sent helicopters to evacuate more than 500 workers, but it turned out that it was just a dream. [93] The company reported that 161 workers evacuated to the neighbouring *Alba* and *Armada* platforms before the operation was called off. [94]

10 Jun 2008	Nigeria	In the early morning, near Port Harcourt, Rivers, Nigeria, armed assailants in speedboats fired upon an oil facility, killing nine naval officers and wounding four civilians. No group claimed responsibility. [95]
19 Jun 2008	Nigeria	Royal Dutch Shell's *Bonga* floating production storage and offloading vessel (FPSO) was attacked by armed militants about 120 km offshore. It was reported that at about 1:00 am around two dozen armed men in speedboats stormed the floating facility and after failing to get access inside they started shooting at FPSO and those on board. Some people were wounded, but no lives were lost. The attack lasted for almost four hours, during which the militants also encountered and hijacked an offshore support vessel and kidnapped its US captain, but released him later that day. [96] The responsibility for the attack was claimed by MEND, the most high-profile militant group in the region. The facility was damaged in the attack, which forced the company to shut down the entire production at its main offshore oil field in Nigeria, interrupting production of approximately 200,000 bpd and 150 million standard cubic feet of gas. [97]
16 Sep 2008	Nigeria	Shooting was reported near Chevron-operated *Idama* offshore production platform, causing Chevron to evacuate offshore workers as a precaution. [98]
26 Dec 2008	Malaysia	Six armed robbers boarded the mobile offshore drilling rig *Allied Centurion* in Malaysia's territorial sea and stole stores and property from the facility. One crew member suffered head injuries, but remained in stable condition. Authorities were informed and later boarded for investigation. [99]
21 Jun 2009	Nigeria	In Rivers state assailants detonated explosives damaging two oil pipelines at Adamakiri and in Kula respectively as well as an offshore facility at the Afremo oil fields operated by Shell, but causing no fatalities or injuries. MEND claimed responsibility. [100]
25 Jun 2009	Nigeria	MEND militants rejected the government's amnesty offer, arguing it did not address the fundamentals of the crisis in the region. MEND claims to have blown up the second remaining well head platform *Jacket B* of the Shell Afremo offshore oil fields in Delta state. [101]
26 Jun 2009	Nigeria	MEND claims that at least 20 soldiers were killed in one of its attacks on Shell's *Forcados* offshore terminal in Delta state. Chevron evacuated hundreds of workers from the Niger Delta after the attacks. [102] At least six high-profile attacks by MEND on oil well heads, offshore platforms, major pipelines and oil pumping stations were reported. [103]
29 Jun 2009	Nigeria	MEND attacked Shell's *Forcados* offshore terminal facility in Delta state using explosives. [104] Cluster 11 and 30 caught on fire after a massive explosion. A confrontation with a military gunboat patrol that stumbled upon heavily armed fighters resulted in the sinking of the gunboat with about 20-25 soldiers on board. [105]
5 Jul 2009	Nigeria	MEND attacked Shell's *Well Head 20* platform located at Cawthorn Channel 1. The facility connects to the Bonny loading terminal in Rivers state. On the same day MEND militants attacked and blew up the strategic Okan manifold which controled about 80 per cent of Chevron Nigeria Limited offshore crude oil to its BOP Crude Loading Platform in Delta state. [106]
12 Jul 2009	Nigeria	MEND conducted a raid on an oil offloading facility in Lagos. This was the group's first attack outside Niger Delta in several months. Five people were killed in the attack. [107]

5 Jan 2010	Nigeria	A group of pirates attacked FSO *Westaf*, off Lagos, Nigeria. Seven crew members were taken to hospital due to the attack including the master who was wounded in the stomach. The attackers stole cash, crew belongings and expensive ship equipment. [108]
31 Aug 2010	Greenland	Greenpeace activists 'boarded' the drilling rig *Stena Don* operating in Arctic waters offshore Greenland and were suspended 15 meters above the water in tents to protest against drilling operations. The activists had to outrun Danish Navy commandos before climbing up the inside of the rig and hanging from it in tents suspended from ropes. They remained on their position for two days forcing the company to suspend drilling. [109] The drillship *Stena Forth*, which is located about 20 miles away, also had to be shut down during the *Stena Don* occupation. [110]
21 Sep 2010	UK	In the waters off the Shetland Islands in the UK, Greenpeace activists climbed the anchor chain of Chevron-operated drill ship *Stena Carron* and were hanging suspended from the chain in a capsule-tent several days, effectively delaying the company's drilling operations in the Atlantic Frontier. [111]
22 Sep 2010	Nigeria	Armed men (believed to be pirates) attacked and attempted to take control of an offshore oil rig at an oil field operated by Addax Petroleum. [112] The assailants became locked in a sustained gunfire with Nigerian Navy patrol boat after it intervened; later it kidnapped three French employees from an offshore supply vessel while retreating. [113] A Thai employee may also have been taken hostage during the attack. The pirates nearly reached the platform by using a vessel which looked like the ships that routinely provide supplies to offshore rig workers. [114]
7 Nov 2010	Nigeria	A group of MEND insurgents attacked the *High Island VII* offshore drilling jack-up rig at the Okoro offshore field located about 12 km offshore and kidnapped 19 crew members including 12 Nigerians, two Americans, two Frenchmen, two Indonesians and one Canadian. Hostages were freed ten days later. [115]
8 Nov 2010	Nigeria	Gunmen attacked an offshore rig operated by Afren PLC, which was engaged in exploratory/survey work at the Okoro oil field about 11 km off the coast of Nigeria. Seven foreigner workers were kidnapped from an oil rig and the company reported that two workers were wounded in the attack and have been flown out by helicopter to receive medical treatment.' [116]
15 Nov 2010	Nigeria	Armed men boarded ExxonMobil's *Oso* offshore platform on the Nigeria's southeast coast and abducted eight offshore workers. At the time of the attack there were 74 people aboard the platform. The company suspended 75,000 bpd production from the facility. [117] The gunmen allegedly came in five speedboats; they beat up some crew members and cut electricity to the offshore facility. [118] A previously unknown group, which identified itself as the Niger Delta Liberation Force (NDLF), claimed responsibility for the attack and threatened to target oil installations in fresh attacks. [119]
17 Nov 2010	Cameroon	The Africa Marine Commando (AMC) rebel group carried out a deadly assault on an offshore oil platform at the offshore Moudi oil terminal (consisting of production platform, FSO *Moudi* and a single buoy mooring) located in the Gulf of Guinea about 50 km off Cameroon's disputed Bakassi peninsula. [120] Six people were killed in the attack, including three members of Cameroon's Rapid Intervention Battalion (a national defence force) involved in the security of offshore oil and gas installations, two Cameroonian civilians and one of the attackers. [121] Cameroonian security service said that the group had threatened further attacks unless they receive money. [122]

22 Nov 2010	Mexico	Four Greenpeace activists took protesting action by climbing 39 metres over the water at the deepwater oil rig *Centenario*, off the coast of the State of Veracruz, in Mexico. The activists boarded the rig and put up a large banner stating 'Go Beyond Oil' to call for an end to deepwater drilling. [123]

Notes

[1] Attacks on offshore underwater pipelines and oil tankers are not included.

[2] It is arguably the most comprehensive chronology of attacks on offshore petroleum installations that has ever been produced and published.

[3] The sources include the International Maritime Bureau (IMB) *Piracy and Armed Robbery Against Ships* annual and quarterly reports; International Maritime Organisation Maritime Safety Committee (IMO MSC) circulars titled *Reports on Acts of Piracy and Armed Robbery Against Ships*; reports such as *Country Reports on Terrorism* and *Patterns of Global Terrorism* which are produced annually by the US Department of State; *Worldwide Threat to Shipping Reports* produced by the US Office of Naval Intelligence; *Anti-Shipping Activity Messages* published by the Federation of American Scientists; *A Chronology of Terrorist Attacks and Other Criminal Actions Against Maritime Targets* published by RAND Corporation in 1983; reports based on the National Memorial Institute for the Prevention of Terrorism (MIPT) database; *NCTC Reports on Terrorism* published by the US National Counterterrorism Center; the Worldwide Incidents Tracking System (WITS) database maintained by the US National Counterterrorism Center; the Global Terrorism Database (GTD) maintained by the National Consortium for the Study of Terrorism and Responses to Terrorism, as well as several studies undertaken by academics and security analysts such as a 2005 study of the Institute for Information Infrastructure Protection (IIIP) titled *Trends for Oil and Gas Terrorist Attacks* and a study by Brynjar Lia and Ashild Kjok entitled *Energy Supply as Terrorist Targets? Patterns of "Petroleum Terrorism", 1968-99.*

[4] Distribution of incidents by 'type of facility': offshore drilling rigs – 18 of 60; fixed offshore production platforms – 7 of 60; FPSOs – 5 of 60; FSOs and other storage facilities – 4 of 60; offshore oil export terminals – 5 of 60; other types of facilities (such as oil derricks, wellhead platforms, flow stations) – 4 of 60; and unspecified types of facilities – 14 of 60.

[5] These include: 39 in Africa, 8 in the Middle East, 3 in Asia, 5 in Europe (including Greenland), and 5 in the Americas.

[6] These include: Angola, Iran, Nigeria, Guyana/Suriname, Iraq, Yemen, Indonesia/Malaysia (Malacca Strait), India, Malaysia, Cameroon, and Mexico.

[7] Distribution of incidents by 'type of perpetrators': insurgents – 20 of 60; terrorists – 2 of 60; pirates – between 1-7 of 60; environmental activists – 5 of 60; anti-oil activists and other protesters – 6 of 60; hostile States – 6 of 60; unidentified/unknown perpetrators – 12 of 60.

[8] Distribution of incidents by 'tactic/scenario': abduction of offshore workers – 17 of 60; armed intrusion – 17 of 60; bomb threat or threat of attack – 5 of 60; hostage-taking 4 of 60; bombings and use of explosives – 5 of 60; unauthorised boarding – 8 of 60; military strikes – 6 of 60.

[9] Robert Gramling and William Freudenburg, 'Attitudes Toward Offshore Oil Development: A Summary of Current Evidence' (2006), 49 *Ocean & Coastal Management,* 442, 442-443; Harvey Molotch, William Freudenburg and Krista Paulsen, 'History Repeats Itself, But How? City Character, Urban Tradition, and the Accomplishment of Place' (2000) 65(6) *American Sociological Review,* 791,804.

[10] *Santa Barbara Morning Press* (Santa Barbara), 3 August 1899, 1 quoted and cited in Harvey Molotch, William Freudenburg and Krista Paulsen, 'History Repeats Itself, But How? City Character, Urban Tradition, and the Accomplishment of Place' (2000) 65(6) *American Sociological Review,* 791,804.

[11] Robert Gramling and William Freudenburg, 'Attitudes Toward Offshore Oil Development: A Summary of Current Evidence' (2006) 49 *Ocean & Coastal Management,* 442, 442-443.

[12] Jan Breemer, 'Offshore Energy Terrorism: Perspectives on a Problem' (1983) 6 *Terrorism* 455, 455.

[13] Jan Breemer, 'Offshore Energy Terrorism: Perspectives on a Problem' (1983) 6 *Terrorism* 455, 455.

[14] Brian Jenkins et al, 'A Chronology of Terrorist Attacks and Other Criminal Actions Against Maritime Targets'(Rand Paper Series, RAND Corporation, September 1983), 15.

[15] Brian Jenkins et al, 'A Chronology of Terrorist Attacks and Other Criminal Actions Against Maritime Targets'(Rand Paper Series, RAND Corporation, September 1983) ,16.

[16] Brian Jenkins et al, 'A Chronology of Terrorist Attacks and Other Criminal Actions Against Maritime Targets'(Rand Paper Series, RAND Corporation, September 1983), 20.

[17] Brian Jenkins et al, 'A Chronology of Terrorist Attacks and Other Criminal Actions Against Maritime Targets'(Rand Paper Series, RAND Corporation, September 1983), 21.

[18] US Gulf Task Force, *Environmental Crisis in the Gulf: The US Response* (6 November 1992) cited in Alicia Watts-Hosmer, Colby Stanton, and Julie Beane, 'Intent to Spill: Environmental Effects of Oil Spills Cased by War, Terrorism, Vandalism, and Theft' (Paper presented at 1997 International Oil Spill Conference, Fort

Lauderdale, USA, 7-10 April 1997), 157, 158 <http://www.iosc.org/papers/01058.pdf> at 5 October 2010. See also Larry West, *The 10 Worst Oil Spills in History: The World's Worst Oil Spills by Amount of Oil Released Into the Environment* About.com <http://environment.about.com/od/environmentalevents/tp/worst-oil-spills.htm> , 5 December 2010.

[19] US Government, Office of Response and Restoration, National Oceanic and Atmospheric Administration, US Department of Commerce, *Nowruz Oil Field* <http://www.incidentnews.gov/incident/6262> at 10 November 2010.

[20] Andrew Garwood-Gowers, 'Case Note: Case Concerning Oil Platforms (Islamic Republic of Iran v United States of America) – Did the ICJ Miss the Boat on the Law on the Use of Force?' (2004) 5(1) *Melbourne Journal of International Law,* 241, 243.

[21] James Green, 'The Oil Platforms Case: An Error in Judgement' (2004) 9(3) *Journal of Conflict & Security Law* , 357, 358.

[22] *Oil Platforms (Islamic Republic of Iran v United States of America) (Merits)* [6 November 2003] ICJ, Summary of the Judgement of 6 November 2003.

[23] James Green, 'The Oil Platforms Case: An Error in Judgement' (2004) 9(3) *Journal of Conflict & Security Law* 357, 358.

[24] David Crist, 'Gulf of Conflict: A History of US-Iranian Confrontation at Sea' (Policy Focus No 95, Washington Institute for Near East Policy, June 2009), 7-8.

[25] Andrew Garwood-Gowers, 'Case Note: Case Concerning Oil Platforms (Islamic Republic of Iran v United States of America) – Did the ICJ Miss the Boat on the Law on the Use of Force?' (2004) 5(1) *Melbourne Journal of International Law* 241, 243. See also *Oil Platforms (Islamic Republic of Iran v United States of America) (Merits)* [6 November 2003] ICJ.

[26] *Oil Platforms (Islamic Republic of Iran v United States of America) (Merits)* [6 November 2003] ICJ, Summary of the Judgement of 6 November 2003.

[27] Greenpeace, *The Brent Spar* (21 June 2007) <http://www.greenpeace.org/international/en/about/history/the-brent-spar/> at 8 July 2010.

[28] Greenpeace, *The Brent Spar* (21 June 2007) <http://www.greenpeace.org/international/en/about/history/the-brent-spar/> at 8 July 2010. See also Simon Mar, *The Precautionary Principle in the Law of the Sea: Modern Decision Making in International Law* (Martinus Nijhoff Publishers, 2003), 129-30.

[29] US Department of State, *Patterns of Global Terrorism 1997* (1998) <http://www.state.gov/www/global/terrorism/1997Report/chron.html> at 25 September 2008.

[30] Earth Rights International, *What Happened at Parabe?* (10 November 2009) <http://www.earthrights.org/legal/what-happened-parabe> at 11 December 2010.

[31] Philippe Le Billon, 'Fuelling War: Natural Resources and Armed Conflict' (2005) 45(373) *Adelphi Papers* 7, 36.

[32] Earth Rights International, *What Happened at Parabe?* (10 November 2009) <http://www.earthrights.org/legal/what-happened-parabe> at 11 December 2010.

[33] Department of Transport of Regional Services, *Offshore Oil & Gas Risk Context Statement* (2005) 25.

[34] Neal Adams, *Terrorism & Oil* (PennWell, 2003) 11. Brynjar Lia and Ashild Kjok, 'Energy Supply as Terrorist Targets? Patterns of "Petroleum Terrorism" 1968-99' in Daniel Heradstveit and Helge Hveem (eds.), *Oil in the Gulf: Obstacles to Democracy and Development* (Ashgate, 2004), 100, 110.

[35] US Department of State, *Patterns of Global Terrorism 1999* (2000) <http://www.state.gov/www/global/terrorism/1999report/appa.html> at 25 September 2008.

[36] US Department of State, *Patterns of Global Terrorism 1999* (2000) <http://www.state.gov/www/global/terrorism/1999report/appa.html> at 25 September 2008.

[37] Neal Adams, *Terrorism & Oil* (PennWell, 2003), 11.

[38] US Department of State, *Patterns of Global Terrorism 1999* (2000) <http://www.state.gov/www/global/terrorism/1999report/appa.html> at 25 September 2008.

[39] Patricia Kwast, 'Maritime Law Enforcement and the Use of Force: Reflections on the Categorisation of Forcible Action at Sea in the Light of the *Guyana/Suriname* Award' (2008) 13(1) *Journal of Conflict and Security Law,* 49.

[40] Donna Nincic, 'Troubled Waters: Energy Security and Maritime Security' in Gal Luft and Anne Korin (eds.), *Energy Security Challenges for the 21st Century: A Reference Handbook* (ABC-CLIO, 2009) 31, 32; Michael Klare, *Resource Wars: The New Landscape of Global Conflict* (Owl Books, 2002), 231.

[41] Patricia Kwast, 'Maritime Law Enforcement and the Use of Force: Reflections on the Categorisation of Forcible Action at Sea in the Light of the *Guyana/Suriname* Award' (2008) 13(1) *Journal of Conflict and Security Law* 49, 50. See also Donald Rothwell and Tim Stephens, *The International Law of the Sea* (Hart Publishing, 2010) , 420.

[42] Brynjar Lia and Ashild Kjok, 'Energy Supply as Terrorist Targets? Patterns of "Petroleum Terrorism" 1968-99' in Daniel Heradstveit and Helge Hveem (eds.), *Oil in the Gulf: Obstacles to Democracy and Development* (Ashgate, 2004) 100, 110. See also Martin Murphy, *Small Boats, Weak States, Dirty Money: Piracy & Maritime Terrorism in the Modern World* (Hurst & Co, 2009) , 119.

[43] Business Wire, *Transocean Sedco Forex Confirms Jackup Trident 8 Crew Safely Evacuated and Rig Secured Following Incident of Community Unrest in Nigeria* (27 August 2001) High Beam Research <http://www.highbeam.com/doc/1G1-77574501.html> , 2 January 2011.

[44] John Thackrah, *Dictionary of Terrorism* (Routledge, 2nd ed, 2004) ,185.

[45] Nicolas Pyke, *Suicide Bomber Boats Explode in Attack on Basra Oil Terminal* (2004) The Independent <http://www.independent.co.uk/news/world/middle-east/suicide-bomber-boats-explode-in-attack-on-basra-oil-terminal-756454.html> at 20 September 2008. See also Jihadi Websites Monitoring Group, *Oil Installations as an Attractive Target for Terrorism* (5 November 2009) International Institute for Counter-Terrorism, 11 <http://www.ict.org.il/Portals/0/Internet%20Monitoring%20Group/JWMG_Oil_Installations_as_a_Target.pdf> at 7 August 2010.

[46] Peter Lehr, 'Maritime Terrorism: Locations, Actors, and Capabilities' in Rupert Herbert-Burns, Sam Bateman and Peter Lehr (eds.) *Lloyd's MIU Handbook of Maritime Security* (Taylor & Francis Group, 2009) 55, 60. However, Peter Lehr notes that according to the report of the Jewish Institute for National Security Affairs (JINSA), both boats exploded before they could reach their targets. See Jonathan Howland, *Countering Maritime Terror, US Thwarts Attacks, Builds Up Foreign Navies* (17 June 2004) JINSA Online <http://www.jinsa.org/articles/print.html/documentid/2567> cited in Peter Lehr, 'Maritime Terrorism: Locations, Actors, and Capabilities' in Rupert Herbert-Burns, Sam Bateman and Peter Lehr (eds.) *Lloyd's MIU Handbook of Maritime Security* (Taylor & Francis Group, 2009) 55, 60, n 12.

[47] Ali Koknar, 'Maritime Terrorism: A New Challenge for NATO' (2005) *Energy Security* 18 <http://www.iags.org/n0124051.htm> at 17 March 2009. See also Nicolas Pyke, *Suicide Bomber Boats Explode in Attack on Basra Oil Terminal* (2004) The Independent <http://www.independent.co.uk/news/world/middle-east/suicide-bomber-boats-explode-in-attack-on-basra-oil-terminal-756454.html> at 20 September 2008; John Daly, 'The Threat to Iraqi Oil' (2004) 2(12) *Terrorism Monitor*; Peter Lehr, 'Maritime Terrorism: Locations, Actors, and Capabilities' in Rupert Herbert-Burns, Sam Bateman and Peter Lehr (eds.) *Lloyd's MIU Handbook of Maritime Security* (Taylor & Francis Group, 2009) 55, 61.

[48] Andrew Forbes, 'The Economic Impact of Disruptions to Seaborne Energy Flows' (2008) 23 *Papers in Australian Maritime Affairs* 57, 65.

[49] US Government, US Navy, *Coalition Maritime Forces Revise Iraqi Oil Terminal Protection Procedures* (6 May 2004) <http://www.navy.mil/search/display.asp?story_id=13177> at 31 January 2011.

[50] See, eg, John Daly, 'Terrorism and Piracy: The Dual Threat to Maritime Shipping' (2008) 6(16) *Terrorism Monitor* 4.

[51] Peter Lehr, 'Maritime Terrorism: Locations, Actors, and Capabilities' in Rupert Herbert-Burns, Sam Bateman and Peter Lehr (eds.) *Lloyd's MIU Handbook of Maritime Security* (Taylor & Francis Group, 2009), 55, 61.

[52] Nicolas Pyke, *Suicide Bomber Boats Explode in Attack on Basra Oil Terminal* (2004) The Independent <http://www.independent.co.uk/news/world/middle-east/suicide-bomber-boats-explode-in-attack-on-basra-oil-terminal-756454.html> at 20 September 2008. See also Jihadi Websites Monitoring Group, *Oil Installations as an Attractive Target for Terrorism* (5 November 2009) International Institute for Counter-Terrorism, 11 <http://www.ict.org.il/Portals/0/Internet%20Monitoring%20Group/JWMG_Oil_Installations_as_a_Target.pdf> at 7 August 2010.

[53] Ali Koknar, 'Maritime Terrorism: A New Challenge for NATO' (2005) *Energy Security* 18 <http://www.iags.org/n0124051.htm> at 17 March 2009. See also Nicolas Pyke, *Suicide Bomber Boats Explode in Attack on Basra Oil Terminal* (2004) The Independent <http://www.independent.co.uk/news/world/middle-east/suicide-bomber-boats-explode-in-attack-on-basra-oil-terminal-756454.html> at 20 September 2008; Red Orbit News, *Iraqi Oil Terminal is Closed After Attack* (2004) Red Orbit <http://www.redorbit.com/news/general/53790/iraqi_oil_terminal_closed_after_attack/> at 20 September 2008.

[54] US Government, US Navy, *Coalition Maritime Forces Revise Iraqi Oil Terminal Protection Procedures* (6 May 2004) <http://www.navy.mil/search/display.asp?story_id=13177> at 31 January 2011.

[55] World Tribune, *Yemen on Alert for Al Qaida Attack on Oil Facilities* (3 September 2004) <http://www.worldtribune.com/worldtribune/WTARC/2004/me_terror_09_03.html> at 22 October 2010. See also Shawn Woodford, 'Al-Qaeda and Saudi Arabia: A Chronology' in Erich Marquardt (ed.) *Saudi Arabian Oil Facilities: The Achilles Heel of the Western Economy* (Jamestown Foundation, 2006) 35, 44.

[56] International Maritime Organization, *Reports on Acts of Piracy and Armed Robbery Against Ships: Issued Monthly - Acts Reported During November 2004*, IMO Doc MSC.4/Circ.61 (16 December 2004) annex 2 ('*Acts of Piracy and Armed Robbery Allegedly Attempted Against Ships Reported by Member States or International Organizations in Consultative Status*'), 1.

[57] International Maritime Organization, *Reports on Acts of Piracy and Armed Robbery Against Ships: Issued Monthly - Acts Reported During November 2004*, IMO Doc MSC.4/Circ.61 (16 December 2004) annex 2 ('*Acts of Piracy and Armed Robbery Allegedly Attempted Against Ships Reported by Member States or International Organizations in Consultative Status*') , 1.

[58] International Maritime Bureau, *Piracy and Armed Robbery Against Ships Annual Report 2005* (2006) 55.

[59] Upstream Online, *Delta Rebels Storm Idama Platform* (22 September 2005) <http://www.upstreamonline.com/live/article98970.ece> at 9 May 2011; Estelle Shirbon, *Armed Militants Seize Oil Platform After Leader is Held* (23 September 2005) The Scotsman <http://thescotsman.scotsman.com/world/Armed-militants-seize-oil-platform.2663710.jp> at 9 May 2011.

[60] Estelle Shirbon, *Armed Militants Seize Oil Platform After Leader is Held* (23 September 2005) The Scotsman <http://thescotsman.scotsman.com/world/Armed-militants-seize-oil-platform.2663710.jp> at 9 May 2011.

[61] Some sources report that the incident took place on 10 January 2006; others report that it took place on 11 January 2006.

[62] RedOrbit News, *Gunmen in Kidnap Raid on Oil Platform* (2008) RedOrbit <http://www.redorbit.com/news/display/?id=356153> at 18 September 2008. See also Erich Marquardt, 'The Niger Delta Insurgency and Its Threat to Energy Security' in Jonathan Hutzley (ed.) *Unmasking Terror: A Global Review of Terrorist Activities* (Jamestown Foundation, 2007) vol 3, 236, 238.

[63] Niger Delta Rising, *Timeline of Events* (2010) <http://www.nigerdeltarising.org/resources/timeline> at 28 March 2010.

[64] Africa Master Web, *Chronology of Nigerian Militants' Attacks* (21 February 2007) <http://www.africamasterweb.com/AdSense/NigerianMilitants06Chronology.html> at 1 November 2010.

[65] Bergen Risk Solutions, *Niger Delta Maritime Security Quarterly Review* (9 July 2007) 15 <http://www.bergenrisksolutions.com/index.php?dokument=294> at 2 January 2011.

[66] Daniel Howden, *Shell May Pull Out of Niger Delta After 17 Die in Boat Raid* (17 January 2006) Corp Watch <http://www.corpwatch.org/article.php?id=13121> at 19 August 2008.

[67] International Crisis Group, 'The Swamps of Insurgency: Nigeria's Delta Unrest' (Africa Report No 115, International Crisis Group, 3 August 2006) 1.

[68] Jennifer Giroux, 'Turmoil in the Delta: Trends and Implications' (2008) 2(8) *Perspectives on Terrorism* 11, 15 citing Daniel Howden, *Shell May Pull Out of Niger Delta After 17 Die in Boat Raid* (17 January 2006) Corp Watch <http://www.corpwatch.org/article.php?id=13121> at 19 August 2008.

[69] International Maritime Bureau, *Piracy and Armed Robbery Against Ships Report for the Period 1 January – 31 March 2006* (2006) 25. See also Ed Kashi and Michael Watts, *Curse of the Black Gold: 50 Years of Oil in Niger Delta* (2008) 37.

[70] International Maritime Organization, *Reports on Acts of Piracy and Armed Robbery Against Ships: Issued Monthly - Acts Reported During March 2006*, IMO Doc MSC.4/Circ.84 (18 April 2006) annex 1 ('*Acts of Piracy and Armed Robbery Allegedly Committed Against Ships Reported by*

Member States or International Organizations in Consultative Status') 1.

[71] Bergen Risk Solutions, *Niger Delta Maritime Security Quarterly Review* (9 July 2007) 15 <http://www.bergenrisksolutions.com/index.php?dokument=294> at 2 January 2011; Niger Delta Rising, *Timeline of Events* (2010) <http://www.nigerdeltarising.org/resources/timeline> at 28 March 2010.

[72] Martyn Wingrove, 'Nigeria Kidnap Hikes Up Oil Price', *Lloyd's List DCN* (Sydney), 8 June 2006, 14. See also See also Erich Marquardt, 'The Niger Delta Insurgency and Its Threat to Energy Security' in Jonathan Hutzley (ed.) *Unmasking Terror: A Global Review of Terrorist Activities* (Jamestown Foundation, 2007), Vol 3, 236, 240.

[73] Bergen Risk Solutions, *Niger Delta Maritime Security Quarterly Review* (9 July 2007) , 19 .<http://www.bergenrisksolutions.com/index.php?dokument=294> at 2 January 2011.

[74] Martyn Wingrove, 'Nigeria Kidnap Hikes Up Oil Price', *Lloyd's List DCN* (Sydney), 8 June 2006, 14.

[75] Andy Critchlow and Marc Wolfensberger, *Iran's Navy Attacks and Boards Romanian Rig in Gulf: Update3* (22 August 2006) Bloomberg <http://www.bloomberg.com/apps/news?pid=newsarchive&sid=adVreywC1G_k> at 20 August 2009. See also BBC News, *Iran 'Attacks Romanian Oil Rig'* (22 August 2006) <http://news.bbc.co.uk/2/hi/europe/5274374.stm> at 20 August 2009; Jihad Watch, *Iran Pre-empted Pending Int'l Court Action to Attack Romanian Oil Rig* (27 August 2006) <http://www.jihadwatch.org/2006/08/iran-pre-empted-pending-intl-court-action-to-attack-romanian-oil-rig.html> at 20 August 2009.

[76] International Maritime Bureau, *Piracy and Armed Robbery Against Ships Annual Report 2006* (2007).

[77] International Maritime Bureau, *Piracy and Armed Robbery Against Ships Annual Report* (2007) 53.

[78] International Maritime Bureau, *Piracy and Armed Robbery Against Ships Annual Report* (2007) 53.

[79] Some sources report that the incident took place on 31 March 2007,; others report that it took place on 1 April 2007.

[80] International Maritime Bureau, *Piracy and Armed Robbery Against Ships Report for the Period 1 April – 30 June 2007* (2007) 42; International Maritime Organization, *Reports on Acts of Piracy and Armed Robbery Against Ships: Issued Monthly - Acts Reported During April 2007*, IMO Doc MSC.4/Circ.102 (19 June 2007) annex 1 ('*Acts of Piracy and Armed Robbery Allegedly Committed Against Ships Reported by Member States or International Organizations in Consultative Status*').

[81] Bergen Risk Solutions, *Niger Delta Maritime Security Quarterly Review* (9 July 2007) 19 <http://www.bergenrisksolutions.com/index.php?dokument=294> at 2 January 2011.

[82] David Pearl and Sarah Aboufasha, *Worldwide Threats to Shipping: Marine Warning Information* (2007) National Geospatial-Intelligence Agency <http://www.nga.mil/MSISiteContent/StaticFiles/MISC/wwtts/wwtts_20070502100000.txt> at 22 September 2008.

[83] Bergen Risk Solutions, *Niger Delta Maritime Security Quarterly Review* (9 July 2007) 20 <http://www.bergenrisksolutions.com/index.php?dokument=294> at 2 January 2011.

[84] David Pearl and Sarah Aboufasha, *Worldwide Threats to Shipping: Marine Warning Information* (2007) National Geospatial-Intelligence Agency <http://www.nga.mil/MSISiteContent/StaticFiles/MISC/wwtts/wwtts_20070502100000.txt> at 22 September 2008; Rupert Herbert-Burns, 'Tankers, Specialized Production Vessels, and Offshore Terminals: Vulnerability and Security in the International Maritime Oil Sector' in Rupert Herbert-Burns, Sam Bateman and Peter Lehr (eds) *Lloyd's MIU Handbook of Maritime Security* (Taylor & Francis Group, 2009) 133, 155.

[85] David Pearl and Sarah Aboufasha, *Worldwide Threats to Shipping: Marine Warning Information* (2007) National Geospatial-Intelligence Agency <http://www.nga.mil/MSISiteContent/StaticFiles/MISC/wwtts/wwtts_20070502100000.txt> at 22 September 2008; International Maritime Bureau, *Piracy and Armed Robbery Against Ships Report for the Period 1 April - 30 June 2007* (2007) 43.

[86] Upstream Online, *Force Majeure at Okono-Okpoho* (6 May 2007) <http://www.upstreamonline.com/incoming/article132853.ece> at 30 October 2010.

[87] Bergen Risk Solutions, *Niger Delta Maritime Security Quarterly Review* (9 July 2007) 20 <http://www.bergenrisksolutions.com/index.php?dokument=294> at 2 January 2011.

[88] International Maritime Bureau, *Piracy and Armed Robbery Against Ships Report for the Period 1 April – 30 June 2007* (2007) 43.

[89] Bergen Risk Solutions, *Niger Delta Maritime Security Quarterly Review* (9 July 2007) 20 <http://www.bergenrisksolutions.com/index.php?dokument=294> at 2 January 2011.

[90] Bergen Risk Solutions, *Niger Delta Maritime Security Quarterly Review* (9 July 2007) 22 <http://www.bergenrisksolutions.com/index.php?dokument=294> at 2 January 2011.

[91] David Cutler, *Chronology - Attacks in Nigeria's Oil Delta* (4 June 2008) Reuters <http://www.reuters.com/article/idUSL04786711> at 18 October 2010.

[92] The Hindu, *Gunmen in Speedboats Kidnap 6 Oil Workers in Nigeria* (26 October 2007) <http://www.hindu.com/thehindu/holnus/003200710261962.htm> 16 August 2010. See also Rig Zone, *FPSO Mystras Attacked* (26 October 2007) <http://www.rigzone.com/news/article.asp?a_id=52081> at 20 October 2010.

[93] Mike Nizza, *Another Security Threat: It was All a Dream* (2008) New York Times <http://thelede.blogs.nytimes.com/2008/02/11/another-security-threat-it-was-all-a-dream/> at 20 September 2008.

[94] Australian Federal Police, *North Sea Oil Rig Evacuated After Hoax* (2008) Sydney Morning Herald <http://www.smh.com.au/news/world/north-sea-oil-rig-evacuated-after-hoax/2008/02/11/1202578630294.html> at 29 March 2009.

[95] US Government, National Counterterrorism Center, *Worldwide Incidents Tracking System* <https://wits.nctc.gov> at 21 November 2009.

[96] Nick Tattersall, *Attack Halts Shell's Bonga Oilfield* (2008) Offshore Technology <http://www.offshore-technology.com/news/news5329.html> at 2 July 2008. See also Jeff Vail, *The Significance of the Bonga Offshore Oil Platform Attack* (2008) The Oil Drum <http://www.theoildrum.com/node/4196> at 1 July 2008.

[97] AFX News Limited, *Shell's Bonga Still Not at Capacity after Militant Attack* (2008) Rig Zone <http://www.rigzone.com/news/article.asp?a_id=6358> at 2 July 2008.

[98] Austin Ekeinde, *Nigerian Militants Sabotage Oil Facilities* (16 September 2008) Reuters < http://uk.reuters.com/article/2008/09/16/businessproind-nigeria-delta-dc-idUKLE51403420080916 > at 9 May 2011; Austin Ekeinde, *Nigerian Militants Attacked Two Oil Installations in the Heaviest Fighting in the Niger Delta in Two Years, Security Sources Said on Tuesday* (16 September 2008) Reuters <http://uk.reuters.com/article/2008/09/16/uk-nigeria-delta-idUKLG63750820080916> at 9 May 2011.

[99] International Maritime Organization, *Reports on Acts of Piracy and Armed Robbery Against Ships: Issued Monthly - Acts Reported During December 2008*, IMO Doc MSC.4/Circ.129 (20 March 2009) annex 1 ('*Acts of Piracy and Armed Robbery Allegedly Committed Against Ships Reported by Member States or International Organizations in Consultative Status*').

[100] US Government, National Counterterrorism Center, *Worldwide Incidents Tracking System* <https://wits.nctc.gov> at 21 November 2009.

[101] Niger Delta Rising, *Timeline of Events* (2010) <http://www.nigerdeltarising.org/resources/timeline> at 28 March 2010.

[102] Integrated Regional Information Networks (IRIN), *Nigeria: Timeline of Recent Unrest in Niger Delta Region* (2010) United Nations High Commissioner for Refugees <http://www.unhcr.org/refworld/docid/4b71214bc.html> at 28 March 2010.

[103] Integrated Regional Information Networks (IRIN), *Nigeria: Timeline of Recent Unrest in Niger Delta Region* (2010) United Nations High Commissioner for Refugees <http://www.unhcr.org/refworld/docid/4b71214bc.html> at 28 March 2010.

[104] US Government, National Counterterrorism Center, *Worldwide Incidents Tracking System* <https://wits.nctc.gov> at 21 November 2009.

[105] Niger Delta Rising, *Timeline of Events* (2010) <http://www.nigerdeltarising.org/resources/timeline> at 28 March 2010.

[106] Niger Delta Rising, *Timeline of Events* (2010) <http://www.nigerdeltarising.org/resources/timeline> at 28 March 2010.

[107] Relief Web, *Nigeria: Timeline of Recent Unrest in Niger Delta Region* (4 February 2010) Relief Web <http://www.reliefweb.int/rw/rwb.nsf/db900SID/MUMA-82D2AY?OpenDocument> at 22 October 2010; Integrated Regional Information Networks (IRIN), *Nigeria: Timeline of Recent Unrest in Niger Delta Region* (2010) United Nations High Commissioner for Refugees <http://www.unhcr.org/refworld/docid/4b71214bc.html> at 28 March 2010.

[108] Chief's Briefs by Oyibos OnLine, *Gulf of Guinea 20th – 26th March 2010 Weekly Intelligence Summary* (2010) <http://www.chiefsbriefs.com/?p=3431> at 3 December 2010.

[109] Greenpeace, *Greenpeace Activists Occupy Arctic Oil Rig* (31 August 2010) <http://www.greenpeace.org/international/en/news/features/Greenpeace-activists-occupy-Arctic-oil-rig-100831/> at 15 October 2010; Greenpeace, *Greenpeace Activists End Arctic Oil Rig Occupation* (2 September 2010) <http://www.greenpeace.org/international/en/news/features/Greenpeace-Activists-End-Arctic-Oil-Rig-Occupation020910/> at 15 October 2010.

[110] Greenpeace, *Greenpeace Activists Occupy Arctic Oil Rig* (31 August 2010) <http://www.greenpeace.org/international/en/news/features/Greenpeace-activists-occupy-Arctic-oil-rig-100831/> at 15 October 2010; Greenpeace, *Greenpeace Activists End Arctic Oil Rig Occupation* (2 September 2010) <http://www.greenpeace.org/international/en/news/features/Greenpeace-Activists-End-Arctic-Oil-Rig-Occupation020910/> at 15 October 2010.

[111] Greenpeace, *Activists Stop Chevron Deepwater Drilling Ship Off the Shetland Islands* (21 September 2010) <http://www.greenpeace.org/international/en/news/features/chevron-shetland-stopped210910/> at 15 October 2010. See also Office of Naval Intelligence, *Worldwide Threat to Shipping Report* (7 October 2010) National Geospatial-Intelligence Agency <http://www.nga.mil/MSISiteContent/StaticFiles/MISC/wwtts/wwtts_20101007100000.txt> at 15 October 2010.

[112] Jon Gambrell, *Nigeria: 5 Kidnapped in Offshore Oil Rig Attack* (8 November 2010) Desert News <http://www.deseretnews.com/article/700079609/Nigeria-5-kidnapped-in-offshore-oil-rig-attack.html?pg=2> at 19 March 2011.

[113] Greg Keller, *Pirates Attack Offshore Oil Platform Near Nigeria, Then Kidnap 3 French Employees from Ship* (22 September 2010) Fox News <http://www.foxnews.com/world/2010/09/22/pirates-attack-french-marine-services-ship-nigeria-employees-taken-hostage/> at 19 March 2011. See also Jon Gambrell, *Nigeria: 5 Kidnapped in Offshore Oil Rig Attack* (8 November 2010) Desert News <http://www.deseretnews.com/article/700079609/Nigeria-5-kidnapped-in-offshore-oil-rig-attack.html?pg=2> at 19 March 2011.

[114] Greg Keller, *Pirates Attack Offshore Oil Platform Near Nigeria, Then Kidnap 3 French Employees from Ship* (22 September 2010) Fox News <http://www.foxnews.com/world/2010/09/22/pirates-attack-french-marine-services-ship-nigeria-employees-taken-hostage/> at 19 March 2011. See also Australian Association for Maritime Affairs, 'Inquiry Set Up Into Sector's Security' (2011) 199 *Australian Maritime Digest* 9, 9.

[115] 'Counter Terrorism Security Response: Energy and Nuclear 15-21 November 2010' (Weekly Report, International Centre for Political Violence and Terrorism Research, November 2010) 2. See also Upstream Online, *Crew Snatched in Okoro Raid*(9 November 2010) <http://www.upstreamonline.com/live/article236087.ece> at 4 December 2010; Petroleum Africa, *Okoro Field Attacked Offshore Nigeria* (9 November 2010) <http://petroleumafrica.com/en/newsarticle.php?NewsID=10598> at 4 December 2010.

[116] Jon Gambrell, *Nigeria: 5 Kidnapped in Offshore Oil Rig Attack* (8 November 2010) Desert News <http://www.deseretnews.com/article/700079609/Nigeria-5-kidnapped-in-offshore-oil-rig-attack.html> at 19 March 2011.

[117] Dulue Mbachu and Elisha Bala-Gbogbo, *Exxon Mobil Says Offshore Platform in Nigeria Attacked* (15 November 2010) Bloomberg Businessweek <http://www.businessweek.com/news/2010-11-15/exxon-mobil-says-offshore-platform-in-nigeria-attacked.html> 4 December 2010.

[118] Will Connors, *ExxonMobil Shuts Some Output After Nigeria Attack* (15 November 2010) Fox Business <http://www.foxbusiness.com/markets/2010/11/15/exxonmobil-shuts-output-nigeria-attack/> at 4 December 2010

[119] See also 'Counter Terrorism Security Response: Energy and Nuclear 15-21 November 2010' (Weekly Report, International Centre for Political Violence and Terrorism Research, November 2010), 1-2.

[120] Radio Netherlands Worldwide, Six Killed in Cameroon Oil Platform Attack: Security Source (17 November 2010) <http://internationaljustice.rnw.nl/africa/bulletin/six-killed-cameroon-oil-platform-attack-security-source> 4 December 2010.

[121] Radio Netherlands Worldwide, Six Killed in Cameroon Oil Platform Attack: Security Source (17 November 2010) <http://internationaljustice.rnw.nl/africa/bulletin/six-killed-cameroon-oil-platform-attack-security-source> 4 December 2010. See also Andrew McGregor, 'Cameroon Rebels Threaten Security in Oil-Rich Gulf of Guinea' (2010) 8(43) *Terrorism Monitor* 7, 7.

[122] See 'Counter Terrorism Security Response: Energy and Nuclear 15-21 November 2010' (Weekly Report, International Centre for Political Violence and Terrorism Research, November 2010) 2. See also Agence France Presse (AFP), *Cameroon Rebels Threaten More Oil Attacks: Security Source* (2010)

<http://www.google.com/hostednews/afp/article/ALeqM5jEs8Jwi8Imy11k0OSNXPsEDflzpQ?docId=CNG.43a57f15426eed4e3d9
58f8281348a4b.501> at 4 December 2010.
[123] Greenpeace, *Activist Occupy Oil Rig in the Gulf of Mexico* (22 November 2010)
<http://www.greenpeace.org/international/en/news/features/Activist-occupy-centenario221110/> at 2 January 2011.

Mikhail Kashubsky *is a Principal Consultant at the Centre for Customs and Excise Studies (CCES), University of Canberra, Australia and a PhD Candidate at the Australian National Centre for Ocean Resources and Security (ANCORS), University of Wollongong, Australia. This chronology is based on part of the author's PhD thesis research.*

Living with terror, not Living in Terror: The Impact of Chronic Terrorism on Israeli Society

By Dov Waxman
Source: http://www.terrorismanalysts.com/pt/index.php/pot/article/view/living-with-terror/html

Abstract
This article discusses the impact of chronic terrorism on a targeted society by examining the case of Israeli society during the second Intifada. The Israeli case demonstrates both the extensive effects of repeated terrorist attacks and their limitations. The article argues that while Israelis were seriously affected by Palestinian terrorist attacks during the second Intifada, this did not result in major, lasting changes in Israeli behaviour. Despite being profoundly affected by terrorism, Israeli society was not demoralized by it, and in this respect Palestinian terrorism failed to achieve its aim. This is because the Israeli public grew accustomed to chronic terrorism and possessed a high level of social resilience.

Introduction
At a time when terrorist attacks and thwarted plots regularly dominate the news headlines, when long queues at airport security checks have become all-too-common, and when once innocuous items (drinks, shoes, backpacks) can become the means of deadly attacks, it is clear that the threat of terrorism hangs over us as never before.[1] Terrorism is currently at the top of the national security agenda in the United States and in many other countries around the world. Indeed, terrorism is widely considered to be the greatest security challenge of our time. Many societies around the world are now faced with the prospect of endemic terrorism on their own soil. The September 11, 2001, terrorist attack in the United States; the March 11, 2004, terrorist attack in Spain; and the July 7, 2005, terrorist attack in Britain these are all unlikely to be one-off events. Rather, the United States and many other Western democracies can expect more terrorist attacks in the future. What affect will such attacks have on these countries? What kinds of domestic effects are they likely to produce? It is sometimes argued that the effects of terrorism are quite minimal, and that the current concern with terrorism is well out of proportion to the threat that terrorism actually poses.[2]

Counting the number of terrorist fatalities and comparing this to the number of fatalities in conventional wars, or even traffic accidents, leads some to claim that the threat of terrorism is wildly exaggerated. But counting fatalities from terrorist attacks is the crudest and most simplistic way to measure the impact of terrorism. The consequences of terrorist attacks often go far beyond the deaths and destruction they cause. The effects of terrorism are not limited to its actual victims. They can be wide-ranging and far-reaching. They include the direct and indirect economic costs of terrorist attacks, the psychological effects of terrorism upon the population, and the social and political impact of terrorist attacks. This article will discuss these different kinds of effects with the aim of presenting a fuller picture of the impact of terrorism on a society. In doing so, I will draw extensively upon recent research into the effects of terrorism conducted by psychologists, sociologists, economists, and political scientists. Brought together, this research into the psychological, economic, social, and political effects of terrorism enables us to develop a more comprehensive and integrated understanding of the overall impact of terrorism. This article, therefore, uses the Israeli experience during the

second Palestinian Intifada as a case study to illustrate various effects of terrorism.

Most discussions of terrorism today are concerned with counter-terrorism and the objectives and tactics of terrorist groups, whereas less attention is generally paid to thinking about the impact of terrorist attacks on targeted societies. The focus on counter-terrorism is understandable given the emphasis placed by politicians and the general public on preventing terrorist attacks. We are, however, unlikely to completely eliminate terrorism—a type of political violence whose history dates back thousands of years.[3] It is, therefore, essential that we devote more attention to considering the effects of terrorism, so that we may be better prepared to deal and cope with these effects. In so far as the effects of terrorism can be minimized, the overall effectiveness of terrorism can be reduced. Thus, studying the severity and longevity of the effects of terrorism is crucial to assessing its effectiveness.

There is a growing body of research, especially since the 9/11 attacks, on the effects of terrorist attacks. Numerous studies have now been conducted on the psychological effects of terrorism on individuals. These studies have looked at how terrorist attacks affect people's mental health;[4] with particular attention paid to the incidence of post-traumatic stress disorder (PTSD) following terrorist attacks.[5] Increased rates of depression and substance abuse have also been studied as indications of the psychological effects of terrorism. Another avenue of research has been on the social psychological effects of terrorism, such as the impact of terrorism on xenophobia within a society,[6] on group stereotypes,[7] and on the attitudes and ideological orientation of the targeted population.[8] There have also been some studies on the economic effects of terrorism.[9] These studies have investigated the immediate economic damage caused by terrorism, and the effect on variables such as Gross Domestic Product (GDP), unemployment, foreign direct investment (FDI), and the tourism industry. Finally, within the field of political science there is an increasing amount of literature about the political effects of terrorism, mostly focusing on the impact of terrorist attacks on public opinion,[10] elections,[11] government policy, and peace processes.[12] The big question this literature poses is whether and under what circumstances terrorism works. Terrorist attacks are deliberately designed to instil fear and intimidate a population in order to achieve a political objective.

But how successful are terrorist groups in achieving their political objectives? There is no agreement among scholars on this critical issue. While some have highlighted the political gains that terrorist groups have achieved,[13] others have argued that terrorism often backfires politically and is not an effective strategy against democratic states.[14]

This article also addresses the question of whether terrorism works, but from a slightly different perspective—it looks at the overall impact of terrorism on the targeted population. To understand how effective terrorism as a strategy is, it is necessary to assess its impact upon the targeted society. Terrorists hope that by sowing fear and panic within the targeted public, this will pressure the government to act in ways they desire. In other words, creating public fear, panic, anxiety, distress etc. is essential to the accomplishment of terrorism's political strategy.

By examining how terrorism affects its audience, therefore, we can gauge the effectiveness of terrorism as a strategy. I will do this by investigating the impact of Palestinian terrorism on Israeli society during the second Intifada.

In this article, I hope to contribute to the ongoing scholarly debate about the effectiveness of terrorism in a number of specific ways. First, in considering the economic, psychological, and social effects of terrorism as well as its political effects, the article provides a more complete account of the impact of terrorism than studies that narrowly look at its political effects alone. Terrorism's political consequences cannot be properly assessed in isolation from its other effects. The political effects of terrorism should be looked at in a broader context.

Second, instead of just examining the consequences of a single terrorist attack, this article investigates the effects of repeated terrorist attacks on the targeted society. A society's response to a single, large-scale terrorist attack such as occurred on 9/11 might be very different than its response to repeated, smaller-scale attacks. Hence, the effects of ongoing, 'chronic terrorism' may significantly differ from the effects of a one-off terrorist attack.[15] This article tackles the question of how societies specifically respond to chronic terrorism. It would seem logical to expect that repeated exposure—direct and indirect—to terrorist attacks and living with the constant possibility of sudden violent death, would severely affect a society. But is this really the case? Do repeated deadly terror attacks create more

public fear and insecurity or do they have a progressively weaker affect on the population? Do societies become traumatized by prolonged terrorism or can they learn to live with it? I argue that a society can gradually grow accustomed to chronic terrorism, and consequently, its impact declines. In short, societies can effectively become habituated to terrorism and learn to cope with it.

Third, by using the example of Israeli society during the second Intifada to illustrate this argument, this article offers an in-depth case study of the effectiveness of terrorism—or its lack thereof—and thus complements the more quantitative, statistically based studies that characterize a lot of political science work on this topic. Unfortunately for Israelis, Israel represents an excellent case study for analyzing the effects of chronic terrorism. Although it is not the only country to have experienced endemic terrorism—Sri Lanka and Northern Ireland are two other examples—no country has endured more acts of terrorism over a prolonged period than Israel. From before the state was established in 1948 and ever since then, Israelis have been the targets of terrorist attacks, both within Israel and around the world. Indeed, the history of modern terrorism is linked to the history of the Israeli-Palestinian conflict, as Arab militant groups have pioneered new terrorist tactics (notably, airplane hijackings and suicide bombings) and carried out some of the best known terrorist attacks in history (such as the hostage-taking of Israeli athletes at the 1972 Munich Olympic games). The threat of terrorism has long been a fact of life for Israelis. Thus, Israeli society's experience with terrorism can potentially offer many insights into the impact of chronic terrorism on societies.

Finally, the conclusion of this article emphasizes the importance of social resilience in coping with terrorism. I argue that Israeli society was able to cope with relentless terrorism during the second Intifada and quickly recover from it because it possessed a high level of social resilience. It is therefore essential to recognize the importance of social resilience and understand what contributes to it in order to better manage the threat of terrorism and maybe even to one day conquer it.

The Toll of Terrorism: Israel during the Second Intifada

In this article, I will focus on the impact of Palestinian terrorism on Israeli society during the second Intifada (sometimes called the "al-Aqsa Intifada"),[16]

specifically during the period from the end of September 2000 until the beginning of 2005 (when the second Intifada effectively ended).[17] During this time, more than one thousand Israelis were killed, the overwhelming majority of them civilians (70 percent were civilians, 30 percent members of the security forces).[18] This figure was more than the number of Israelis killed in all terrorist attacks in the thirty-five years prior to the second Intifada.[19] Thus, the second Intifada inflicted a heavy death toll upon Israelis, especially civilians.[20] In all, according to casualty figures calculated by the Israeli human rights group B'Tselem, from 29 September 2000 to 15 January 2005, a total of 431 Israeli civilians were killed inside Israel by Palestinians (including 78 aged under the age of 18), and an additional 218 Israeli civilians were killed in the West Bank and Gaza Strip.[21] In just over four years of the second Intifada, therefore, a total of 649 Israeli civilians were killed. By way of comparison, throughout more than thirty years of the "Troubles" in Northern Ireland (1969-2001), 1857 civilians of all sides were killed.[22] The impact of Palestinian terrorist attacks upon Israeli society during the second Intifada, however, cannot simply be measured in terms of the number of Israeli fatalities. It was much more far-reaching and profound, as this article will show.

Suicide terrorist attacks were a prominent feature of the second Intifada.[23] Although Palestinians began carrying out these attacks years before the second Intifada (the very first took place in 1989), suicide attacks skyrocketed after its outbreak in September 2000, peaking in the years 2001 to 2003 (4 suicide attacks occurred in 2000, increasing to 35 in 2001, up to 53 in 2002, then dropping to 26 in 2003, and down to 12 in 2004). These suicide terror attacks were responsible for a large proportion of Israeli casualties.[24] For instance, although less than one percent of all Palestinian attacks against Israelis between September 2000 and August 2002 were suicide terrorist attacks, almost 44 percent of Israeli fatalities from Palestinian attacks were killed in these attacks.[25] Thus, suicide terrorism became the deadliest weapon in the arsenal of Palestinian militant groups (and was widely supported and extolled by Palestinian society during this time[26]). As Hamas leader Abdel Aziz al-Rantisi declared, suicide attacks were "one of our most effective means, which can rival the impact of their F-16s."[27] In addition to Hamas, many other Palestinian

groups (notably, Palestinian Islamic Jihad, Fatah and its offshoots Tanzim and the al-Aqsa Martyrs Brigade, and the Popular Front for the Liberation of Palestine) conducted suicide terrorist attacks in Israel during the second Intifada.[28] Most of these attacks were directed against Israeli civilians ('soft targets') and sought to inflict the maximum number of civilian casualties by being carried out in locations where many civilians congregate such as cafes, restaurants, outdoor markets, shopping malls, and public buses. Among the most notorious suicide attacks were the bombing at the Dolphinarium disco in Tel Aviv on 1 June 2001 that killed twenty-one people (most of them teenagers); the bombing at the Sbarro pizza restaurant in Jerusalem on 9 August 2001 that killed fifteen; and the bombing of the Park Hotel in Netanya on the Jewish Passover holiday on 27 March 2002 that killed thirty.

Apart from the many deaths and injuries resulting from these terrorist attacks, what other effects did they have? In the following sections of this article, I will try to answer this question by discussing the psychological, economic, social, and political effects of terrorism, and describing how these effects manifested themselves in Israel during the period of the second Intifada.

Psychological Effects

The first and most immediate effects of terrorism are psychological.[29] Terrorist campaigns can be expected to psychologically affect a sizeable portion of the population of a targeted society, either directly, by harming a person or their family, or indirectly, through the extensive media coverage of terrorist attacks.[30] The greater the number of attacks and the more lethal those attacks are, the more people that will be psychologically affected by them. Terrorism is a form of psychological warfare against a society.[31] It is designed to strike fear into the heart of the targeted society, and it generally succeeds in doing so. Suicide terrorism can be particularly effective in terrifying people because it projects an aura of fanaticism,[32] which makes the threat of future attacks seem more likely. Peoples' fear of terrorism is both rational and irrational; rational in that there is an ever-present threat of a terrorist attack being repeated, but irrational in the probability assigned to that potential event.[33] Since people tend to overestimate their chances of being a victim to terrorism,[34] the fear of terrorism is widespread in a society. It does not, however, affect everyone to an

equal degree. Research has shown that there is a negative correlation between a person's education and their fear of being a victim of terrorism. This suggests that the more educated a person is, the less likely they are to succumb to the irrational fear evoked by terrorism.[35]

In the case of Israel, a large majority of Israeli civilians have long feared terrorism. Israelis' personal fear of terrorism has been recorded in public opinion surveys over many years. In a 1979 survey, 73 percent of respondents reported being "afraid" or "very afraid" that they, or their close family members, would be hurt in a terrorist attack.[36] Similarly, 85 percent of Israelis expressed this fear in a poll conducted in 1995, and 78 percent in a 1996 poll.[37] Israelis' fear of terrorism reached new heights during the second Intifada. In the spring of 2002—when Palestinian suicide bombings inside Israel were most frequent—92 percent of Israelis reported fear that they or a member of their family would fall victim to a terrorist attack.[38] Hence, at this time, almost every member of Israeli society feared for the safety of their family members and themselves. While this fear certainly had some basis, it was not grounded entirely in the facts, since the probability of themselves or a member of their family being killed or wounded in a terrorist attack was actually far smaller than what the Israeli public believed.

Nevertheless, Palestinian terrorist attacks during the second Intifada affected a large number of Israelis. Nineteen months into the second Intifada, 16.4 percent of Israeli adults said they were the victims of a terrorist attack, 22.1 percent had friends or relatives who were victims, and a further 15.3 percent knew someone who survived a terrorist attack without injury. In total, a staggering 44.4 percent of the Israeli population was exposed to a terrorist attack.[39] With terrorist attacks affecting so many people, it is not surprising that they resulted in widespread psychological problems. More than a third of Israelis who participated in a major psychological study reported at least one traumatic stress-related symptom (TSR), with an average of four symptoms reported per person.[40]

The number and intensity of TSR symptoms reported by the Israeli sample during the second Intifada was similar to the number and intensity reported by Americans following the terrorist attacks on September 11, 2001, even though far fewer Americans were directly exposed to

the 9/11 attacks.[41] This suggests that terrorism can psychologically affect people who have no direct connection to a terrorist attack. Indeed, there is no statistically significant association between psychosocial responses to traumatic events and the level of exposure.[42] Being an actual victim of terrorism has little affect on the prevalence of stress-related psychological disorders, while gender and age have a far more acute affect. Hence, a person who is injured in a terrorist attack is no more likely to suffer from psychological disorders than a person whose only connection to the attack was seeing it on television. The extensive media coverage of terrorist attacks can therefore seriously harm people's psychological well-being.

The psychological effect of terrorism that is easiest to quantify is the prevalence of post-traumatic stress disorder (PTSD).[43] PTSD is a potentially socially crippling psychological disorder. One of the major symptoms of PTSD is avoiding people or situations that remind one of the traumatic experience. PTSD can change the way people behave at home and at work; hence neither the private nor public sphere is immune from the harm caused by terror attacks.[44] In the middle of the second Intifada, 9.4 percent of Israelis suffered from PTSD. But the occurrence of PTSD varied considerably between men, women, and children, with 40 percent of Israeli children suffering from this disorder.[45] Women are also more likely to have PTSD than men, and also have a significantly higher chance of having TSRs and depression.[46] Hence, the psychological effects of terrorism are by no means uniform. Different people are affected to different degrees.

The psychological effects of terrorism are not limited to PTSD. For example, those who witness terrorist attacks but are not directly harmed are generally the last to be evacuated from the scene of the attack, since medics typically focus their attention on the casualties.[47] These people typically replay the scenes of carnage endlessly in their heads, and many end up with "hypertension, accelerated pulse, disassociation, and a desire to flee from the slightest noise, such as a car exhaust pipe backfiring or even a slamming door."[48] In the wake of terrorist attacks, people can become incapable of concentrating on their typical daily tasks. For example, following the 9/11 attacks, 52 percent of Americans polled said that they could not concentrate on their work as a result of those attacks.[49] Terrorism, therefore, has a

significant impact on people's everyday lives, whether or not they are directly exposed to it.

The psychological effects of terrorism are by now well-documented. What is less clear, however, is the psychological impact of repeated terrorist attacks. Do more terrorist attacks result in more psychological damage to the population or does their psychological impact diminish over time? One might think that a wave of suicide attacks would have an increasingly negative psychological impact on the targeted population. After all, it stands to reason that repeated exposure to traumatic events will make the affected public more fearful and more prone to stress-related disorders. In Israel's case, however, this does not appear to be the case. Despite experiencing numerous traumatic events during the second Intifada, which should logically cause progressively more psychological damage, the rate of PTSD symptoms among the Israeli population remained at a fairly low level.[50] This was the case despite the fact that 60 percent of Israelis believed that their lives were in danger, and 68 percent believed the same about the lives of their family and friends.[51]

The explanation for this lies in what is known as the accommodation effect.[52] The accommodation effect means that the amount of stress created by recurring traumatic events actually decreases.[53] Hence, as terrorism becomes a regular occurrence, a process of habituation and de-sensitization may occur, and people become able to maintain a semblance of a normal life.[54] This suggests that people can learn to live with terrorism and psychologically cope with it. Further evidence of the ability of the Israeli population to cope with repeated exposure to *terrorism* is provided in a study of the effect of terrorism on the life satisfaction (happiness) of Israelis between 2002-2004.[55] This study revealed that Palestinian terrorist attacks had a very limited effect upon the overall happiness of Israelis, and that despite living with a high level of terrorism "Israelis were not particularly unsatisfied with their lives when compared to citizens of other, mostly terrorism-free, countries."[56]

The negligible impact that the campaign of terrorism from 2002-2004 had upon the happiness of Israelis suggests that the psychological effects of terrorism should not be overstated. While they can be severe, they are generally short-lived. Despite experiencing fear, anxiety and stress in the aftermath of a terrorist attack, and even suffering

from PTSD, over time most people recover well and are soon able to function normally again (at least within a matter of months).[57] Even repeated exposure to terrorism, as Israelis experienced during the second Intifada, does not have devastating psychological consequences upon a population. To be sure, there is some evidence to suggest that chronic exposure to terrorism is more psychologically harmful than the experience of a single terrorist attack (such as 9/11),[58] but even in this extreme case people demonstrate a great deal of psychological resilience.

Economic Effects

The economic effects of terrorism can be broken down into its direct costs, associated with the destruction caused by an act of terrorism, and its indirect costs, which affect nearly every aspect of a targeted state's economy. The most direct economic effect of a terrorist attack is the damage caused to life and property at the site of the attack. As an example, a suicide attack in a supermarket would cause direct economic damage in four different ways. First, it would damage the infrastructure of the building and destroy products. While the costs of rebuilding or repairing the building and restocking goods might be significant to the store in question, they do not have any affect on the economy at large. Second, the supermarket would probably have to shut down, at least temporarily. With no income generated by the store, national economic output would fall. This would also have no major impact upon the national economy. Even in a small country like Israel there are 470 supermarkets controlled by the main three supermarket chains, hence the damage to one of them is not going to affect Israel's economy.[59] Third, if the terrorist attack killed people, one must also take into account the lost lifetime earnings of each individual killed. Since the numbers of people killed in individual terrorist attacks are relatively few (compared with the amount of deaths in civil wars or inter-state conflicts) this is also an insignificant cost for the national economy. Fourth, if the terrorist attack results in many casualties, then the wounded both lose earnings and need to pay for medical procedures (the cost to an economy does not change if the cost of medical procedures is borne by the wounded themselves or by their government), but this too has no real impact on the national economy. Thus, the direct economic impact of a terrorist attack is minimal. Even 9/11, the most devastating terrorist

attack in modern history, had a direct cost of roughly $27 billion.[60] In comparison, World War II cost the U.S. government over $15 trillion, when adjusted for inflation.[61]

The indirect economic costs of terrorist attacks, however, are potentially more significant. The indirect economic effects of terrorism are many and varied, yet they are very difficult to accurately gauge. Terrorism can affect an economy in numerous ways. A long-running terrorist campaign can definitely impact a state's GDP, as happened to Israel during the second Intifada.[62] Israel's GDP growth dropped sharply following the outbreak of the second Intifada. Israel's GDP growth slowed from an average of 5 percent in the two years prior to the Intifada to -0.8 percent in the first two years of the Intifada.[63] Only by the fourth year of the Intifada, did Israel's GDP growth rebound.[64] A terrorist campaign can make an economy more unstable, which in turn increases risk in the economy. With a higher risk and the same or slightly lower potential return, foreign direct investment in the targeted country's economy can decline. Since foreign investors have a large choice of countries to invest in, any kind of uncertainty, even one resulting from minor terrorist acts, can lead to a drop in the inflow of foreign funds.[65] In Israel, FDI dropped sharply from $5.01 billion in 2000 to $1.72 billion in 2002, before recovering to $3.7 billion in 2003.[66] Finally, the perceived risk of future terrorist attacks can lower confidence in the economy, which in turn affects consumer spending, an integral part of an economy.[67]

A country's tourism industry is particularly hard hit by terrorism since tourist destinations can be easily substituted, and dangerous ones usually become instantly unattractive to foreign tourists.[68] Even a small risk of terrorism leads potential tourists to travel elsewhere. Thus, the more reliant a country's economy is on tourism, the more it will be affected by terrorism. In Israel's case, terrorism in the second Intifada had a significant impact on the country's tourist industry. The amount of foreign tourists in Israel declined from 2.7 million in 2000 to 718,000 in 2002, before recovering slightly to 1.25 million in 2004.[69] Yet since tourism is only responsible for about 1.5 percent of Israel's GDP, a decline in foreign tourists (who comprise roughly 30-35 percent of tourists in Israel) does not have a great effect on the overall health of the Israeli economy.

Ultimately, the economic effects of terrorism depend upon many factors. Significant economic costs are unlikely to be incurred as a result of a single terrorist attack, but a prolonged campaign of terrorism can negatively impact a country's GDP, especially in the case of a small country in which tourism is a large sector of the national economy.[70] Of course, relatively wealthy countries are more able to absorb the economist costs of terrorism than poorer countries, where any loss of national income can have immediate repercussions on the population's living standards. In Israel's case, while terrorism definitely hurt the Israeli economy during the second Intifada, it soon recovered and Israel's economic development continued.

Social Effects

Whereas the economic impact of terrorism ranges from minimal to moderate, the same is not necessarily the case with the social impact of terrorism. The social effects of terrorism can be pronounced and far-reaching, influencing many different aspects of a society. The starting point for the impact of terrorism on a society is the affect that terrorist attacks have upon people's beliefs and attitudes. Major events influence people's beliefs and attitudes.[71] Shavrit et al. explain that: "terror attacks are negative, threatening events. Considerable evidence from psychological studies has shown that negative information tends to be more closely attended, better remembered, and have a stronger impact on evaluations and judgments than positive information."[72] Thus, since terrorist attacks are events of a highly negative nature, they can lead to changes in people's beliefs and attitudes. One such belief concerns how people view other societies, especially the society which the terrorists belong to.

In a situation of inter-group conflict, terrorist attacks increase negative beliefs about and hostile attitudes toward the opposing group the terrorists claim to represent.[73]

A sense of victimhood is common to a society experiencing terrorism.[74] Civilians are not expected to be victims of political violence (whereas military casualties are expected); hence, a public feels victimized when it is the target of political violence (i.e. when it experiences terrorist attacks).[75] The more the civilian population is targeted, the more this sense of victimhood increases. This sense of victimization in turn leads to a de-legitimization of the terrorists and the people they claim to represent. Consequently, the

targeted society becomes unwilling or unable to consider the other side's grievances and objectives.[76] No longer is the opposing group believed to have rational objectives and/or justifiable grievances; instead, the worst views become 'common sense,' especially those concerning its propensity towards violence. Thus, while 39 percent of Israeli Jewish respondents perceived Palestinians as violent in a 1997 survey, by the end of 2000 after the onset of the second Intifada, this figure had risen to 68 percent of Israeli Jews.[77]

The threat of terrorism increases a group's reliance on stereotypes,[78] leading to more negative stereotyping by members of the targeted society.[79] There have been numerous instances of this such as the rise of "Islamophobia" in the United States following the 9/11 attacks,[80] and the increase in anti-Arab sentiments in Spain in the wake of the 2004 Madrid train bombings.[81] Likewise, in Israel during the second Intifada, Israelis held extremely negative stereotypes of Palestinians, viewing them as dishonest, violent, and having little regard for human life.[82]

Another major social effect of terrorism is a rise in ethnocentrism and xenophobia as a group increases its solidarity in the face of violence.[83] Hence, identification with, and support for, the in-group rises as a result of terrorism, while identification with, and support for, any out-group decreases. This was apparent in Russia in the wake of terrorist attacks carried out by Chechen militants, when ethnic Russian identity became more salient, while xenophobia rose.[84] This also took place in the United States in the aftermath of 9/11, when there was a surge of patriotic sentiment (evident, for instance, in the numerous American flags that adorned windows in New York City—a place where such overt displays of American patriotism are generally less common than elsewhere in the country). So too, in Israel during the second Intifada repeated Palestinian terrorist attacks led to a renewed sense of national unity among Israeli Jews. A public opinion survey taken in March 2002, for example, posed the question: "In your opinion have recent events, including terrorist attacks and operation 'Defensive Shield,' strengthened or weakened the sense of national unity in the Israeli-Jewish public?" Eighty-six percent of Israeli Jewish respondents answered that the events strengthened national unity.[85] As one Israeli commentator

put it: "Israeli (Jewish) society in Israel has returned to a state of cohesiveness."[86]

While Israeli Jews experienced a renewed sense of solidarity in the face of the wave of Palestinian terrorism unleashed in the second Intifada, Arab citizens of Israel became the object of intensified suspicion and hostility.[87] Israeli Arabs were increasingly perceived as a security threat and a potential 'fifth column' in Israel's conflict with the Palestinians.[88] As more and more Israeli Jews came to view Israeli Arabs as the enemy (because of their general identification with, and support for, Palestinians in the West Bank and Gaza), popular support increased for policies that would promote their voluntary emigration or even force them to leave Israel. In one survey in 2003, for example, 57 percent of Israeli Jews expressed support for the government encouraging the emigration of Arabs from Israel, and 33 percent favored their expulsion.[89] Growing intolerance of Israeli Arabs was evident not only in social attitudes, but also in government legislation aimed at them. For example, the Knesset (the Israeli parliament) passed a bill in 2002 that curtailed the freedom of expression of Arab political parties and Knesset members by allowing the Central Elections Committee to ban parties and individuals that supported (in action or speech) "the armed struggle of enemy states or terror organizations" against the State of Israel.[90] Another law passed on July 22, 2002, lifted the parliamentary immunity of Knesset members who violated this restriction, thereby allowing them to be legally prosecuted.

Just as Muslims in the United States and Europe have complained about suffering from intolerance, harassment, and discrimination in the aftermath of recent terrorist attacks (most notably 9/11),[91] Arabs in Israel during the second Intifada made similar complaints. Although official and unofficial discrimination against Israeli Arabs long predates the second Intifada and cannot simply be attributed to Palestinian terrorism, there is evidence that Palestinian terrorism during the second Intifada did increase discrimination against Arabs in the Israeli labor market.[92] More generally, Palestinian terrorist attacks increased anti-Arab attitudes within Israeli-Jewish society[93]—the most blatant expressions of which were the calls of "Death to Arabs" in soccer stadiums and at the sites of terrorist attacks, and in slogans like "No Arabs – No Terror Attacks" appearing in graffiti and on car bumper stickers.[94] Hence, Palestinian terrorism undoubtedly

exacerbated the already tense relationship between the Jewish and Arab communities in Israel.

Beyond these specific effects of Palestinian terrorism on Israeli society are the less obvious, but no less real, social repercussions of persistent political violence. In Israel's case, it has been argued that the stress that terrorism creates manifests itself in a rise in violent crimes (homicide and robbery), and a general "brutalization of Israeli society."[95] The fact that criminal homicide in Israel increased by 28 percent from 2000-2001 (i.e., from the year before to the year after the beginning of second Intifada) and robberies increased by 11 percent offers some evidence—though by no means conclusive—to support this argument.[96] Although it is difficult, if not impossible, to prove a causal connection exists between terrorist attacks and societal violence, further support for this linkage comes from the discovery by scientists of a positive relationship between stress and aggression.[97] Aggressive social behavior in Israel may, therefore, be linked to the high threat of terrorism Israelis face.[98]

Political Effects

The extensive social effects of terrorism described above often have political implications. The unifying effect that terrorism had upon Israeli-Jewish society during the second Intifada is typical of what is known as the "rally around the flag" syndrome, which is common to societies experiencing terrorism.[99] The "rally around the flag" syndrome generally leads to a muting of public criticism of the government and its policies. This public reaction to terrorism is also in line with "system justification theory," according to which threats increase social conservatism (the desire to defend and maintain the status quo).[100] The role that terrorism can play in strengthening conservatism was demonstrated in a study that compared Spanish attitudes before and after the Madrid train bombings, which found that the bombings increased adherence to conservative values.[101]

In some cases, the political effects of terrorism are clear-cut and pronounced, but often they can be difficult to accurately assess because specific political outcomes cannot be casually linked to terrorism due to the multiplicity of potential causes. A government's policy or a particular political decision may be the result of any number of factors, and can therefore rarely be definitively

attributed only to a terrorist attack or series of attacks. Take the case of the Sharon government's adoption of the policy of disengagement, which brought about the complete withdrawal of Israeli settlers and soldiers from the Gaza Strip in September 2005. *Was this policy the result of Palestinian terrorist attacks, as many Palestinians at the time believed?*[102] Even if Palestinian terrorism was a factor, it was certainly only one of a number of reasons behind the Sharon's government decision to unilaterally withdraw from Gaza.[103]

While the political impact of terrorism is often hard to pinpoint, nevertheless it can hardly be doubted that terrorism has political effects and influences the political process, at least in democratic and partially democratic states. The most obvious way in which terrorism can influence the political process is by bringing about changes in public opinion, which governments then tend to take into account when formulating their policies.[104] It can be very hard for governments to resist the pressure from public opinion for a strong reaction in the wake of a terrorist attack. For an elected policymaker, the political costs of under-reacting to a terrorist attack are always higher than the political costs of overreacting. The failure to prevent future attacks due to inaction can be fatal to a politician's career, while failing to prevent them after having taken strong measures can be justified as having done everything possible.[105]

The impact of terrorism on public opinion, however, is not as straightforward or predictable as one might imagine. There is no uniform public response to a terrorist attack. Numerous factors affect how a public responds to a terrorist attack, such as the nature and scale of the terrorist attack, and the context in which it occurs. Moreover, different groups within the general public respond in different ways to a terrorist attack. People with different political orientations are likely to have different responses since existing political orientations serve as a mechanism through which new information is received and processed.[106] Nor do terrorist attacks necessarily change people's political opinions. The greater a person's confidence in their views, the less likely they are to change as a result of a major event, like a terrorist attack.[107] Finally, people's views are more likely to be influenced by a terrorist attack when it receives a lot of media coverage since this serves to increase its perceived importance.[108]

In Israel's case during the second Intifada, Palestinian terrorism definitely had an impact on Israeli public opinion concerning the conflict with the Palestinians and the prospects for peace with them (although, of course, it was not the only factor affecting Israeli public opinion).[109] Prior to the second Intifada while the Oslo peace process was ongoing, a large majority of the Israeli public was optimistic about the possibility of achieving peace with the Palestinians (according to one survey in 1999, 68 percent of Israeli Jews believed that peace between Israel and the Palestinians would be achieved within three years).[110] Israeli hopes for peace were dashed by the collapse of the peace process and especially the outbreak of the second Intifada.[111] The surge of Palestinian terrorist attacks between the years 2001-2004 contributed to a significant change in Israeli Jewish beliefs about Palestinian intentions and the prospects for peace.[112] Whereas in 1999 less than 50 percent of Israeli Jews thought that the Arabs wanted to conquer the State of Israel, in 2002 this number had risen to 68 percent, and by 2004 it reached 74 percent.[113]

Palestinian terrorism helped convince Israeli Jews that, in the oft-repeated phrase first used by their Prime Minister Ehud Barak, they had "no partner for peace."[114] Although a majority consistently continued to support a two-state solution to the Israeli-Palestinian conflict, there was little hope that such a solution could be reached in the foreseeable future. In a March 2001 survey, for instance, 72 percent of Israeli Jews thought that the Palestinian Authority (PA) was not interested in a peace treaty with Israel.[115] Similarly, in a 2002 survey, 68 percent of Israelis thought that it was impossible to reach a peace agreement with the Palestinians, and only 26 percent thought that signing peace treaties would mean an end to the Arab-Israeli conflict (compared to 30 percent in 2001, 45 percent in 2000, and 67 percent in 1999).[116]

Accompanying the change in Israeli views of the Palestinians and the possibility of achieving peace with them, was greater public support for the use of more aggressive military measures against the Palestinians and less support for continuing peace negotiations. Prime Minister Barak's premiership became a casualty of this change in Israeli public opinion. He was attacked by his political opponents on the right for not responding to the Intifada with the force necessary to quell it (slogans like "Let the IDF win" and "Barak is humiliating Israel" became popular). Whilst Barak was

accused abroad (and by some in Israel) of excessive use of force against the Palestinians, he was assailed by the right for insufficient use of force. Increasingly unpopular with the Israeli public, Barak eventually suffered a massive defeat in the February 2001 election for prime minister at the hands of right-wing Likud party leader Ariel Sharon.[117] Disillusioned with the Oslo peace process and convinced of the futility of further negotiations with the Palestinians (at least with its current leadership), the Israeli public elected a strong, hard-line leader who they hoped could bring them greater security (by implementing a policy of severe military retaliation for Palestinian terrorist attacks).

Palestinian terrorism during the second Intifada clearly affected the political preferences of the Israeli electorate.[118] Sharon's resounding victory in the 2001 election was one indication of this effect. Another was the Likud's party decisive win in the 2003 Knesset elections, doubling the number of its seats in parliament (from 19 to 38), while the rival center-left Labor party lost seven seats (dropping from 26 to 19 seats). Not only did Palestinian terrorism boost the electoral appeal of the political right in Israel,[119] it also helped to bring about a rightward shift in the political positions of the Israeli public. In general, more Israelis identified themselves as right-wing and fewer as left-wing.[120] On the specific issue of 'land for peace' (that is, the idea of returning territories in exchange for peace), Israeli-Jewish support for it dropped from 50 percent in 2000 to only 37 percent in 2002.[121] This shift to the right was also evident in the increased number of Israeli Jews who were opposed to removing any Jewish settlements in the event of a peace agreement—a ten percent increase in just one year from 2000-2001 (from 26 percent to 36 percent of Israeli Jews).[122] Nevertheless, these changes in Israeli-Jewish public opinion were not lasting—support for the principle of 'land for peace' gradually rose after 2002 as the level of violence decreased, reaching 48 percent in 2005 at the end of the second Intifada.[123] Likewise, opposition to the removal of Jewish settlements also declined after 2002.[124] This suggests that Palestinian terrorism only had a temporary impact on the political views of Israeli Jews.[125] It initially had a pronounced affect on Israeli-Jewish public opinion, but gradually this affect lessened over time.

Although Palestinian terrorism only had a short-term impact on Israeli-Jewish political opinion (concerning things like their willingness to compromise for the sake of peace, and their positions regarding a permanent solution to the conflict with the Palestinians), it had a major impact on their attitudes towards the use of force against Palestinians. Israeli Jews became much more militant and 'hawkish.' Terrorist attacks increased Israeli public support for strong military actions. The militancy of Israelis rose during periods when there was an upsurge in terrorism, and declined in periods of relative quiet.[126] The rise in militant attitudes among Israelis was clearly apparent during the early years of Sharon's tenure as prime minister at the height of the second Intifada. Angry and embittered by the seemingly endless series of gruesome Palestinian suicide bombings inside Israel, the vast majority of the Israeli public staunchly supported the Sharon government's offensive military measures against the Palestinians. In 2001, for instance, 89 percent of Israeli Jews supported the Sharon government's policy of "targeted assassinations" of Palestinian militants involved in terrorism against Israel; the following year the number was 90 percent; and in 2003 it had risen to 92 percent.[127] The overwhelming public support for Prime Minister Sharon's tough policies towards the Palestinians revealed the emergence of a new national consensus in Israel. According to Ephraim Yuchtman-Yaar: "This consensus is reflected in widespread mistrust of the Palestinians' commitment to make peace with Israel, and in the common conviction that so long as Palestinian terror continues, Israel must resort to arms in order to protect the lives of its citizens."[128] Palestinian terrorism undoubtedly played a role in creating this new national consensus in Israel.

The powerful influence that Palestinian terrorist attacks could have upon Israeli public opinion and consequently Israeli government policy toward the conflict with the Palestinians during the second Intifada was most evident in the spring of 2002. March 2002 was the bloodiest month of the second Intifada for Israelis. During that month, Palestinian suicide bombing attacks killed at least eighty Israeli civilians and wounded or maimed some 420 people.[129] In one week alone, Palestinian suicide bombers struck at a restaurant in Haifa, a Jerusalem supermarket, a café in Tel Aviv, and a hotel in Netanya, the latter during a meal for the Jewish holiday of Passover (this last attack killed thirty people and wounded over 140). This devastating series of suicide bombings unleashed

a wave of public shock, fear, and anger. The militancy of the Israeli public reached new heights. In a poll taken in April 2002, 71 percent of Israeli Jews agreed with the statement "every military action that Israel initiates is justified," and 80 percent believed that "all means are justified in Israel's war against terror."[130] It was in this climate of opinion that the Sharon government initiated two large-scale military operations in the West Bank (Operations "Defensive Shield" and "Determined Path"). These military offensives into the West Bank—in which Israel's military reoccupied large parts of the territory—received overwhelming support from the Israeli public.[131]

The massive Israeli public support for the construction of a security barrier between the West Bank and Israel was also a direct result of Palestinian terrorism during the second Intifada, as Israelis became desperate to find a way to stem the relentless tide of Palestinian suicide bombing attacks.[132] The idea of building a wall or fence to separate Israel from the Palestinian territories was not new, but it was Palestinian terrorist attacks that propelled the idea to the top of the political agenda. In October 2001, a new political movement called "Fence for Life" emerged with the aim of increasing public support for a security barrier.[133] The Israeli public enthusiastically embraced the idea of a security barrier between the West Bank and Israel. Faced with a steadily mounting civilian death toll from suicide bombing attacks, Israelis fervently hoped that such a barrier would at least greatly reduce the chances of successful suicide attacks by making it much harder for suicide bombers to enter Israel (not only would there be a high concrete wall or electrified fence for them to surmount, but also ditches, razor wire, electronic motion sensors and armed guard posts).[134] Growing public support for a security barrier eventually led the Sharon government in June 2002 to adopt the idea and announce its plans to begin building the barrier,[135] despite Prime Minister Sharon's initial opposition.[136]

Conclusion: Social Resilience and Coping with Terror

This article has discussed the different effects of terrorism and described how many of these effects occurred in Israel as a result of Palestinian terrorist attacks during the second Intifada. In doing so, it has sought to emphasize the many effects of terrorism—psychological, economic, social, and political. To

varying degrees, terrorism can affect the psychological health and well-being of a country's population, its economy, its societal beliefs and attitudes, and its politics. These effects can range from minimal to severe, depending on a host of other factors. In the case of Israel discussed here, Palestinian terrorism during the second Intifada had a profound and far-reaching impact upon Israeli society. The frequency of terrorist attacks, especially at the height of the second Intifada in 2002-2003, spread fear and anxiety among Israelis, hurt the Israeli economy, affected social attitudes and intra-societal relations, influenced Israeli public opinion and domestic politics, and the actions and policies of Israeli governments. Life in Israel was conducted under the shadow of terror during the years of the second Intifada—the most visible sign of this was the ubiquitous presence of armed security guards at the entrances of malls, retail stores, restaurants and cafes, who inspected people's bags and if necessary tried to prevent potential suicide bombers from entering these public spaces.

Given the many effects that Palestinian terrorism had on Israeli society during this period, one might conclude that it was highly effective. This is true in so far as it exacted a heavy toll on Israelis. But the purpose of terrorism is not just to kill people, inflict material damage, or frighten an audience. Terrorism seeks to alter the social and political dynamics of the societies it targets. In the words of one scholar, terrorism is "a form of psychological warfare against the public morale, whereby terrorist organizations, through indiscriminate attacks, attempt to change the political agenda of the targeted population."[137] One of the key objectives of terrorism, then, is to demoralize the targeted society—to induce a widespread sense of helplessness and hopelessness and feeling of despair among members of the society. If the targeted society does not become demoralized, terrorism fails in this respect.

By this criterion, Palestinian terrorism during the second Intifada was ineffective because it did not succeed in demoralizing the Israeli-Jewish public. While Israelis were certainly fearful of terrorist attacks, they did become despondent and dispirited.[138] Rather, Israelis demonstrated resolve and steadfastness in the face of relentless terrorism. Indeed, any visitor to Israel during the second Intifada could not help but be struck by the seemingly nonchalant manner with which Israelis

lived with the constant threat of terrorism. Instead of panic and public hysteria, there was stoicism and fortitude.[139] Israelis did not allow the threat of terrorism to dominate their lives. Although they experienced high levels of stress and fear, they went on with their lives. They did not retreat into their homes, nor did they significantly alter their daily routines.[140] Instead of allowing their lives to be seriously disrupted by terrorism, Israelis only made minor changes in their behaviour. They continued to go out to cafes, for example, but made sure that they sat far from the entrances where suicide bombers might blow themselves up if stopped by a security guard from entering. Those Israelis who regularly used public buses continued to do so,[141] others avoided buses that had been repeatedly targeted by terrorists, while some chose to take taxis instead. Although less people would go to restaurants and cafes or travel on public buses in the immediate aftermath of a terrorist attack (within the first few days), as time passed these activities would resume to normal levels.[142]

When one considers the huge toll in Israeli lives that Palestinian terrorism during the second Intifada took—from September 2000 until May 2004, 1030 people had been killed, and 5788 injured in more than 13,000 terrorist attacks, which means that approximately 0.1 percent of Israel's population was injured or killed (the same percentage in the United States would equate to a staggering 295,000 people being injured or killed)[143]—the ability of Israeli society to cope with this terrorism is quite remarkable.[144] How did Israelis cope with ongoing terrorism despite suffering enormously from it? There are no doubt many factors that are responsible for this, but three are particularly worth noting here. First, acclimatisation to chronic terrorism. In other words, Israeli society basically became accustomed to terrorism and adapted accordingly.[145] The threat of chronic terrorism simply became part of normal life in Israel during the second Intifada. Second, media attention to terrorist attacks declines during chronic terror—repeated terrorist attacks receive less television coverage and less television viewing. This occurred in Israel during the second Intifada.[146] Thus, since exposure to media coverage of terrorist attacks has been shown to generate symptoms of anxiety and distress,[147] as the media pays less attention to terrorism, this helps the society to become less affected by it. Finally, and most importantly, social resilience got stronger. Resilience is a

characteristic of both individuals and societies. Like individual resilience, social resilience involves the "ability to withstand adversity and cope effectively with change."[148] Thus, with regards to terrorism, social resilience prevents terrorism from seriously disrupting the normal functioning of a society. It means that a targeted population is able to cope with the threat of terrorism and not be intimidated or demoralized by it. The concept of social resilience, therefore, helps explains why Israeli society was not demoralized by repeated terrorist attacks, despite the serious affects these attacks had on Israelis. Israeli-Jewish society demonstrated a high level of social resilience during the second Intifada.[149] One factor that contributes to social resilience is social cohesion.[150] Israeli-Jewish society is still very cohesive, notwithstanding its serious political, cultural, and social divisions. There is a strong sense of social solidarity among Israeli Jews. Although this sense of solidarity has declined over the years, it rises during times of external conflict (as mentioned earlier, this occurred during the second Intifada). Hence, war and terrorism bolster social cohesion in Israel, which helps it to cope with these violent episodes. Social trust is another factor behind social resilience.[151] In Israel's case, the high level of trust that Israeli Jews have in the country's army and security services boosts their social resilience. During the second Intifada, the Israeli-Jewish public had confidence in the Israeli military and believed that quick and effective actions were being taken against Palestinian militant groups that were carrying out terrorist attacks (at least during the tenure of the Sharon government). In this respect, Israel's counter-terror actions helped prevent Israeli society from becoming demoralized. Finally, Israelis Jews are very patriotic[152]—this is most apparent in their high level of willingness to perform military service—which also contributes to their social resilience.[153]

In sum, the case of Israel during the second Intifada suggests that societies can become inured to prolonged terrorism and that the more resilient a society is, the less it will be demoralized by terrorism. Although terrorist attacks do succeed in causing mass fear and anxiety, they do not necessarily undermine a society's morale and willpower. Terrorism tests a society's unity and resolve. Israeli society essentially passed that test in the second Intifada due to its social resilience. As such, it offers a useful example that other societies faced

CBRNE Terrorism Newsletter – Winter 2011

with the threat of terrorism can potentially learn from. Whether the case of Israel is typical or exceptional of societies living with chronic terrorism should be the subject of further study. Future research should also be devoted to exploring the causes of social resilience and ways of strengthening it.[154] Understanding social resilience has important implications for how we think about terrorism and how we deal with it. It may even ultimately help us to win the 'war on terror' that we are currently engaged in—not because we stop all terrorist attacks (perhaps an impossibility), but because we are not greatly affected by them.

Notes

[1] This article adopts the U.S. State Department's definition of terrorism as "premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents, usually intended to influence an audience," see <http://www.state.gov/s/ct/rls/crt/2000/2419.htm>. This definition is consistent with that used by many scholars of terrorism. See, for example, Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 2006); Walter Reich (ed.), *Origins of Terrorism* (New York: Cambridge University Press, 1990).

[2] See for instance John Mueller and Mark G. Stewart, "Hardly Existential: Thinking Rationally about Terrorism," *Foreign Affairs*, April 2, 2010.

[3] For a history of terrorism see, Walter Laqueur, *A History of Terrorism* (New York: Transaction, 2001).

[4] Not surprisingly, it has been found that a terrorist attack can result in high levels of stress and anxiety. See Schlenger et al., "Psychological Reactions to Terrorist Attacks – Findings from the National Study of Americans' Reactions to September 11," JAMA 288, no. 5 (2002): 581-88; Schuster et al., "A National Survey of Stress Reactions after the September 11, 2001, Terrorist Attacks," *New England Journal of Medicine* 345, no. 20 (2001): 1507-12.

[5] See, for example, Avraham Bleich, Marc Gelkopf, and Zahava Solomon, "Exposure to terrorism, stress-related mental health symptoms, and coping behaviors among a nationally representative sample in Israel," *Journal of the American Medical Association* 290, no. 5 (2003): 612-620.

[6] Leonie Huddy et al., "The Consequences of Terrorism: Disentangling the Effects of Personal and National Threat," *Political Psychology* 23, no. 3 (2002): 485-509.

[7] See for example, Daniel Bar-Tal and Daniela Labin, "The Effect of a Major Event on Stereotyping: Terrorist Attacks in Israel and Israeli Adolescents' Perceptions of Palestinians, Jordanians and Arabs," *European Journal of Social Psychology* 31, no. 3 (2001): 265 – 280. See also, Daniel Bar-Tal and Keren Sharvit, "Psychological Foundations of Israeli Jews' Reactions to Al Aqsa Intifada: The Role of the Threatening Transitional Context," in V. M. Esses and R. Vernon, eds., *Why neighbors kill: Explaining the breakdown of ethic relations* (Montréal: McGill-Queen's University Press, 2004).

[8] See Agustin Echebarria-Echabe and Emilia Fernandez-Guede, "Effects of terrorism on attitudes and ideological orientation," *European Journal of Social Psychology* 36 (2006): 259–265.

[9] See for example, Bruno S. Frey et al., "Calculating Tragedy: Assessing the Costs of Terrorism," Cesifo Working Paper No. 1341, November 2004; Nadav Morag, "The Economic and Social Effects Of Intensive Terrorism: Israel 2000 – 2004," *The Middle East Review of International Affairs* 10, no. 3 (2006); Rafi Eldor and Rafi Melnick, "Financial Markets and Terrorism," *European Journal of Political Economy* 20, no. 2 (2004): 367-86.

[10] See for example, Christopher Hewitt, "Terrorism and public opinion: A five country comparison," *Terrorism and Political Violence* 22, no. 2 (1990): 145-170; Theodore Downes-Le Guin and Bruce Hoffman, *The Impact of Terrorism on Public Opinion - 1988 to 1989* (Santa Monica, CA: Rand, 1993); Huddy et al., "Trends: Reactions to the Terrorist Attacks of September 11, 2001," *Public Opinion Quarterly* 66, no. 3: 418-450.

[11] See for example, Claude Berrebi and Esteban F. Klor, "On Terrorism and Electoral Outcomes: Theory and Evidence from the Israeli-Palestinian Conflict," *Journal of Conflict Resolution* 50, no. 6 (2006): 703-23.

[12] See for example, Andrew Kydd and Barbara F. Walter, "Sabotaging the Peace: The Politics of Extremist Violence," *International Organization*, 56 (2002): 263–296.

[13] For the argument that terrorism works see: Robert A. Pape, "The Strategic Logic of Suicide Terrorism," *The American Political Science Review* 97, no. 3 (2003): 343-361; and Pape, *Dying to Win: The Strategic Logic of Suicide Terrorism* (New York: Random House, 2005).

[14] For the argument that terrorism does not work, see: Max Abrahms, "Why Terrorism Does Not Work," *International Security* 31, no. 2 (2006): 42–78.

[15] Seymour Spilerman and Guy Stecklov, "Societal Responses to Terrorist Attacks," *Annual Review of Sociology* 35 (2009): 167-89.

[16] For an analysis of the causes of the second Intifada see, Jeremy Pressman, "The Second Intifada: Background and Causes of the Israeli-Palestinian Conflict," *Journal of Conflict Studies* (Fall 2003): 114-141. For a detailed history of the second Intifada see, Amos Harel and Avi Issacharoff, *The Seventh War: How We*

Won and Why We Lost the War with the Palestinians (Tel Aviv: Yediot Ahronot and Hemed Books, 2004) [Hebrew].

[17] Although the second Intifada had no clear, definitive end, many analysts consider it to have ended in early 2005 after Mahmoud Abbas was elected President of the Palestinian Authority in January of that year (after Yasser Arafat's death) and he then made a truce with Israel at a summit meeting in February 2005.

[18] Israel Ministry of Foreign Affairs, "Four Years of Conflict: Israel's war against terrorism," available at http://www.mfa.gov.il/MFA/Terrorism-+Obstacle+to+Peace/Terrorism+and+Islamic+Fundamentalism-/Four+Years+of+Conflict+3-Oct-2004.htm>.

[19] Reuven Erlich, "The Battle for Hearts and Minds: The ongoing Israeli-Palestinian confrontation as a case study," 14 February 2006, Intelligence and Terrorism Information Center <http://www.intelligence.org.il/eng/eng_n/pdf/i_p_conflict_e.pdf>.

[20] Compared with the Second Intifada, the First Palestinian Intifada (1987-1993) was much less lethal for Israeli civilians, with 100 Israeli civilians killed in Israel and the Occupied Territories, according to figures compiled by the Israeli human rights organization B'Tselem, <http://www.btselem.org/statistics/first_intifada_tables>. Accessed on 21 November 2011.

[21] It is worth noting that in this same period, more than 3,000 Palestinians (combatants and non-combatants) were killed by Israeli security forces in the West Bank and Gaza. See, <http://news.bbc.co.uk/2/hi/middle_east/3694350.stm>. Accessed on 17 March 2008.

[22] Malcolm Sutton, "An Index of Deaths from the Conflict in Northern Ireland," <http://cain.ulst.ac.uk/sutton/tables/Status.html>. Accessed on 19 March 2008.

[23] For an analysis of the Palestinians' use of suicide terror attacks during the second Intifada and Israel's efforts to stop them see, Yoram Schweitzer, "The Rise and Fall of Suicide Bombings in the Second Intifada," *Strategic Assessment* 13, no. 3 (October 2010): 39-48.

[24] Ariel Merari, "Israel Facing Terrorism," *Israel Affairs* 11, no. 1 (January 2005): 227-228.

[25] Assaf Moghadam, "Palestinian Suicide Terrorism in the Second Intifada: Motivations and Organizational Aspects," *Studies in Conflict & Terrorism* 26 (2003): 65-92.

[26] On Palestinian popular support for suicide terror attacks against Israelis see, Mia M. Bloom, "Palestinian Suicide Bombing: Public Support, Market Share, and Outbidding," *Political Science Quarterly* 119 (Spring 2004): 61–88;

[27] Quoted in Daniel Byman, *A High Price: The Triumphs and Failures of Israeli Counterterrorism* (New York: Oxford University Press, 2011), p. 131.

[28] Schweitzer 2005, 42-43.

[29] Psychological effects are limited to those that affect individuals, not society as a whole. For example, stress is a psychological effect, while xenophobia belongs in the social category.

[30] Bleich et al. 2003, 11.

[31] Martha Crenshaw, "Introduction: Reflection on the Effects of Terrorism," in Martha Crenshaw, ed., *Terrorism, Legitimacy and Power: The Consequences of Political Violence* (Middletown, CT: Wesleyan University Press, 1983), p.1.

[32] Hoffman 2006, 142.

[33] Boaz Ganor, "Israel's Counter-Terrorism Policy: 1983-1999 Efficacy versus Liberal Democratic Values," unpublished Ph.D. Dissertation, Hebrew University, 2002, 15.

[34] Part of the reason has to do with the disproportionate coverage terrorism receives in the media. See Hoffman 2006, 189.

[35] Huddy et al. 2005, 499.

[36] Ariel Merari and Nehemia Friedland, *Memorandum: Public Positions on Terrorism*, Tel Aviv, 1980 (Hebrew). Cited in Merari, "Israel Facing Terrorism": 228.

[37] Asher Arian, *Security Threatened: Surveying Israeli Opinion on Peace and War,* Tel Aviv, 1999, pp. 72-73 (Hebrew). Cited in Merari, "Israel Facing Terrorism": 228.

[38] Bar-Tal and Shavrit 2004, 15.

[39] Bleich et al. 2003, 6.

[40] Ibid. 9.

[41] Ibid. 10.

[42] Ibid. 10.

[43] According to the Anxiety Disorders Association of America, PTSD is "a condition that results from experiencing or witnessing an unusually distressing event; symptoms range from repeatedly reliving the trauma, such as in dreams or flashbacks, to general emotional numbness, which often causes sufferers to withdraw from family and friends." Anxiety Disorders Association of America <http://www.adaa.org/gettinghelp/glossary.asp>. Accessed on March 4, 2008.

[44] Ami Pedahzur, *Suicide Terrorism* (Cambridge: Polity Press, 2005), 183.

[45] Morag 2006.

[46] Bleich et al. 2003, 11. It is also possible that there is a gender bias in the reporting of these disorders.

[47] David Eshel, "Post-Traumatic Stress in Emergency Rescue Teams: The Israeli Experience," *Journal of Homeland Security* (February 2003).

[48] Ibid.

[49] Huddy 2002, 496.

[50] Bleich et al. 2003, 10.

[51] Ibid. 9.

[52] Alan Kirschenbaum, "Surviving Terror Threats through Adaptive Behaviors: The Israeli Experience," paper presented at European Sociological Association Conference, Torun, Poland, September 9-12, 2005, p.15.

[53] Bleich et al. 2003, 10.

[54] Strong social support networks may also have been responsible for the relatively low level of PTSD among Israelis. Peter Roy-Byrne, "Effects of Terror and Violence Vary by Culture," *Journal Watch Psychiatry* (October 8, 2003).

[55] Asaf Zussman, Noam Zussman and Dmitri Romanov, "Does Terrorism Demoralize? Evidence from Israel," *Economica* (2010): 1-16.

[56] Ibid, 3.

[57] Two recent studies have demonstrated the psychological resilience of populations in the aftermath of terrorist attacks. George A. Bonanno et al., "Psychological Resilience After Disaster: New York City in the Aftermath of the September 11th Terrorist Attack," *Psychological Science* 17, no. 3: 181-186; and Juan J. Miguel-Tobal et al., "PTSD and depression after the Madrid March 11 train bombings," *Journal of Traumatic Stress* 19, no. 1 (2006): 69-80.

[58] Stevan E. Hobfoll et al., "Trajectories of Resilience, Resistance, and Distress During Ongoing Terrorism: The Case of Jews and Arabs in Israel," *Journal of Consulting and Clinical Psychology* 77, no. 1 (Feb 2009): 138-148; and Avi Besser and Yuval Neria, "PTSD symptoms, satisfaction with life, and prejudicial attitudes toward the adversary among Israeli civilians exposed to ongoing missile attacks," *Journal of Traumatic Stress* 22, no 4: 269-275.

[59] <http://www.israeltrade.org.au/israel_agrifood_July2004.htm>, accessed on March 8, 2008.

[60] Morag 2006.

[61] Ibid.

[62] According to one study, in the period from 2000-2003, terrorism was responsible for a ten percent reduction in per capita production in Israel. Zvi Eckstein and Daniel Tsiddon, "Macroeconomic consequences of terror: theory and the case of Israel," *Journal of Monetary Economics* 51, no. 5 (2004): 971-1002.

[63] Morag 2006. - Although the slowdown of the Israeli economy in the first two years of the Intifada coincided with the weakening of the economies of Israel's main trading partners, the United States and the European Union (EU), the economic slowdown of the Israeli economy was much greater than America's or the EU's, suggesting that the Israeli economy experienced a shock from the onset of the second Intifada.

[64] Ibid.

[65] Frey et al. 2004, 11.

[66] Morag 2006. It must be noted that during the same time period, global FDI fell from $1.388 trillion to $560 billion. The second Intifada was therefore certainly not the only reason for the sharp decline in FDI flowing into Israel.

[67] Ibid. 499.

[68] Frey et al. 2004, 6.

[69] Morag 2006.

[70] See for instance, Alberto Abadie and Javier Gardeazabal, "The Economic Cost of Conflict: A Case Study of the Basque Country," *American Economic Review* 93 (2003), 113-132.

[71] Keren Sharvit et al., "Jewish-Israeli attitudes regarding peace in the aftermath of terror attacks: the moderating role of political worldview and context"; paper presented at the annual meeting of the Israeli Sociological Society, Tel-Hai, Israel, 2005, 3.

[72] Sharvit et al., 4.

[73] Bar-Tal and Labin 2001, 6.

[74] Bar-Tal and Shavrit 2004, 17.

[75] Katrina Mosher, "Public Interpretations and Reactions to Terror Related Casualties: The Effects of Numbers and Identities," paper presented at the annual meeting of the International Studies Association, Hawaii, 2005, 16.

[76] Bar-Tal and Shavrit 2004, 15.

[77] Ibid. 16.

[78] Huddy et al. 2005, 486.

[79] Shavrit et al. 2005, 4.

[80] Pedahzur 2005, 185.

[81] Echebarria-Echabe and Fernandez-Guede 2006, 263.

[82] Bar-Tal and Shavrit 2004, 2.

[83] Huddy et al. 2005, 386.

[84] Pedahzur 2005, 184.

[85] Tamar Hermann, "Tactical Hawks, Strategic Doves: The Positions of the Jewish Public in Israel on the Israeli-Palestinian Conflict," *Strategic Assessment*, 5, no. 2 (Aug 2002).

[86] David Landau, "Carpe diem," *Ha'aretz*, 6 April 2001.

[87] In 2003, two-thirds of Israeli Jews felt that Palestinian Israelis were disloyal to the state. Asher Arian, *Israeli Public Opinion on National Security 2004* (Tel Aviv: Jaffee Center for Strategic Studies, October 2003), 34.

[88] Nearly two-thirds of Israeli Jews saw Israeli Arabs as a security threat in 2001, and over 70 percent did so in 2002. Nadim Rouhana and Nimer Sultany, "Redrawing the Boundaries of Citizenship: Israel's New Hegemony," *Journal of Palestine Studies* 33, no. 1 (2003): 15.

[89] In 2002, these figures were 53 percent and 31 percent, respectively. Arian, *Israeli Public Opinion on National Security 2004*, 30.

[90] Oren Yiftachel, "The Shrinking Space of Citizenship: Ethnocratic Politics in Israel," *Middle East Report*, no. 223 (2002): 40-41.

[91] See, "Intolerance and Discrimination against Muslims in the EU: Developments since September 11," report by the International Helsinki Federation for Human Rights, Vienna, Austria, 2005; Council on American-Islamic Relations, *The Status of Muslim Civil Rights in the United State*s (Washington DC, 2006). Accessed at <http://www.cair.com/pdf/2007-Civil-Rights-Report.pdf>.

[92] Sami Miaari, Asaf Zussman, and Noam Zussman, "Labor Market Segregation in the Shadow of Conflict," unpublished manuscript, Hebrew University, November 2007.

[93] For these attitudes see, Sammy Smooha, *An index of Jewish-Arab relations in Israel* (Haifa: Haifa University, 2005). See also, Daphna Canetti-Nisim, Gal Ariely, and Eran Halperin, "Life, Pocketbook, or Culture: The Role of Perceived Security Threats in Promoting Exclusionist Political Attitudes toward Minorities in Israel," *Political Research Quarterly* 61 **(**2008): 90-103.

[94] Shimon Shamir, "The Arabs in Israel – Two Years after the Or Commission Report," Tel Aviv University, Konrad Adenauer Program for Jewish-Arab Cooperation, 2006.

[95] Simha Landau, "Societal Costs of Political Violence: The Israeli Experience," *Palestine-Israel* Journal 10, no. 1 (2003): 28-35.

[96]Ibid, 34.

[97] American Psychological Association, "Stress and Aggression Reinforce Each Other at the Biological Level," 5 October 2004, <http://biopsychiatry.com/aggression/index.html>. Some sociologists have also pointed to the link between stress and aggression; see for instance Arnold S. Linsky, Ronet Bachman, and Murray Straus, *Stress, Culture, and Aggression* (New Haven: Yale University Press, 1995).

[98] This is also suggested by a study that found that fatalities from traffic accidents in Israel increased in the days after a terrorist attack. Guy Stecklov and Joshua R. Goldstein, "Terror attacks influence driving behavior in Israel," *Proceedings of the National Academy of Science* 101, no. 40 (2004): 14551-56; Guy Stecklov and Joshua R. Goldstein, "Societal Responses to Endemic Terror: Evidence from Driving Behavior in Israel," *Social Forces* 88, no. 4 (June 2010): 1859-1884.

[99] Pedahzur 2005, 184.

[100] For "system justification theory," see John T. Jost et al., "A Decade of System Justification Theory: Accumulated Evidence of Conscious and Unconscious Bolstering of the Status Quo," *Political Psychology* 25, no. 6 (2004): 881-917.

[101] Echebarria-Echabe and Fernandez-Guede 2006, 263.

[102] "Palestinians believe armed struggle led to pullout," *Associated Press*, 12 September 2005.

[103] Jonathan Rynhold and Dov Waxman, "Ideological Change and Israel's Disengagement from Gaza," *Political Science Quarterly* 123, no. 1 (2008): 1-27.

[104] For the role of public opinion in influencing recent Israeli government policy toward the conflict with the Palestinians see, Jacob Shamir, *Public Opinion in the Israeli-Palestinian Conflict: From Geneva to Disengagement to Kadima and Hamas* (Washington DC: United States Institute of Peace, 2007).

[105] Michael Ignatieff, *The Lesser Evil: Political Ethics in an Age of Terror* (Edinburgh: Edinburgh University Press, 2005), 58.

[106] Shavrit et al. 2005, 5. See also, Asher Arian, "Opinion Shifts among Israeli Jews, 1987-2004," *Palestine-Israel Journal* 11, no.4 (2005): 83-84.

[107] R. E. Petty and J. A. Krosnick, eds., *Attitude strength: Antecedents and consequences* (Hillsdale, NJ: Lawrence Erlbaum Associates 1995), cited in Shavrit et al. 2005, 6.

[108] Ibid. 4.

[109] The collapse of the Oslo peace process, especially the failure of the July 2000 Camp David summit meeting between Barak and Arafat, and the way this failure was publicly interpreted and 'framed' by Prime Minister Barak also had very important influences on Israeli public opinion. Eran Halperin and Daniel Bar-Tal, "The fall of the peace camp in Israel," *Conflict and Communication Online* 6, no. 2 (2007).

[110] Bar-Tal and Shavrit 2004, 18.

[111] A public opinion poll carried out by the School of Education at Tel Aviv University showed that it was the violence that broke out in September 2000 far more than the failure at Camp David that eroded Israeli faith in the peace process. Akiva Eldar, "The revolutionary road to 194," *Ha'aretz*, July 22, 2002.

[112] In a poll taken at the end of January 2001, 54 percent of Israeli Jews responded that they did not believe that the Oslo peace process would bring about peace between Israel and the Palestinians in the coming years. Yaar and Hermann, "Peace Index – January 2001."

[113] Bar-Tal and Shavrit 2004, 14.

[114] "Statement by Prime Minister Ehud Barak, Jerusalem, October 7, 2000," <http://www.mfa.gov.il/MFA/Government/Speeches+by+Israeli+leaders/2000/Statement+by+Prime+Minister+Ehud+Barak+-+07-Oct-20.htm>.

[115] The Peace Index survey from March 2001 conducted by the Tami Steinmetz Center at Tel Aviv University. Reported in *Ha'aretz*, April 4, 2001.

[116] Asher Arian, *Israeli Public Opinion on National Security 2002*, Memorandum No. 61, July 2002 (Tel Aviv: Jaffee Center for Strategic Studies, 2002), 10, 16-17.

[117] Sharon received 62.4 percent of the vote to Barak's 37.6 percent. This margin of victory—almost 25 points—was the largest in any Israeli election.

[118] For statistical evidence of the effect of terrorism on the political preferences of the Israeli electorate, see: Claude Berrebi and Esteban F. Klor, "Are Voters Sensitive to Terrorism? Direct Evidence from the Israeli Electorate," *American Political Science Review* 102, no. 3 (2008): 279-301.

[119] Berrebi and Klor have shown that terrorist attacks influenced Israelis to vote for right-wing parties, see Berrebi and Klor, "Are Voters Sensitive to Terrorism?"

[120] Shamir, *Public Opinion in the Israeli-Palestinian Conflict*: 31-32.

[121] Yehuda Ben Meir and Olena Bagno-Moldavsky, "The Second Intifada and Israeli Public Opinion," *Strategic Assessment* 13, no. 3 (2010): 75-76.

[122] Ibid, 77.

[123] Ibid, 74-75.

[124] Ibid, 77.

[125] Ibid, 83.

[126] Daphna Canetti-Nisim, "Militant Attitudes among Israelis throughout the al-Aqsa Intifada," *Palestine-Israel Journal* 11, nos.3-4 (2004/2005): 104-111.

[127] Asher Arian, *Israeli Public Opinion on National Security 2004* (Tel Aviv: Jaffee Center for Strategic Studies, October 2003), 29.

[128] Ephraim Yuchtman-Yaar, "The Oslo Process and Israeli-Jewish Public: A Story of Disappointment?" *Israel Studies Forum* 18, no. 1 (Fall 2002): 23.

[129] "Erased In A Moment: Suicide Bombing Attacks Against Israeli Civilians," *Human Rights Watch*, October 2002.

[130] Canetti-Nisim, 2004-05: 109.

[131] Operation "Defensive Shield" in March 2002 was supported by 90 percent of Israeli Jews. Bar-Tal and Shavrit 2004, 19.

[132] According to an opinion poll conducted in January and February 2004, 80 percent of Israelis supported building the security barrier. Arian, *Israeli Public Opinion on National Security 2004*.

[133] David Rudge, "New Movement Calls for Unilateral Separation from Palestinians," *The Jerusalem Post*, October 15, 2001.

[134] Some 63 percent of Israelis Jews believed that the barrier could significantly reduce the number of Palestinian terrorist attacks against Israel, and another 19 percent believed that it could stop terrorism altogether. Yaar and Hermann, "Peace Index – October 2003."

[135] Mazal Mualem, "Smart Fence, Stupid Politics," *Ha'aretz*, August 30, 2003.

[136] Sharon initially dismissed the idea of a security barrier as "populist." Amit Ben-Aroya, "Sharon: The Separation Fence is a Populist Idea," *Ha'aretz*, April 12, 2002.

[137] Ganor, 2.

[138] Zussman et al., "Does Terrorism Demoralize?"

[139] Nothing expresses this popular attitude better than the inscription on a memorial outside the site of one of the worst terrorist atrocities during the second Intifada (the Tel Aviv disco where 21 young people were killed)—"We won't stop dancing."

[140] The only time that daily life in Israel was seriously disrupted by terrorism was during the first few months of 2002 when suicide bombings were taking place in Israeli towns and cities every few days—there were five attacks within just ten days in March 2002 killing a total of 51 Israelis. During this period of unrelenting terrorist attacks, people avoided crowded places and stopped going out to cafes and restaurants. They didn't take buses or go shopping in malls. They stayed indoors. Palestinian terrorism was succeeding in terrorizing Israelis and disrupting their normal lives. However, this was short-lived. When the volume of terrorist attacks declined, life

CBRNE Terrorism Newsletter – Winter 2011

in Israel returned to normal.

[141] Gary S. Becker and Yona Rubinstein, "Fear and the Response to Terrorism: An Economic Analysis," Department of Economics, University of Chicago, working paper, February 2011.

[142] Ibid.

[143] Avraham Bleich et al, "Mental health and resiliency following 44 months of terrorism: a survey of an Israeli national representative sample," *BMC Med* 4 (2006), published online. Accessed 22 March 2008 <http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=1560155>.

[144] For more in-depth treatments of how Israelis have 'coped' with terrorism see, Ira Sharkansky, *Coping with Terror: An Israeli Perspective* (Lanham, MD: Lexington, 2003); Leonard A. Cole, *Terror: How Israel Has Coped and What America Can Learn* (Bloomington: Indiana University Press, 2007); and Nadav Morag, "Measuring Success in Coping with Terrorism: The Israeli Case," *Studies in Conflict and Terrorism* 28, no. 4 (2005).

[145] Alan Kirschenbaum, "Adapting Behaviors of Israeli Civilians to Palestinian Terror," in Nehemia Friedland et al., "The Concept of Social Resilience," Samuel Neaman Institute for Advanced Studies in Science and Technology, Working Paper, December 2005, 36-82.

[146] Tamar Liebes and Zohar Kampf, "Routinizing Terror: Media Coverage and Public Practices in Israel, 2000-2005," *Harvard International Journal of Press/Politics* 12, no. 1 (2007): 108-116.

[147] Michelle Slone, "Responses to Media Coverage of Terrorism," *Journal of Conflict Resolution*, 44 (2000): 508-522.

[148] Nehemia Friedland, "The Elusive Concept of Social Resilience," in Friedland et al. 2005, 8.

[149] For a detailed examination of the resilience of Israeli society during the second Intifada see, Meir Elran, "Israel's National Resilience: The Influence of the Second Intifada on Israeli Society," (Tel Aviv University Jaffee Center for Strategic Studies, Working Paper No. 81, January 2006) [Hebrew]. See also the "National Resilience Project" conducted by the Center for the Study of National Security at the University of Haifa, which uses regular surveys of the Israeli public to measure its national resilience over time.

[150] Gabriel Ben-Dor et al., "The Social Aspect of National Security: The Impact of Terror on Israeli Society," unpublished paper (2007).

[151] Ibid.

[152] "Patriotism survey: 88% proud to be Israeli," *Ynet*, January 29, 2009.

[153] Ben-Dor et al.

[154] Social resilience can be increased through deliberate efforts and advance planning. For possible measures to enhance social resilience see: Meir Elran, "Benchmarking Civilian Home Front Resilience: Less than meets the Eyes," in Shlomo Brom and Anat Kurtz, eds., *Strategic Survey for Israel 2010* (Tel Aviv: Institute for National Security Studies, 2010): 75-77.

Dov Waxman *is an associate professor of political science at Baruch College and the Graduate Center of the City University of New York. He specializes in International Relations, Middle East politics, Israeli politics, and Israeli-Palestinian relations. He received his Ph.D. in International Relations from Johns Hopkins University's School of Advanced International Studies, where he also received an M.A. in International Relations and International Economics. He has a B.A. degree in Politics, Philosophy and Economics from Oxford University. He has been a visiting fellow at the Begin-Sadat Center for Strategic Studies at Bar-Ilan University in Israel, a visiting scholar at the Middle East Technical University in Ankara, Turkey, and a visiting fellow at the Moshe Dayan Center for Middle Eastern and African Studies at Tel Aviv University, Israel. He is the author of The Pursuit of Peace and the Crisis of Israeli Identity: Defending / Defining the Nation (Palgrave Macmillan, 2006), and the co-author of Israel's Palestinians: The Conflict Within (Cambridge University Press, 2011).*

What Have We Learned about Lone Wolves from Anders Behring Breivik?

By Raffaello Pantucci

Source: http://www.terrorismanalysts.com/pt/index.php/pot/article/view/what-we-have-learned/html

Abstract

Anders Behring Breivik's massacre on July 22, 2011 showed the danger that a well-organized Lone Wolf could cause. The methodical and calculated way with which he

CBRNE Terrorism Newsletter – Winter 2011

prepared and justified his act awoke security services the world over as to the potential menace that this form of terrorism can pose. As they revise their strategies, this article casts a preliminary eye on the case using a particular Lone Wolf prism of analysis to try to see what lessons can be learned from the case. Drawing on Breivik's own writing and public sources, the article analyses his biography, the ideology he used to justify his act, the degree to which he seems to have been connected to others, his effectiveness, what role the Internet played and his mental competence all to try to draw some early lessons from the case. In concluding it offers some possible lessons learned that might offer practitioners some ideas of how to counter this sort of a threat in the future.

Introduction

Anders Behring Breivik's heinous massacre in Oslo cast a light once again on the dangers and potential dangers posed by 'Lone Wolf' or 'Lone/Solo Actor' terrorists.[1] Governments and security agencies have to reconsider their counter-terrorism approaches to try to figure out how it is possible to counter or detect such individuals. This article will examine what lessons can be drawn at this early stage from Norway's experience with Breivik that may be applicable or relevant for future planning.

Before proceeding, a caveat must be included to state that at this stage many details are still unknown. It seems clear that Anders Behring Breivik was responsible for the atrocities in Oslo and he has admitted as much, but a court case is still underway.[2] However, it is still possible to draw some early conclusions to understand him and the broader phenomenon better. Using a structure first laid out in the ICSR paper "A Typology of Lone Wolves: Preliminary Analysis of Lone Islamist Terrorists,"[3] this short article seeks to apply some of the lessons from there to Anders Behring Breivik before drawing some conclusions that might be useful from the perspective of trying to counter such individuals in the future. Admittedly, any recommendations are drawn from a very limited dataset, but analyzing an individual as effective as Breivik in a methodological manner is doubtless useful in preventing such acts in the future.

Biography

The first point in understanding Breivik as a Lone Wolf is to understand his personal biography. Unless otherwise indicated much of Breivik's information is taken from his self-published

manifesto, "2083: A European Declaration of Independence" that is available online.

Anders Breivik appears to have come from a broken home, though it does not seem to have been an outwardly traumatic experience. Born in London in 1979 to an economist at the Norwegian Embassy and a nurse, Breivik's parents split up a year after he was born. He moved back to Norway with his mother, while his father moved to Paris and re-married (it appears to have been his father's third marriage). According to Norwegian contacts, Breivik lived in a relatively affluent area though was not in an affluent household himself. Breivik reports making a number of visits to his father in Paris, but these slowly faded over time.[4] He claims his father cut off contact when he was fifteen years old (he says his father was not happy with 'his graffiti phase' when he was 13-16) and when Breivik tried to get back in touch was told that, 'he [his father] was not mentally prepared for a reunion due to various factors, his poor health being one.' Nevertheless, Breivik is clearly fixated by a patriarchal society, dedicating a section of his screed to defining it and its importance.

In 2006, he decided to move back in with his mother in an attempt to save money, though he seems to have been paying rent to her. He is quite cold to her in his 'compendium', saying that she 'was infected by genital herpes by her boyfriend (my stepfather) when she was 48,' something brought on by her 'lack of good judgment and moral[s].' This sense of revulsion towards his mother was something that she later reported him reacting on in person as well, accusing her of infecting him and wearing an antiseptic mask around the

house.[5] He also says his sister has suffered from venereal diseases due to her loose morality and described them both as having 'not only shamed me but they have shamed themselves and our family.' Both of his parents have been quoted as being shocked at their son's actions and his father in particular said his son 'should have committed suicide' after his act.

Breivik describes his teenage years as ones where he was popular and dabbled in what he calls the 'hip-hop movement,' meaning graffiti communities and rap music culture. This led to some clashes with police and community services. However, by the time he was sixteen, he claims to have noticed that his peers in this movement were failing academically and he abandoned them to focus on his schoolwork. This account was disputed by friends quoted in the press who denied he was as successful or popular as he claimed and that while he did get into some trouble with the police for his involvement in graffiti gangs he got out of it by informing on friends.[6]

At around this time he claims to have fallen out with Arsalan, his close Pakistani Muslim friend whom apparently told another person to punch Breivik for 'no reason.' This attack is the second he records from his youth by Muslims and seems to be something of a breaker in his mind. According to Arsalan's father quoted in the press, this account does not accord with the facts and the two of them (Arsalan and Breivik) were only friends at primary school.[7]

Two other claims from his personal biography about his youth are that at age 15 he chose to be baptized and confirmed in the Norwegian State Church and that he avoided military service at age 18 'because I didn't feel any loyalty to the ruling political parties.' Neither have been verified or denied in the press.

He appears to have maintained an interest in politics throughout his late childhood. At 16-17, he says he joined the Progress Party Youth Organization (FpU) who were 'anti-immigration and free-market.' But he seems to have rapidly become disillusioned with political parties in Europe and by 2000 'realized that the democratic struggle against the Islamisation of Europe, European multiculturalism was lost.' By his own account, it was his government's involvement in the attacks on Serbia (NATO bombings in 1999) that 'tipped the scales.' However, he continued to be involved with mainstream politics and in 2003 claims to have been a candidate for the Oslo City Council on behalf of the Oslo Progress Party. He was also on the board of a local school and retirement home, both of which he claims were political positions he chose to bolster his candidature.[8]

By the early 2000s he had concluded what he wanted to do with his life ideologically (more on that in a later section), and apparently focused on making money to fund his cause. He worked as a 'mid level leader' in a customer service company while running his own outsourcing programming services company on the side. He claims this was so successful that by May 2003 he had quit his day job and focused on his company called 'E-Commerce Group' that had two employees in Norway, two in Russia, and one each in Romania and Indonesia. This was a success and by age of 24 he claims to have earned his 'first mill' in Norwegian Kroner. By 2005-2006, the economic recession hit and he shut the company down filing for bankruptcy after withdrawing what funds he could. He then says he spent three years focused on writing his 'compendium', while also playing World of Warcraft 'part-time' for the first 12-month period. He also admits to having lost considerable funds trying to play the stock market between 2005-2008.

In his 'compendium' he starts to keep a relatively regular diary in the autumn of 2009, during what he describes himself going into a 'phase shift.' In November 2009 he spends some time trying to help develop a newspaper, then he spends two months 'email farming.'[9] This is mostly a period of isolation, but he reports hanging out with friends and deceiving them about what he is up to with stories of being fixated with online games or letting rumors spread that he has a secret homosexual relationship. Living at home with his mother towards the

end of his operation, she reported that he became obsessive in talking about politics and history and displayed all sorts of paranoid behavior in the run up to the attack.[10]

Aside from his active interest in politics and his terrorist plotting, none of this is a particularly distinct public biography; by many accounts Breivik was a typical Norwegian boy who appears to have veered way off the path.

Analysis:

- Breivik came from broken home and had strained relationship with his father.
- He seems to have been obsessed with his mother as unclean (according to one report in the press, he described his mother as his 'Achilles heel' and a person who would make him very emotional)[11].
- Breivik encountered issues early in his career that sent him in a different direction. His career as a politician was squashed after he was defeated by a rival, leading him to abandon mainstream politics altogether.
- Breivik tried to work within the system but ended up being betrayed by it. Having worked and sought a position in political life from a young age, when he tried to graduate into a real political position, he was unable to.
- Nevertheless, Breivik was able to function seamlessly in society prior to his action.

Ideology

At this stage of the investigation, it looks like Breivik was acting alone (see below for more details on his connections), but he was driven to carry out, or attempt to carry out, an act of terror deploying a rationale that was dictated by an extremist ideology. Using what information is at this moment available, this section will explore what we currently understand about Breivik's ideology. Some caveat must be added here to say that this assessment might be confused by Breivik's 'insanity' ruling, but at the same time,

his ideology is worth analyzing given its complete and considered nature.

Much has been written in the press about Breivik's motivation for carrying out his heinous act. Most of this is drawn from his own supposed writings that appeared on the Internet in the hours prior to his attack on Oslo. The document is entitled "2083: A European Declaration of Independence" and is referred to throughout as a 'compendium'. Drawing heavily on online sources and websites (he is a particular fan of a number of prominent right-wing, anti-Muslim or anti-immigrant bloggers and writers), the document is a distillation of this information describing the battle Breivik sees in Europe between advancing hordes of Muslims and the indigenous Christian populations on the continent. Dotted with his own experiences, the vast majority of the document quotes others, with much of the rest made up of a detailed manifesto for what his perfect society and army should look like. He goes into particular detail providing future followers with an outline of how they should go about building bombs, weaponry and military equipment.

Breivik sees himself as a crusader warrior fighting for Christendom. He claims to be a member of a secret society that was "re-founded" in April 2002 in London under the name Pauperes Commilitones Christi Templique Solomonici (the poor fellow-soldiers of Christ and the Temple of Solomon, PCCTS) or more succinctly the Knights Templar or, as he continuously refers to himself, a "Justiciar Knight." In this medieval light, Breivik's concerns are focused around the growing Islamicisation of Europe and the 'cultural Marxism' that is allowing Europe to let itself get taken over by Islam.

At what point in his childhood Breivik developed his fixation with the Islamicisation of Europe is unclear, but in his own narrative he suggests that this moment may have come during his early teenage years when he claims to have had some Muslim friends. He describes how they start as friends, but as they grow older they drift away towards their own cultures and in some cases he describes how his ethnically

Norwegian friends got attacked and robbed by gangs of Muslim boys. He describes hearing stories of Norwegian girls being referred to as "whores" by the Muslim community and how one Pakistani he knew was part of a group who gang-raped an ethnically Norwegian girl in the mid-1990s and got away with it. He further describes how a number of Muslim girls he went to school with disappeared as their families sent them back home, fearing they had become "too Norwegian." These experiences seem to have had an impact on him from a relatively young age and his first political experiences (detailed above) were all with right-leaning parties that had strong anti-immigration platforms. Breivik is eager not to paint himself as a racist though, highlighting that "I have always been terrified of the prospect of being labeled as a racist, to such a degree that I have put significant restrictions on myself, not only verbally but concerning all aspects of my social image. And I know this is the case for a majority of Europeans. I would say I have allowed myself to be paralyzed by fear." He goes on to condemn neo-Nazi's and national socialists saying that they are either ignorant or that they are unreliable hooligans. In Breivik's eyes, he is different from these individuals as he sees himself as a defender of a European identity that is being overwhelmed by Muslim masses, rather than someone who despises anyone that is not of European stock like him.

Serbia plays an important role in Breivik's ideological formation. He stoutly declares that the NATO war on Serbia in 1999 was the "tipping point" for him to go in the ideological direction he went – though this is somewhat contradicted by the fact that he remained active in mainstream Norwegian politics for a number of years yet; something that suggests that he had not gone completely down the path of violence yet and something of a post-facto determination on his behalf. He claims that in 2002 he travelled to Monrovia, Liberia where he sought out an individual Serbian nationalist who was living there and he was obviously very impressed by him. At other points in the book he praises Radovan Karadic as a great man and lists him as one of

his most revered leaders. He sees the wider victimisation of Serbia within Europe as a fundamental part of Europe's surrender to Islam. There is also a strong strain of Christianity in his ideological framework. He reports choosing religion at age 15 and his imagery is all drawn from the Crusader canon. At one point in his journal, he admits praying, and admits to how long it had been: "I prayed for the first time in a very long time today. I explained to God that unless he wanted the Marxist-Islamic alliance and the certain Islamic takeover of Europe to completely annihilate European Christendom within the next hundred years he must ensure that the warriors fighting for the preservation of European Christendom prevail." This neatly summarizes the underlying ideology that Breivik ascribes to.

Most salient for the purposes of this article, however, is the heavy reliance in Breivik's text and ideology on the notion of the Lone Warrior, or as he defines them "solo martyr cells." Given the vanguard nature of the struggle he is fighting – he repeatedly highlights that people will probably hate him after his act – he recognizes the need for intense secrecy and of not trusting anybody. He even nods towards small cell structures that he calls "clandestine cells….it is not in any way lead under a fixed, fragile hierarchy but works as an extremely distributed movement, a resilient network made up of small, autonomous groups or cells. Each group is led by a cell commander, often working solo, who makes all the decisions based on fixed fundamental principles. We therefore avoid the use of electronic communications."

While this discussion is made within the context of laying out what he believes to be the structure of the resistance army he is part of should look like, he talks about his own experiences, highlighting the importance of this aspect to his ideological formation:

"I have never in my life felt that I have done anything more meaningful than what I am doing now regardless of the lack of moral support from my founding brothers

or other armed resistance fighters."

"I have managed to stay focused and highly motivated for a duration of more than 9 years now. I feel really happy about my current course."

"Learning the ability/rituals to motivate yourself and being able to follow this ritual on a daily basis is perhaps the most essential aspect of our armed resistance effort in phase 1."

All of the things he prepares for are individual acts, like self-interviewing himself or preparing himself for future media interviews he expects to give, "philosophizing", going for long walks, listening to motivational music.

"Becoming and maintaining the position as a self-sufficient Justiclas Knight sleeper cell involves the capability to motivate/indoctrinate yourself over a prolonged period of time. Self-financed and self-indoctrinated single individual attack cells, is the backbone of the Knights Templar Europe."

This is the archetypal lone wolf attacker of any ideological stripe, and the image he paints is undoubtedly the one that most concerns security planners when they are assessing the threat matrix.

What is intriguing about Breivik's narrative is the fact that he makes no mention of Louis Beam or Ulius Louis Amoss, the men who first laid out the notion of "leaderless resistance" that best provides a strategic framework within which to consider the strategy of Lone Wolf terrorism. While Beam advocates for small cell resistance, he does also mention individuals taking up arms by themselves. The correlation comes in the notion that the individual or small cells are going to be scattered around and out of contact with each other, and consequently need to act on their own – an approach that lends itself conveniently to individuals pursuing a path of Lone Wolf activity. It could be that he simply did not come across them – something that would be surprising given what an assiduous Internet user Breivik seems to have been. Or it could be that he did not want to be associated with Beam, a notorious racist leader of the Ku Klux Klan. At the same time, however, he could have simply referred back to Beam's source material, coming

from Amoss, a US intelligence officer who first coined the strategy as a final resort should communism successfully invade mainland America. This anti-communist message would have resonated with Breivik and it is curious that he did not use it.

Ideological Analysis:

- Religion plays a role in Breivik's life – while it is unclear whether he considers himself a holy warrior or rather the identity of a crusader is useful as an image of someone defending European identity (that happens to have religious connotations), he does see Islam and Muslims in Europe as opponents, something that highlights that religion is something that he focuses on.
- His teenage years were important in the formation of his religious identity: Breivik reports being baptized and confirmed at age 15.
- He is captivated by the global clash of cultures and ideologies that have been a defining feature of the past ten years – specifically through what he sees as the Islamicization of Europe.
- He further seems to have personally experienced the issues – he may discuss them quite breezily, but Breivik lists nine specific instances over a decade in which Muslim youths have attacked him, suggesting a quite strong personalized rage in reaction.
- Breivik is clearly in the ideological thrall of the anonymous older Serbian whom he apparently met in Monrovia. The fact he made such a long and expensive journey to meet him suggests previous contact as well.
- In Breivik's ideology he repeatedly paints himself as a lone vanguard and lone warrior and he seems to be content in this role.
- Yet at the same time, there is no clear evidence that

he was planning on dying in the course of his action. He continually accepts this is a possibility (at one point he says: "I know I will die fighting…and that's not a problem for me at all."), but he is also constantly preparing himself for what happens were he to be captured.[12]

- Breivik claims to have been thinking about his big plot for almost a decade, certainly his direct attack planning took over a year at least, with some time before that dedicated to ideological formation and raising of funds.

Connections

This element has been touched on to some degree in the ideology section, but within the context of him as a Lone Wolf it is important to highlight the exact extent of his connections and contacts.

Breivik appears to have operated on the fringes of an extremist community. Aside from being an active participant in online forums focused on far right or anti-Muslim views, he also appears to have been in contact at various points in his past with other individuals and groups operating on the far right fringe. When arrested, Breivik seems to have alternatively claimed that he was alone and that other cells existed that would follow his action. Subsequently, he maintained this story, claiming that "two more cells" were working with him.[13] However, at time of this writing there has been no evidence of this, suggesting that these other individuals either did not exist or that Breivik had overestimated their dedication to the cause that led him to carry out his act.

Nonetheless, Breivik's own treatise explaining his act offers a long list of individuals whom he claims to have had contact with, including a secretive network of "Justiciar Knights" with whom he was inducted into the reformed Pauperes Commilitones Christi Templique Solomonici (PCCTS). In his text he lists them as: two Britons, and single individuals from France, Germany, Holland, Greece, Russia, Norway,

Serbia – as well as a missing Swede, Belgian and European-American. Presumably Breivik is the Norwegian he is referring to. According to Breivik they met in London in April 2002 in separate groups of four founding members and a host as a precautionary security measure. Breivik reports that at 23 years old, he was the youngest one at the meeting. The groups were told not to stay in contact and to go away and "cut off contact indefinitely." One of the British men takes a mentor role with Breivik; he anonymises him by calling him "Richard." But aside from him and the Serbian living in Monrovia, it is unclear that Breivik knows the identities of the other participants. At one point Breivik reads a newspaper story about the theft of the "Arbeit macht frei" sign from the entrance to Auschwitz by a Swedish group, and wonders whether this might be a Swedish "sister cell" presumably formed around the Swedish individual. However, he dismisses this notion quickly though it is unclear whether this is because he knows the identity of the Swede or because it becomes clear it is a clumsy neo-Nazi effort.

For the most part, however, Breivik is very careful not to name people in his document out of a sense of operational security. Whether this is a genuine concern or whether he was delusional is unclear at this point, but there is some evidence that Breivik was in contact with British anti-Muslim extremists like the English Defence League (though Breivik does dismiss them as naïve in his writing). He appears to have attended some of their marches and was Facebook friends with a great many. He further seems to have quite a fixation with the United Kingdom – his chosen name was clearly British (maybe a nod to the fact he was actually born there), his mentor "Richard" was a Briton, he gave London as the dateline for his magnum opus (the 'compendium'), he expresses great anger at British political parties in particular in his text, and of course his indoctrination into the PCCTS took place in London. All of which sent security services in the UK off to busily track his contacts down,

suggesting as it did an active network in the UK.

As was highlighted before in the ideology section, however, it seems clear that Breivik was eager to paint himself as a lone warrior who was a single sleeper cell that was self-indoctrinated and planned over a period of nine years with minimal interaction with others. His own account of obtaining equipment suggests he did this by himself with no outside support. He is also meticulous in building cover stories for himself prior to purchasing items that are commonly available but could raise suspicions if bought abruptly and in large quantities. From an ideological standpoint some key meetings seem to have helped form his worldview, specifically his meeting in London in April 2002, though a number of key interactions appear to have taken place online as well.

Analysis of Possible Connections:

- Based on current information, Breivik was acting alone.
- He was, however, on the periphery of the far right and anti-Muslim ideological community in Europe with some links and interaction with such groups. He seems to have drawn some ideological sustenance from interactions with them, though he seems also to have concluded that they are not to be trusted with information and do not necessarily share his goals.
- He also seems to have believed he was part of a wider network that he does not appear to have much immediate interaction with or knowledge of where they are currently located.

Effectiveness

A key element of any terrorist plot or attack is the degree to which it is able to disseminate terror or chaos. Understanding how effective an attack is, or might have been, offers analysts a metric by which to classify a terrorist attack.

Breivik's attack was clearly a highly successful one. If reports in the press of his statements are to be believed, he himself was surprised at the

success he was able to achieve, expecting to be either captured or cut down in the wake of his bombing of Oslo's political heart. However, he was able to carry out a solo twin-attack with a grim efficiency at a cost of 77 lives. The attack itself was clearly planned far in advance (according to Breivik's own writing, he had started to formulate his plan almost nine years prior to action) and had the hallmarks of a clearly conceived and executed plan.

His operation had two phases to it, first a bombing in Oslo's political district; and second, a mass shooting on an island where the youth wing of the ruling Labor party was holding an annual conference. In a particularly cunning move, Breivik was dressed as a policeman when he arrived on Utoya Island where the aspirant politicians were staying, claiming in the first instance to have come to talk to them as a result of the bomb blast in Oslo. Having gathered some around him, he then opened fire, marching methodically around the island for almost an hour and a half shooting people as he found them. According to eyewitness reports from the island, he walked around and calmly shot individuals who were running away. He furthermore went around methodically shooting bodies he found on the ground suspecting, correctly, that some were individuals who were masquerading as dead to evade him. He appears to have attempted to lace his bullets with nicotine poison, though it is unclear how effective this was.

In preparing for his act, Breivik was careful both in obtaining the necessary weapons and bomb making materials without raising security officials concerns. One dubious chemical purchase he made from Poland in March 2011 did raise red flags, but at the same time, according to the head of the Norwegian intelligence service, there had not been enough evidence to investigate this further.[14] Breivik describes trying to go to Prague to purchase weaponry, a trip that was a failure and resulted in him instead utilizing legitimate avenues to purchase weaponry in Norway.

Analysis:

- Breivik is an example of what an effective lone wolf attack can look like.
- Breivik was meticulous in his long-term planning for every aspect of his operation. Having defined what he is going to do, he then goes about preparing for it building cover stories at every stage. If he is to be believed this was his focus for nine years, though it is likely that actual planning was conducted over a much shorter time period.
- Breivik appears to have been interested in utilizing chemicals to enhance the damage he inflicted, but it is unclear how successful he was in doing this.
- He was also very effective in using the Internet (as shown in next section) to establish a database of individuals who would read his text and maybe agree with parts of it and who would help further disseminate it. In this he appears to have been very successful.

The Internet

Often with Lone Wolves or Lone Actors, it is the Internet that acts as a catalyst or plays a supportive role in pushing the individual from radical thought into action. This plays out in a number of ways: lost individuals can find fellow believers through the Internet, networks can establish themselves over long distances without the individuals ever knowing each other and individuals seeking to conduct some malicious attack can find operational guidance and support using the Internet.

The Internet appears to have been a key tool for Breivik, both in ideological terms and operational terms. In the first instance, it seems clear that his treatise is based mostly upon research he conducted on the Internet, mostly trawling through right-wing and anti-Muslim forums. It has since been reported in the press that he was an active participant in discussions online, though other participants or moderators highlight that he did not particularly distinguish himself as being an extremist. In his 'compendium', Breivik mentions that he spends time online ideologically

guiding others in these discussions – clearly seeing himself as a more active participant. He seems particularly impressed with a blogger named Fjordman, though a number of other individuals appear regularly in his citation lists.[15]

In some cases, he appears to have tried to shift online interactions into real world ones. He claims to have tried to meet with Fjordman, but failed. He also says that he met a community of Serb conservatives online whom appear to have played a crucial part in his ideological formation. One is the unidentified Serb who lives in Monrovia, but he appears to have found a community online of such individuals who had a considerable influence upon him. So much so that he was willing to travel to Monrovia to meet the individual.

He also appears to have been quite innovative in his use of the Internet as a tool to obtain material and information to support his action. When planning his trip to Prague to buy weapons he used a Hyundai discussion forum for tips on how to make the trip from Oslo to Prague by car. He reports that alibaba.com, a Chinese website linking Chinese manufacturers to global retailers, is a particularly good source of chemicals and materials. He also used eBay and a number of sellers in the UK to purchase chemicals and tools.[16] He uses a wide array of different websites to locate different tools and to collect information on building bombs, chemical mixtures, ideal body armors to use and so on. In addition to using the Internet as a source of material, he claims to have raised much of the money he uses in his action through establishing companies whose business model is based around e-commerce.

The Internet not only plays a role in his information collection and fundraising, but also in information dissemination. He uses Facebook as a tool to locate ideological fellow travellers or potential supporters and spends considerable time 'email farming' by 'friending' individuals whom he believes hold views similar to his and then once they have accepted,

collecting their email addresses off their profiles. He creates two profiles to do this from and apparently uses up his daily allowance of 50 friend requests regularly in trying to gather this data. Presumably, he also does this through identifying individuals from his regular visits to far right or anti-Muslim websites and forums.

Finally, the Internet also appears to play a key role in his downtime. Breivik regularly admits to enjoying playing computer games, and in particular demonstrates a fixation with multiplayer role-playing fantasy games. At one point he admits that this was practically his entire occupation for a whole year.

As a modern man brought up in an Internet age, Breivik appears to have been very much at home using the Internet and was able to navigate ideology and operational information with ease. He repeatedly demonstrates a knowledge of Internet masking technology and at a number of points says that he destroys his hard drives to hide any evidence of what he is doing or of having security services somehow compromise him.

Analysis:

- There is evidence that Anders Breivik sought ideological and operational support online.
- Breivik demonstrated a high level of Internet savvy and capacity to mask his online activity.
- However, it was an online purchase from a foreign country that did put Breivik on Norwegian intelligence's radar.

Mental Competence

A further complicating factor when looking at Lone Wolves or Lone Actor terrorists is how to separate and distinguish them from those individuals who for their own perverse reasons decide to open fire on crowds of random foreigners. What is the distinct feature of individuals who are motivated by an ideology to carry out a terrorist attack versus individuals who launch mindless orgies of violence due to some chemical imbalance? This is a difficult line to

draw and this author is conscious of the deficiencies in his own analysis in this aspect. In an earlier paper, this author concluded with the possibility that some sort of social inadequacy and general sense of alienation from society might leave an individual prone to going to seek radical ideas that might in turn lead to terrorism.[17] Following this line of analysis and the subsequent official Norwegian report that seemed to indicate Breivik may have been mentally unstable, this section will analyze the degree to which at this point the individual's mental competence has been called into question or issues have been highlighted.

Breivik's sanity has been questioned by his own lawyer. And an early assessment by Norwegian professionals concluded that it was unlikely he is going to be declared legally insane given how hard it would have been for someone insane to carry out an act with such methodological effectiveness.[18] However, a subsequent psychological evaluation did conclude that "Anders Behring Breivik during a long period of time has developed the mental disorder of paranoid schizophrenia, which has changed him and made him into the person he is today....[they uncovered] grandiose delusions whereby he believes he is to determine who is to live and who is to die."[19] The immediate result of this is that it is unlikely he is going to serve his time in a prison, but it is not clear what the value of this assessment is within the context of trying to understand Breivik as a Lone Wolf terrorist. On the one hand, it does help de-fang the impact of his attack from an ideological perspective and would depress Breivik who sees himself as a warrior rather than a madman, but on the other hand, it is unclear whether it would impact potential copycats or others who read his text and find it convincing. Doubtless for them, this assessment would be seen as part of a grander conspiracy.

But this post-fact analysis apart, there is no evidence that Breivik was not able to function perfectly in everyday Norwegian society. Some stories have emerged of him as a

cruel and duplicitous child, but it is almost impossible to verify these in the current overheated climate surrounding his act. In a subsequent interview, his mother revealed that as early as 2005 he had demonstrated some strange activity, moving back home talking obsessively about politics and history "totally beyond reason and [believing] all the nonsense he said." By April 2011 he was still living at home and had started acting in an even stranger manner, wearing an antiseptic mask around the house, refusing to eat food she had cooked for him and calling the family doctor accusing her of infecting him with some illness.[20]

Breivik's act clearly seems the actions of a sociopath – his methodical murder of young people in cold blood and willingness to commit mass murder for a cause he knows is unpopular. However, he says that he is outwardly appalled by his own acts, but that they were "necessary." All of which suggests at the very least a deep lack of empathy (at the same time, stories from Utoya Island indicate that he did spare some individuals who pled for their lives in front of him). Breivik demonstrates a high level of narcissism and he is reported to have told people he had plastic surgery to look more Aryan.[21] Something he subsequently is reported to have regretted, having concluded that he previously "had a great Nordic nose."[22] Throughout his text he talks constantly of how good he looks and he mentions how easy it would be for him to get girls because of his charm and good looks. The posed pictures he places at the end of his 'compendium' – pictures that have become the standard images of him in the public domain - show him as he clearly wants to be seen. And prior to conducting his act, Breivik not only prepared how he wanted to be seen by the world, but he also practiced drilling himself for possible interviews he might have to undergo. All of which demonstrates a very high level of self-obsession.

Analysis:
- Currently, Anders Behring Breivik has displayed no evidence of obvious insanity beyond the official preliminary

Norwegian psychological report. The ideological framework (as currently understood) he offers holds up as a driver for his actions with some coherence.
- Breivik was, however, clearly a narcissist and obsessed with his own image. As we see in previous sections, he spent a lot of time preparing for what would happen post-event and appears to have undergone cosmetic surgery to improve his image. This all suggests a high level of self-involvement and obsession.
- In his chosen targets, he demonstrated a specific anger at the government and the ruling Labor Party in Norway – both in their Oslo offices, and in their summer camp. This reduces the lunacy claim, but does emphasize the importance of conspiracies in his outlook.

Lessons Learned
Using the typology identified in my earlier paper, Breivik fits the Lone Wolf profile since he has demonstrated substantial connections to other far right and anti-Muslim communities globally. Yet at the same time it is unclear that they have any operational command and control with regards him. It is not even clear that his PCCTS network of individuals has any idea of what he was planning or would have known – it seems like the group set up before disbanding for security reasons so that the individuals could all go plot by themselves.

Breivik's action demonstrates the potential danger that can be posed by a Lone Wolf attacker. Intelligent enough to be very cautious in how he goes about his action, he is able over a long period of time to assemble a large and effective bomb and gather weapons and ammunition. He withdrew from the world moving to a farm where he prepared his bomb. From an operational counter-terrorism perspective this is not that useful a conclusion – identifying individuals who suddenly drop off the radar is by definition hard to do. And

particularly when there is little evidence in their previous behavior that this is what they are about to do.

Breivik relied heavily on the Internet to provide him with motivation and operational information. Breivik went online to find fellow believers and supporters and seems to have found his way into the PCCTS through the Internet. He also appears to have been active in far right and anti-Muslim forums and websites and was apparently an avid consumer of the type of literature that they churn out. None of this is that useful from an operational counter-terrorism perspective except if technology exists that is able to somehow connect online surfing behavior of individuals who are active on extremist forums with their online purchasing patterns. This might have detected Breivik at an earlier stage, though the careful manner he claims to have operated online and build cover stories for his purchases also suggests that this may not have been possible.

Carefully planning notwithstanding, Breivik did come into contact with security services when he attempted to purchase a specific chemical online. This action generated an official reaction, but was too low level to result in deeper investigation. All of this is positive to some degree from a counter-terrorism perspective as it suggests that some level of detection is possible – it then ends up being down to the laborious task of following up every lead (possibly a very high number).

Offering another potential avenue for detection, Breivik did purchase actual munitions and was not reliant on completely homemade devices. Given the usual high level of vigilance around weaponry this also offers itself as a detection point – though he used legal methods to obtain his weapons. He started down the illicit path, but recognizing it as too hard, instead went down the legal route and was successful. Clearly, however, unless nations want to pursue situations of zero weapons tolerance for civilians to own weapons it would be hard to strengthen things to the point of detecting someone like Breivik who goes out of his way to fit the correct profile.

However, the weapons point does offer another interesting analytical consideration. Looking back at the cases of Lone Wolves historically, it seems as though the vast majority of those took place in nations that have available guns seek to use or gather traditional weapons at some point. Organized and trained terrorist cells seem to sometimes shun such weaponry recognizing that this will potentially bring them to the attention of security services or bring them into interaction with the criminal underworld which, in turn, might also lead to detection. Lone individuals in nations where such weapons are available to the public, however, seem to choose to try to obtain such weapons whether they use them or not. Certainly in many cases described as 'Lone Wolf' in the United States, guns are purchased and used.[23] In contrast, in most European nations where guns are hard to obtain or unavailable, individuals resort to homemade weapons – for example in the UK the separate cases of home bomb makers Andrew Ibrahim and Nicky Reilly and attempted MP murderer Roshonara Choudhry (and none of this is not to consider the growing number of home bomb makers demonstrating far right ideological inclinations). This suggests a detection tripwire for some countries – though clearly, as Breivik showed, there are ways around it if careful enough.

A final point on ideologies is important. This Lone Wolf case demonstrates the importance of the Internet in disseminating extremist ideology and operational material. But at the same time, it also shows how individuals can become involved in a global ideological battle that they see swirling around themselves and how, with a little effort, they can become quite actively involved in it in a manner that is dangerous to the society in which they are living.

Breivik's case shows the danger of the virulent anti-Muslim rhetoric that sometimes pollutes the political discourse in the West. Written in self-justifying terms that distance it from racism and Islamophobia and portrayed as a defense of a European identity that is being subsumed by waves of Muslim immigrants, it nevertheless is clearly open to different interpretations if they are sought.

As analyst Marc Sageman correctly put it in the *New York Times* in the wake of Breivik's act, "this rhetoric [that of anti-Muslim writers] is not cost free."[24] Breivik's repeated use of specific websites and writers highlights their importance in shaping his ideology and while these writers cannot be held accountable for what he decided to do with the ideas that they were circulating, they must bear some responsibility for fostering the backdrop against which an individual like Brevik can find the justification for his horrendous act.

From the perspective of countering people going down Breivik's path, it is almost impossible to imagine solutions without moving into the space of curtailing individual free speech rights something that is clearly counter-productive. However, some recognition of the potential for such virulent language to be taken further into action by certain individuals is important. Mainstream political parties should make greater efforts to counter it through debate when they see it emerge. A parallel case to be considered in this light is that of Congresswoman Gabrielle Giffords in the US. She was shot by a man who thought he was doing his part to support the extreme right of his party that had attacked Congresswoman Giffords as a traitor for holding certain views. Ideas and words have great power and in a world where we can see the ease with which terrorist operations can be launched by individuals without much outside direction, consideration must be paid to the fact that such extreme ideas might resonate in different ways than they are intended. While stamping out such ideas and thoughts is going to be impossible, currently in some European countries, such ideas have been allowed to slowly move into the mainstream with little confrontation from established political entities. More effort could be expended to confront such ideas and prevent them being mainstreamed. The result otherwise is likely to be more Lone Wolf attacks in the future with a few managing to get through with results as spectacular and tragic as Anders Behring Breivik's.

Notes

[1] The reference to Lone/Solo Actor is a nod to the fact that it is a known preferred nomenclature amongst security agencies.

[2] "Norway suspect Anders Behring Breivik 'admits attacks'," *BBC News*, July 24, 2011.

[3] R. Pantucci, 'A Typology of Lone Wolves: Preliminary Analysis of Lone Islamist Terrorists', International Centre for the Study of Radicalisation, March 2011.

[4] "Norway killer: Anders Behring Breivik was a 'mummy's boy'," *Daily Telegraph*, July 25, 2011.

[5] "Anders Behring Breivik was insane five years ago, mother says," *Telegraph*, November 30, 2011.

[6] "Norway Massacre: the real Anders Behring Breivik," *Sunday Telegraph*, July 31, 2011.

[7] "Norway Massacre: the real Anders Behring Breivik," *Sunday Telegraph*, July 31, 2011.

[8] While these details are not all confirmed, the Progress Party has confirmed that he was a member between 1999-2006, "Norway's right-wing on defensive after attacks," *Associated Press*, August 3, 2011.

[9] Email farming involves using the Internet and social networking sites to obtain email addresses.

[10] "Anders Behring Breivik was insane five years ago, mother says," *Telegraph*, November 30, 2011.

[11] *Ibid.*

[12] Within this context, some consideration must be given of the fact that during his shooting on Utoya Island he made a pair of calls to the police stating that he was a "Norwegian anti-communist resistance commander" and that he wanted to surrender. In both instances, however, he hung up. "Norway massacre: tape of Breivik call to police aired," *BBC News*, November 25, 2011.

[13] "Norway: Anders Behring Breivik claims 'two more cells'," *BBC News*, July 25, 2011.

[14] "Norway: Anders Behring Breivik claims 'two more cells'," *BBC News*, July 25, 2011.

[15] It is worth pointing out that the majority have completely distanced themselves from Breivik's act, and in some cases, have closed down sites that he claims to have drawn inspiration from.

[16] "Norway suspect 'bought from British eBay traders'," *AFP*, August 1, 2011.

[17] R. Pantucci, op. cit.

[18] 'Insanity ruling not likely in Norway," *Associated Press*, July 31, 2011.

[19] "Norway killed Anders Behring Breivik to escape jail as declared 'insane'," *Telegraph*, November 29, 2011.

[20] "Anders Behring Breivik was insane five years ago, mother says," *Telegraph*, November 30, 2011.

[21] "Norway Massacre: the real Anders Behring Breivik," *Sunday Telegraph*, July 31, 2011.

[22] "Anders Behring Breivik regrets loss of 'Great Nordic Nose'," *Telegraph*, November 30, 2011.
[23] Madeleine Gruen and Alfredo Kuilan, "Lone-Wolf Shooters Motivated by Al Qaidist Ideology," *NEFA Foundation Target America series*
[24] "Killings in Norway spotlight anti-Muslim thought in US," *New York Times*, July 24, 2011.

Raffaello Pantucci is an Associate Fellow at the International Center for the Study of Radicalisation (ICSR) at King's College, London. He is the author of the forthcoming 'We Love Death As You Love Life: Britain's Suburban Mujahedeen' (Hurst/Columbia University Press), and the author of "A Typolpogy of Lone Wolves: Preliminary Analysis of Lone Islamist Terrorists" (London: ICSR Press, March 2011). He is a regular contributor to a number of specialist terrorism publications and has written on the topic for media outlets like the Telegraph, Guardian, Washington Times, Foreign Policy, Prospect and New Statesman.

Preventing Lone Wolf Terrorism: some CT Approaches Addressed

By Edwin Bakker and Beatrice de Graaf [1]
Source: http://www.terrorismanalysts.com/pt/index.php/pot/article/view/preventing-lone-wolf/html

Abstract
After a brief discussion of the epistemological and phenomenological difficulties associated with the concept of lone wolf terrorism, a number of possible counter-terrorist approaches are discussed. Lone operator terrorist acts should be considered 'black swan' occurrences that are almost impossible to categorize or systematize, let alone forecast. Thus, not the profile of the perpetrator, but the modus operandi offer clues for a better response to this particular threat. Furthermore, almost all lone operators do display a degree of commitment to, and identification with, extremist movements – providing leads for preventing new rounds of radicalization within this potential group of sympathizers or followers. With the apparent increase of Islamist lone wolf terrorism and fears for right-wing extremists wanting to follow the example of the Norwegian mass murderer A.B. Breivik, new questions need to be posed, addressing the role of virtual communities with which lone operators identify themselves.

Introduction
After the cold-blooded murder of 77 people in Oslo and Utoya (Norway) on 22 July 2011, the threat of lone wolf terrorism has quickly moved (further) up on the agenda of counter terrorism officials. Two questions were raised in the aftermath of the horrible killings by Anders Breivik : (i) could it have been prevented? and (ii) how to discover new plots, possibly by individuals who want to answer Breivik's explicit call to follow his example? Both questions are difficult to answer. The Norwegian authorities are investigating the first question, which has already resulted in the arrest of the owner of an online trading business who is suspected of supplying chemicals to the Norwegian killer. Finding satisfactory answers to the second question – is it possible to discover and prevent future cases – is even more difficult. 'Probably not' is perhaps the most frank and honest answer, but an unacceptable one at that. In this article, we address seven possible counter-terrorist

approaches to the threat posed by lone wolf terrorism with an eye on reducing chances of deadly attacks like the one experienced in Norway. First, however, we have to define lone wolf terrorism.

Defining the Concept
The term 'lone wolf' was popularized in the late 1990s by white supremacists Tom Metzger and Alex Curtis as part of an encouragement to fellow racists to act alone for tactical security reasons when committing violent crimes.[2] Other terms that have been used to describe similar or comparable forms of political violence include 'leaderless resistance'[3], 'individual terrorism'[4] and 'freelance terrorism'[5].

In this article the definition proposed by Burton and Stewart in a STRATFOR essay functions as the point of departure. They define a lone wolf as "a person who acts on his or her own without orders from — or even connections to — an

organization."[6] They stress the difference with sleeper cells, arguing that sleepers are operatives who infiltrate the targeted society or organization and then remain dormant until a group or organization orders them to take action. In contrast, "A lone wolf is a stand alone operative who by his very nature is embedded in the targeted society and is capable of self-activation at any time."[7]. However, by stressing the absence of connections with a broader network or organization, Burton and Stewart neglect the ideological connections individuals might have with other networks or organizations, either through personal contacts or inspirational content on the Internet.

We focus our attention in this article on the operational aspect of lone wolf terrorism. Even though some lone wolves have been linked to larger (underground) networks, such as Baruch Goldstein (who has been linked to Kach) and Timothy McVeigh (who has been linked to several right wing-groups), they decided, planned and performed their act on their own, rather than as having followed instructions from some hierarchical command structure.[8] In our view, a definition of lone wolf terrorism has to be extended to include individuals that are inspired by a certain group but who are not under the orders of any other person, group or network. They might be members of a network, but this network is not a hierarchical organization in the classical sense of the word.[9]

No Single Profile

Infamous examples in the United States, Israel and Europe include Baruch Goldstein, an American-born Israeli citizen who was responsible for the death of 29 Muslims praying in the Cave of the Patriarchs in Hebron; the Austrian Franz Fuchs who used letter bombs to kill four persons and injure 15 more; US army major Nidal Malik Hassan who is accused of a mass shooting at Fort Hood where 13 people died and 30 others were wounded, and the American mathematician Theodore Kaczynski, also known as the 'Unabomber', who engaged in a mail bombing spree that killed three persons and wounded 23 others. In addition, there have been several assassinations of political leaders committed by lone wolves. Think of Yigal Amir, the assassin of Prime Minister of Israel Yitzhak Rabin, or Volkert van der Graaf who killed the Dutch politician Pim Fortuijn.

These individuals and their violent acts exemplify the variations in targeting and modus operandi within lone wolf terrorism, as well as the variety of political and ideological backgrounds of the perpetrators. Anarchist revolutionaries, religious zealots, environmental and animal rights extremists, white supremacists and jihadists all have engaged in lone wolf attacks. When it comes to religious backgrounds we also see a variety of motivations. Among those who claim or justify their acts in the name of a religion are individuals of all faiths. Muslim lone wolves like Nidal Malik Hassan and Abdulhakim Mujahid Muhammad who opened fire on a US military recruiting office, as well as *anti-Semitic/Christian-identity adherents like Buford Furrow who* attacked a Jewish Community Center *and Eric Rudolph, also known as* the Olympic Park Bomber, who killed two people and injured at least 150 others. Lone wolf terrorism also includes *radical Roman Catholics like James Kopp and radical Protestants like Scott Roeder* who both killed a physician who performed abortions.

Obviously, there is no single profile for a lone wolf. Nonetheless, it is possible to distinguish between different categories of lone wolf terrorists based on their ideological or religious background. In addition to this distinction, there are a few common characteristics shared by many lone wolves. One of the problems for both counterterrorism practitioners and academics is the relatively low number of terrorists who act their own without orders from – or even connections to – an organization. According to a study by COT/TTSRL, a total number of 72 lone wolf terrorist incidents accounted for only 1.28 percent of the total number of terrorist incidents in the US, Germany, France, Spain, Italy, Canada and Australia.10] This statistical *quantité négligable* turns these incidents into the typical 'black swan' occurrences that are almost impossible to categorize or systematize, let alone preview.[11] However, the number of incidents linked to lone operator terrorists seems to be on the rise.

Encouraging Lone Wolf Terrorism

The increase in lone wolf terrorism in the United States in the last three decades can partly be explained by the adoption and dissemination of the lone wolf tactic by and amongst right wing extremists.[12] For example, in the late 1990s the white supremacists Tom Metzger and Alex Curtis explicitly encouraged fellow extremists to act alone when committing violent crimes. A few years earlier, white supremacist Louis

Beam, a former Ku Klux Klan and Aryan Nations member, popularized the strategy of *leaderless resistance*.[13] He envisaged a scenario where 'all individuals and groups operate independently of each other, and never report to a central headquarters or single leader for direction or instruction".[14]

Also, in Islamist circles the idea of support for small-scale, loosely organized terrorist attacks can hardly be called new. In 2003, an article was published on the extremist Internet forum *Sada al Jihad* (Echoes of Jihad), in which Osama bin Laden sympathizers were encouraged to take action without waiting for instructions.[15] In 2004, Abu Musab al-Suri (or: Mustafa Setmarian Nasar), a dual citizenship Spanish-Syrian who had been in the inner circle around Bin Laden but fell out with him after 9/11 due to differences on strategic issues, published a "Call for Worldwide Islamic Resistance," on the Internet. In this sixteen hundred pages manuscript, al-Suri proposes a next stage of jihad, characterized by terrorism created by individuals or small autonomous groups, which he also labelled "leaderless resistance". These individuals will wear down the enemy and prepare the ground for the far more ambitious aim of waging war on "open fronts" - an outright struggle for territory [16]. In 2006, Al Qaeda leader Abu Jihad al-Masri followed suit with a call to arms, entitled "How to fight alone" circulated widely in jihadist networks.

The 1,518 page-long manifesto of Anders Breivik can also be regarded as a guide into the workings of lone operator terrorism. In one part of his manifesto, Breivik explains how to publish documents on the Internet and how to use social media for recruiting purposes. Moreover, he shows the tricks he himself used to circumvent European custom agents and describes in detail how he manufactured the explosives he used to blow up the government building in Oslo. Breivik also points at the possibilities of the use of unconventional weapons, such as Radiological Dispersal Devices, or so-called dirty bombs.

The Challenge of Fighting Lone Wolf Terrorism

Attacks by lone operator terrorists provide the most puzzling and unpredictable form of terrorism. Lone wolf terrorists are a nightmare for the counterterrorism organizations, police and intelligence communities as they are extremely difficult to stop.

First of all, lone wolves are solitary actors, whose intentions are hard to discern since they usually avoid contact with others. This makes identifying, monitoring, and arresting a lone wolf extremely difficult. Compared to (conventional forms of) group terrorism or network-sponsored terrorists, lone operators have a critical advantage in avoiding identification and detection before and after their attacks since most of them do not communicate their plans with other people. When militants operate in a cell consisting of more than one person, chances increase substantially that law enforcement authorities will be able to foil a terrorist plot. Breivik was well aware of this. He even warns other potential terrorists they will increase their chance of being apprehended by 100% for every other person they involve in their plans: "Don't trust anyone unless you absolutely need to (which should never be the case). Do absolutely everything by yourself", he writes in his manifesto.[17]

Second, even if lone wolves like Breivik make references to existing political or ideological discourses, they remain very hard to pinpoint as political terrorists/activists. This pose some problems to CT practitioners since insights into the disenfranchised, alienated or frustrated movement behind individual terrorists often provides clues as to their modus operandi, target preferences or outreach and/or propaganda activities. Lone wolfs, by definition, are idiosyncratic. They display a variety of backgrounds with a wide spectrum of ideologies and motivations: from Islamists to right wing extremists, and from confused suicidal psychopaths to dedicated and mentally healthy persons. This vast array of expressions and visions, ranging from ideological ramblings on the Internet and hate mail to fully-fledged acts of terrorism, hardly gives away anything in the sense of patterns or recurring methods behind lone wolf's attacks.

Third, it is particularly difficult to differentiate between those lone operator extremists who intend to commit attacks and those who simply express radical beliefs or issue hollow threats (hoaxes). In Western countries in general and in the United States in particular, the freedom of speech is a fundamental freedom which limits possibilities to investigate radical scenes unless they are violent. While most terrorists are radical but not all radicals are terrorists, it is extremely difficult to single out lone wolves who will carry out an actual attack before they strike, even with the help of the most sophisticated technical intelligence gathering tools.

Fourth, lone wolves inspire copycat behavior and become role models for other alienated youngsters; they often invite bandwagon attacks. Kazcynski's manifesto still circulates on the Internet, as do Bouyeri's letters. And it is likely that we will see the same of Breivik's 'European Declaration of Independence' ten to twenty years from now. In addition to this, certain tactics – shooting sprees, bomb letters, arson attacks or anthrax letters – also have a tendency to continue over a long period of time – although not necessarily by the same perpetrator.

Finally, although lone operator terrorists have the disadvantage of lacking the means, skills, and 'professional' support of terrorist groups or networks, their attacks nonetheless have proven to be very lethal — Anders Breivik and Timothy McVeigh are cases in point.

Possible CT Responses

How to deal with the threat of lone wolf terrorism and the challenge of identifying, targeting, and arresting persons who act entirely on their own? The question has not yet been sufficiently answered and poses the problem of how to reconcile fundamental principles of open societies with guaranteeing security to citizens. One thing, however, is clear: the challenge is enormous, especially when confronted with a person like Anders Breivik who used years to meticulously prepare his horrible attacks – the Oslo bombing (8 killed) and the Utoya massacre (69 killed).

Nonetheless, the above described commonalities and challenges provide some clues as to where to start with CT responses.

First of all, according to Alex Shone of the Henry Jackson society, a British-based think-tank, the key factor of the UK's CT response concerning locating lone wolf attacks is in knowing not *who* will carry out an attack (almost an impossibility) but rather in knowing *how* such attacks are formulated. In his essay, Shone stresses the need to learn about the radicalization processes of lone wolves. He shows that insight into these processes open up possible avenues for effective CT measures to prevent or counter the threat of lone wolf terrorism.[18]

Knowing how lone operator attacks are formulated requires a far more sensitive detection system at the tactical, sharp-end of operations than most CT organizations currently use. According to Shone, CT services need to be far more attuned to those signals, as minimal as they might be, that any individual with a

terrorist intent will inevitably give off in preparing his attack. This requires not only effective data capture and exploitation enabled by efficient overall information management, but also fused intelligence products. This requires intelligence analysts and collectors to work in far closer union.[19]

Secondly, given the 'commonality' shared by many lone wolves that there is a degree of commitment to, and identification with, extremist movements and that their radicalization process does not take place in a vacuum, it is important to both investigate and cooperate with afflicted communities. And given the general agreement that an effective counter radicalization strategy depends on effective community engagement, it is essential to promote passive and active aversion towards the terrorist seed in these communities with the help of influential community members.

In the third place, even a seemingly spontaneous combustion of violence is often triggered by some catalyst event. It could be rewarding to study and compare the nature of potential triggers or catalyst events in the radicalization processes of lone wolves. Are they located within the private domain or are they provided by outside political developments? Or are triggers even mastered by 'entrepreneurs of violence' who use them to call upon their anonymous followers to become active?

In the fourth place, exactly because lone wolves – although operating alone – draw inspiration from other extremists or ideologues, disseminating counter narratives ought to be an important element of an effective CT strategy. A crucial ingredient of counter narratives is the de-legitimisation of perpetrators and their acts and the falsification of their ideologies.

In the fifth place, although lone wolves are not part of hierarchical organisations, they do formulate their acts in a certain context. Awareness programs for parents, schools, universities are worth considering – obviously without launching large-scale public campaigns that only serve to create a moral panic.

A sixth clue as to where to start with CT responses also involves communication processes. On the one hand, communicating the potential threat of lone wolves to relevant target audiences is very important. At the same it is important to refrain from handing them the public theatre they strive for.

Handling lone wolves without giving them any positive public status should be one core principle. Of course, much depends on the channels used

CBRNE Terrorism Newsletter – Winter 2011

by the perpetrator. In the days of Kaczynski, one could, at least for a while, successfully prevent the publishing of his manifesto. Today, the Breivik case in Norway has shown that a lone wolf can send an email to possible supporters and post his video and the 1,500 pages of his manifesto on the Internet in the last remaining hour before he detonates the explosives and heads for his destination to engage in mass murder.

Lastly, perhaps the most concrete clue concerning lone wolf operators and their tactics is their modus operandi. In recent cases of shooting sprees (including high school shootings and mall shootings) all perpetrators were male and all had a license to possess (semi-automatic) firearms. This specific group of people who are allowed to keep firearms – of which the overwhelming majority are law-abiding citizens who use their weapon for hunting or sport shooting – needs special scrutiny. The same holds for the procedures for applying for a weapon permit and membership of a shooting club.

As stated above, the challenge to prevent lone wolf terrorism is enormous and any CT response can only partly reduce this particular threat or limit its impact. As with other forms of terrorism, it is not possible to reach 100% security against this threat. Obviously, there is still a long way to go in preventing lone wolf terrorism. Potential answers on the 'how?' question regarding the modus operandi of lone wolf terrorists and their radicalization processes are still preliminary, needing further investigation. And with the apparent increase of Islamist lone wolf terrorism and fears for right-wing extremists wanting to follow the example of Breivik, new questions need to be posed, for instance about the role of the Internet or the possible impact of attacks on minority groups in society. The fact that there are – fortunately – few cases we can learn from does not make the task to know more about the '*how*' of lone wolf terrorism any easier. Therefore, sharing experiences, data and ideas regarding this particular terrorist threat between practitioners, policy makers and researchers is essential to be able to develop at least some viable responses to lone wolf terrorism.

Final Remarks

Notes

[1]This article is based on a ICCT article on lone wolf terrorism by the same authors; it is available at www.icct.nl. With profound thanks to Liesbeth van der Heide for her research assistance.

[2] COT/TTSRL, Lone-Wolf Terrorism, *Transnational Terrorism Security and the Rule of Law*, July 2007. Cf: http://www.transnationalterrorism.eu/tekst/publications/Lone-Wolf%20Terrorism.pdf, p. 13.

[3] Jeffrey Kaplan. 'Leaderless Resistance', *Terrorism and Political Violence*, vol. 9 (1997), no. 3, pp. 80-95.

[4] Ze'ev Iviansky. 'Individual Terror: Concept and Typology', *Journal of Contemporary History*, vol. 12, no. 1 (January 1977), p. 45.

[5] H. W. Kushner. *Encyclopedia of Terrorism*, Thousand Oaks: Sage 2003, pp. 144-145; C. Hewitt. *Understanding Terrorism in America. From the Klan to al Qaeda*, London and New York: Routledge 2003, p. 79.

[6] Scott *Stewart and Fred Burton, 'The Lone Wolf Disconnect', 30 January 2008, Stratfor, Cf: http://www.stratfor.com/weekly/lone_wolf_disconnect*.

[7] Ibid.

[8] L. van der Heide. 'Individual Terrorism: Indicators of Lone Operators', 30 August 2011, http://igitur-archive.library.uu.nl/student-theses/2011-0902-02354/MA%20Thesis%20Liesbeth%20van%20der%20Heide.pdf p.24.

[9] Marc Sageman, *Understanding Terror Networks*, Philadelphia: University of Pennsylvania Press, 2004.

[10] COT/TTSRL, 2007, op. cit., pp. 16-17.

[11] N. N. Taleb. *Fooled by Randomness: The Hidden Role of Chance in Life and in the Markets*. New York: Random House, 2005.

[12] Mark S. Hamm, *In Bad Company. America's Terrorist Underground*, Northeastern University Press, 2002.

[13] Louis Beam. 'Leaderless Resistance', *The Seditionist*, Issue 12, 1992, cf: http://www.louisbeam.com/leaderless.htm.

[14] COT/TTSRL, 2007, op. cit. p. 13.

[15] Integrated Threat Assessment Center (Canada), "Lone-Wolf Attacks: A Developing Islamist Extremist Strategy?", 29 June 2007, cf: http://www.nefafoundation.org/miscellaneous/FeaturedDocs/ITAC_lonewolves_062007.pdf, p. 4.

[16] Lawrence Wright, 'The Master Plan', in: *The New Yorker*, 11 September 2006, cf: http://www.newyorker.com/archive/2006/09/11/060911fa_fact3?printable=true#ixzz1f7mqzvZe; cf. ´Major Al Qaeda Leader Arrested in Pakistan´, on *Foxnews*, 2 May 2006.

[17] Andrew Berwick, *2083 – A European Declaration of Independence*, London, 2011, p. 844.
[18] Alex Shone, 'Countering lone wolf terrorism: sustaining the CONTEST vision', *Henry Jackson Society*, 17th May 2010, Cf. http://www.henryjacksonsociety.org/stories.asp?id=1582 .
[19] Ibid.

Edwin Bakker *is professor of (counter-) terrorism studies of the Institute of Public Administration of Leiden University where he teaches courses on terrorism and crisis communication. He heads the Centre of Terrorism (CTC) and Counterterrorism and is a Fellow of the International Centre for Counter-Terrorism (ICCT), both based in The Hague, The Netherlands. His research interests include violent radicalization, jihadist terrorism, including lone wolf operations and unconventional forms of terrorism and the potential threat of CBRN terrorism. Recently published work includes chapters in Rik Coolsaet (Ed.), Jihadi Terrorism and the Radicalisation Challenge, Ashgate, 2011 and in Gelijn Molier (Ed.), Terrorism, Ideology, Law and Policy, Republic of Letters, 2011.*

Beatrice de Graaf *is Associate Professor at the Centre for Terrorism and Counterterrorism/Leiden University and Fellow of the International Centre for Counter Terrorism, The Hague. Historian by training, she conducts research projects on 'The making of the national security state, 1945-present', 'Terrorists on Trial', 'The global 1970s' and 'Female Terrorism', focusing on Western countries. She published widely on topics addressing conflict and security issues in historical perspective. Her latest monograph is 'Evaluating Counterterrorism Performance' (Routledge, 2011).*

Terrorist Threats to Commercial Aviation: A Contemporary Assessment
By Ben Brandt
Source: http://www.ctc.usma.edu/posts/terrorist-threats-to-commercial-aviation-a-contemporary-assessment

Ten years ago, al-Qa`ida utilized four U.S. commercial airliners to destroy the World Trade Center's towers, damage the Pentagon, and kill close to 3,000 people. This attack spurred the United States to convert its counterterrorism efforts into a sustained war on terrorism, resulting in the invasion of Afghanistan and Iraq, the capture or killing of hundreds of al-Qa`ida members, and the eventual death of al-Qa`ida chief Usama bin Ladin. There has been extensive reflection in recent months regarding the implications of Bin Ladin's death and the Arab Spring to al-Qa`ida and its affiliated groups.

Two critical issues, however, have been partially sidelined as a result. How has the terrorist threat to commercial aviation evolved since the events of 9/11? How have actions by the U.S. and other governments worked to mitigate this threat?

This article offers a thorough review of recent aviation-related terrorist plots, subsequent mitigation strategies, and current terrorist intentions and capabilities dealing with commercial aviation. It concludes by offering three steps security experts can take to reduce the terrorist threat to commercial aviation.

Aviation-Related Plots Since 9/11 and the Regulatory Response
A number of al-Qa`ida-affiliated plots sought to target commercial aviation since 9/11. A sampling of these include the "shoe bomber" plot in December 2001, an attempt to shoot down an Israeli airliner in Kenya in 2002, the liquid explosives plot against transatlantic flights in 2006, the Christmas Day plot in 2009, and the cargo bomb plots in 2010. Other prominent operations attempted or executed by Islamist extremists during this period include a 2002 plot to hijack an airliner and crash it into Changi International Airport in Singapore, the 2002 El Al ticket counter shootings at Los Angeles International Airport, the 2004 bombings of two Russian airliners, the 2007 Glasgow airport attack, a 2007 plot against Frankfurt Airport by the Sauerland cell, a 2007 attempt by extremists to target fuel lines at JFK International Airport in New York, the 2011 suicide bombing at Moscow's Domodedovo International Airport, and the 2011 shootings of U.S. military personnel at Frankfurt International Airport.

In response to these incidents, the U.S. government and many other countries have dramatically increased aviation security measures to prevent or deter future attacks. Many of these measures are well known to the public, including: the hardening of cockpit doors; federalization of airport security screening staff and the creation of the Transportation Security Administration (TSA); deployment of federal air marshals (FAMs) and federal flight deck officers (FFDOs) aboard aircraft; implementation of new detection equipment and methods, such as advanced imaging technology (AIT), often referred to as "body scanners"; increased amounts of screening for cargo; explosive trace detection (ETD), full body "patdowns," and behavioral detection officers (BDOs); enhanced scrutiny for visa applicants wanting to travel to the United States; and the use of watch lists to screen for terrorists to prevent them from boarding flights or from gaining employment in airports or airlines.

Certain measures—such as invasive patdowns, AIT scanning, inducing passengers to remove jackets, belts, and shoes for inspection, and requiring them to travel with minimal amounts of liquid in their possession—have drawn widespread complaints regarding their inconvenience, as well as questions about their supposed efficacy. The reactive nature of many such measures has been widely noted as well, with some security practices designed to counter highly specific attack techniques utilized in past terrorist plots. Al-Qa`ida in the Arabian Peninsula (AQAP) sarcastically commented on this tendency in its online magazine Inspire, rhetorically asking the U.S. government whether it thought the group had no other way to conceal explosives after the TSA prohibited passengers from carrying printer cartridges.

Current Threats to Aviation

Despite the strenuous efforts by governments to harden commercial aviation in the post-9/11 era, the number of plots illustrates that al-Qa`ida core, its affiliates, and numerous other Islamist extremist groups and self-radicalized individuals maintain a high level of interest in attacking aviation. Despite the organizational disruptions caused by the deaths of numerous senior al-Qa`ida leaders in 2011, and the current preoccupation of several al-Qa`ida affiliates with local conflicts, this ongoing interest in attacking aviation is unlikely to dissipate in the long-term. Furthermore, the evolving tactics utilized in these various plots lend weight to AQAP's contention that

government regulators suffer from a lack of imagination in anticipating and mitigating emergent and existing threats. As indicated by numerous accounts, including the description of the cargo plot contained in Inspire, terrorists constantly seek to analyze existing aviation security measures to probe for weaknesses and develop countermeasures. Terrorists' ongoing efforts to study and defeat security are further exemplified by the arrest of Rajib Karim, a former information technology employee at British Airways; prior to his arrest, Karim maintained an ongoing dialogue with AQAP operative Anwar al-`Awlaqi and attempted to provide al-`Awlaqi with information on aviation security procedures.[1]

Therefore, despite government efforts to improve aviation security, a number of critical tactical threats remain.

Insider Threats

Rajib Karim sought to stage a terrorist attack on behalf of AQAP, seeking to become a flight attendant for British Airways to stage a suicide attack. He also attempted to recruit fellow Muslims (including a baggage handler at Heathrow Airport and an employee of airport security) to stage an attack.[2] Coupled with the aforementioned 2007 JFK airport plot, which involved at least one airport employee, and a reported 2009 plot by Indonesian terrorist Noordin Top to target commercial aviation at Jakarta's main airport, which included assistance from a former mechanic for Garuda Indonesia,[3] this illustrates the primacy of the so-called "insider threat" to aviation.

Although TSA and U.S. airports currently conduct criminal and terrorist database checks on potential airport, airline, and vendor employees who are to be granted access to secure areas, there are significant vulnerabilities in this approach,[4] which has proven notably unsuccessful at stopping members of street gangs from gaining employment and carrying out criminal activities such as narcotrafficking, baggage theft, and prostitution at airports nationwide. In 2010, an individual named Takuma Owuo-Hagood obtained employment as a baggage handler for Delta Airlines, then promptly traveled to Afghanistan where he made contact with the Taliban, reportedly providing advice on how to effectively engage U.S. troops.[5]

The magnitude of this vulnerability is compounded because most airport employees working in secure areas do not undergo security screening prior to entering their workspace due to practical constraints. Additional measures, such

as random screening and security probes, are unable to effectively mitigate this threat. The insider threat becomes markedly worse at non-Western airports in regions such as West Africa or South Asia, where local authorities' ability to effectively screen prospective airport employees is frequently negligible due to incomplete or poorly structured terrorist and criminal intelligence databases.

Threats from Ranged Weapons

MANPADS, or man-portable air defense systems, have been described as a growing threat to commercial aviation following the outbreak of Libya's civil war in early 2011 and subsequent news reports claiming that al-Qa`ida in the Islamic Maghreb (AQIM) has obtained surface-to-air missiles.[6] Some reports suggest that missiles stolen from Libyan arsenals have spread as far as Niger, the Gaza Strip, and the Sinai Peninsula. In addition to AQIM, al-Shabab has been known to possess advanced MANPADS, allegedly provided by Eritrea.[7] Given that AQAP maintains ties to al-Shabab and has reportedly taken over multiple military depots in Yemen following the outbreak of civil unrest there,[8] it is not implausible to assume that AQAP could acquire additional MANPADS. There are also reports that the Taliban acquired MANPADS from Iran,[9] making it conceivable that elements of the group sympathetic to al-Qa`ida's aims could provide al-Qa`ida with MANPADS for a future attack.

Although MANPADS are unable to target aircraft at cruising altitudes, commercial aircraft would become vulnerable for several miles while ascending and descending, particularly due to their lack of countermeasure systems.

In addition to the MANPAD threat, a significant variety of ranged weapons could be used to target commercial aircraft, particularly when taxiing prior to takeoff or after landing. Rocket-propelled grenades (RPGs), for example, are inaccurate at extended ranges; however, they have been used to shoot down rotary wing aircraft in combat zones, and have been used in at least one plot against El Al aircraft.[10] The Irish Republican Army (IRA) used homemade mortars to attack Heathrow Airport in the 1990s, while heavy anti-material sniper rifles such as the Barrett M82 fire .50 caliber rounds to a range of more than one mile and have been previously used by non-state actors, such as the IRA and the Los Zetas drug cartel.[11]

Evolving Threats from Explosive Devices

Terrorist groups, particularly AQAP, have continuously refined their ability to conceal improvised explosive devices (IEDs) from security screening equipment, as shown by the 2009 Christmas Day plot, where a would-be suicide bomber concealed explosives in his underwear, and the 2010 cargo bomb plot, where bombmakers hid explosives in printer cartridges.

Following the 2009 plot in particular, TSA, foreign regulatory agencies, and some airlines sought to increase safeguards against passenger- or cargo-borne IEDs by the deployment of AIT and ETD equipment. IEDs, however, are likely to remain a significant threat to commercial aviation due to limitations in current screening technology. AIT can be defeated by concealing IEDs internally, either by the frequently discussed stratagem of surgically implanting devices in a would-be suicide bomber or by the simpler route of secreting the device within a body cavity. Alternately, IEDs concealed within complex electronic devices are likely to defeat all but the most thorough visual inspection, as illustrated by explosives experts' initial failure to detect the devices used in the 2010 cargo plot.[12] AQAP has shown itself to be particularly adept at concealing IEDs within electronic devices such as printers and radios, which it will likely continue to use in the future.

ETDs and explosives detection dogs, meanwhile, can be defeated by numerous countermeasures. For example, many (though not all) ETD devices detect only two popular explosive compounds. ETD equipment is also not designed to detect the components of improvised incendiary devices (IIDs), making the use of these correspondingly attractive to terrorists. Lastly, IEDs can be sealed and cleaned to degrade the ability of ETD equipment to detect explosive vapors or particles.[13]

Nor is behavioral profiling likely to provide the solution to passenger-borne IEDs and IIDs. Umar Farouk Abdulmutallab underwent two interviews by security staff prior to staging his attack on Northwest Airlines Flight 253 in 2009. Similarly, a GAO report examining the TSA's use of BDOs noted that the scientific community is divided as to whether behavioral detection of terrorists is viable.[14]

Threats Against Airline Facilities and Airports

One aspect of aviation security that is not frequently addressed is the potential for terrorists to strike other

aspects of aviation infrastructure beyond aircraft. Commercial airlines are highly reliant upon information technology systems to handle critical functions such as reservations and crew check-in, a fact not lost upon Rajib Karim when he suggested in correspondence with Anwar al-`Awlaqi that he could erase data from British Airways' servers, thus disabling the airline's website.[15] Such an approach would mesh closely with al-Qa`ida core's and AQAP's stated aims of waging economic jihad against the West. The operational control centers operated by air carriers are another significant point of vulnerability, which conduct the airlines' flight control, meteorology, and emergency management functions. Despite their criticality to flight operations, these control centers are rarely heavily guarded, meaning that a team of attackers equipped with inside knowledge could temporarily shut down the global operations of a major air carrier, particularly if backup facilities were to be targeted as well.

Another threat to commercial aviation is the increasing number of plots and attacks targeting airports themselves rather than aircraft. There have been two significant attacks staged at international airports thus far in 2011 in Frankfurt and Moscow. Attacks against airports have been planned or executed using a variety of tactics, such as firearms, car bombs, suicide bombers, and hijacked aircraft. The targets have included airport facilities such as fuel lines, arrival halls, and curbside drop-off points. Terrorists could also breach perimeter fencing and assault aircraft on runways, taxiing areas, and at gates. This tactic was used during the 2001 Bandaranaike airport attack in Sri Lanka, when a team of Black Tigers[16] used rocket-propelled grenades and antitank weapons to destroy half of Sri Lankan Airlines' fleet of aircraft.[17] More recently, Afghan authorities announced the discovery of arms caches belonging to the Haqqani network near Kabul Airport and claimed that the group had planned to use the caches to stage an assault on the airport.[18] The actions of activist groups—such as Plane Stupid, which has breached perimeter fencing at UK airports so that activists could handcuff themselves to aircraft in a protest against the airline industry's carbon emissions[19]—demonstrate the viability of such an attack in the West as well.[20]

The trend toward attacking airports rather than aircraft has likely been driven by a number of factors, particularly increased checkpoint screening measures and terrorists' growing emphasis on decentralized, small-scale attacks on targets of opportunity. Firearms will likely prove to be a key component of future attacks, given their relative ease of use compared to explosives, as well as their wide availability in the United States and many other countries. This trend was exemplified by the 2011 Frankfurt attack, which was conducted by Arid Uka, an employee at the airport's postal facility, who shot and killed two U.S. soldiers at a bus at the terminal. Although deployment of plainclothes security personnel and quick reaction teams can help ameliorate the impact of attacks on airports, their ease of execution and the impossibility of eliminating all airport queues (be they for drop-off, check-in, security screening, baggage claim, or car rentals) make this tactic a persistent threat.

Required Steps to Improve Aviation Security

Given the breadth and complexity of threats to commercial aviation, those who criticize the TSA and other aviation security regulatory agencies for reactive policies and overly narrow focus appear to have substantial grounding. Three particularly serious charges can be levied against the TSA: it overemphasizes defending against specific attack vectors (such as hijackings or passenger-borne IEDs) at the expense of others (such as insider threats or attacks on airports); it overemphasizes securing U.S. airports while failing to acknowledge the significantly greater threat posed to flights arriving or departing from foreign airports; and it has failed to be transparent with the American people that certain threats are either extremely difficult or beyond the TSA's ability to control. Furthermore, the adoption of cumbersome aviation security measures in the wake of failed attacks entails a financial burden on both governments and the airline industry, which has not gone unnoticed by jihadist propagandists and strategists. While the U.S. government has spent some $56 billion on aviation security measures since 9/11, AQAP prominently noted that its 2010 cargo plot cost a total of $4,900.[21]

With this in mind, there are several measures that could be undertaken to improve U.S. aviation security. First, policymakers must recognize the timely collection and exploitation of intelligence will always be the most effective means of interdicting terrorist threats to aviation, whether by disrupting terrorist leadership in safe havens, breaking up nascent plots, or preventing would-be

terrorists from boarding aircraft. The successful exploitation of intelligence gathered from the Bin Ladin raid in May 2011 has likely done far more to defend commercial aviation from al-Qa`ida than the use of advanced imaging equipment and patdowns.

Second, the TSA and other aviation security regulators must increase their liaison with the airline industry regarding the development of risk mitigation strategies, as airlines are far more aware of the vulnerabilities inherent to commercial aviation, as well as the practical constraints on proposed security measures.

Third, rather than increasing spending on screening equipment and employees deployed in the United States, the TSA and other regulators should instead provide financial support for airlines attempting to improve security for their overseas operations. This could include subsidizing background checks on airlines' international employees and vendors, paying for armed guards at ticket counters, helping upgrade security for airlines' computer networks and control centers, and paying for the deployment of ETD screening equipment. Aviation security regulators should also work to improve the quality of threat information shared with airlines, which is frequently dated, irrelevant, or inaccurate.

Most importantly, the TSA and policymakers must publicly acknowledge that it is impossible to successfully protect every aspect of commercial aviation at all times. Intelligence gaps will occur, watch lists will not always be updated, scanners will fail to detect concealed items, and employees will become corrupt or radicalized. As politically painful as such an admission may be, it is essential to scale back bloated security measures that add significant expense and inconvenience to commercial aviation without materially reducing risk. The TSA's leadership has begun to take small steps in this direction, such as a current pilot program designed to prescreen travelers to facilitate expedited screening, but more must be done to ensure that commercial aviation remains both secure and commercially viable.

Notes

[1] "BA Worker to Stand Trial on Terror Charges," CNN, March 26, 2010.

[2] Vikram Dodd, "British Airways Worker Rajib Karim Convicted of Terrorist Plot," Guardian, February 28, 2011.

[3] "Terror Suspect Top Said Planning Attack on Airline – Indonesian Police Chief," BBC, September 1, 2009.

[4] For example, it is difficult to conduct effective background screening on immigrants who have migrated to the United States from countries with poor records systems.

[5] Alissa Rubin, "Tangled Tale of American Found in Afghanistan," New York Times, October 11, 2010.

[6] See, for example, "Qaeda Offshoot Acquires Libyan Missiles: EU," Agence France-Presse, September 6, 2011.

[7] "Report of the Monitoring Group on Somalia," UN Monitoring Group on Somalia, July 18, 2007.

[8] Fawaz al-Haidari, "Blast at Qaeda-Looted Yemen Ammo Plant Kills 75," Agence France-Presse, March 28, 2011.

[9] Declan Walsh, "Afghanistan War Logs: US Covered Up Fatal Taliban Missile Strike on Chinook," Guardian, July 25, 2010; "Afghanistan War Logs: Anti-Aircraft Missiles Clandestinely Transported from Iran into Afghanistan – US Report," Guardian, July 25, 2010.

[10] Richard Cummings, "Special Feature: The 1981 Bombing of RFE/RL," Radio Free Europe/Radio Liberty, February 9, 1996. Some news reports claim that Islamic militants planned to target an El Al flight with rocket propelled grenades in Switzerland in 2005 as well.

[11] Scott Kraft, "New IRA 'Spectaculars' Seen Stalling Peace," Los Angeles Times, March 19, 1994; Samuel Logan, "Los Zetas: Evolution of a Criminal Organization," ISN Security Watch, March 11, 2009.

[12] "Failure to Find Airport Bomb 'a Weakness,' Expert Says," BBC, November 1, 2010.

[13] For details, see Brian Jackson, Peter Chalk et al., Breaching the Fortress Wall (Santa Monica, CA: RAND Corporation, 2007).

[14] "Aviation Security: Efforts to Validate TSA's Passenger Screening Behavior Detection Program Underway," U.S. Government Accountability Office, May 2010.

[15] Alistair MacDonald, "U.K. Prosecutors Tie BA Employee to Awlaki," Wall Street Journal, February 2, 2011.

[16] The Black Tigers were a specially selected and trained group of suicide operatives deployed by the Liberation Tigers of Tamil Eelam during their insurgent campaign in Sri Lanka.

[17] Celia W. Dugger, "Rebel Attack on Airport Shocks Leaders of Sri Lanka," New York Times, July 25, 2001.

[18] Matt Dupee, "NDS Smashes Haqqani Network Plots in Kabul," The Long War Journal, July 31, 2011.
[19] See, for example, Helen Carter, "Plane Stupid Demo at Manchester Airport Increased Emissions, Court Hears," Guardian, February 21, 2011.
[20] Ibid.
[21] See, for example, Bruce Riedel, "AQAP's 'Great Expectations' for the Future," CTC Sentinel 4:8 (2011). For details on the $56 billion, see Ashley Halsey III, "GOP Report: TSA Hasn't Improved Aviation Security," Washington Post, November 16, 2011.

Ben Brandt is a director at Lime, a political risk consultancy based in the United Arab Emirates. Prior to joining Lime, he worked as a threat analyst for a major U.S. airline, as well as at the New Jersey Office of Homeland Security and Preparedness. Mr. Brandt holds an MA in Security Studies from Georgetown University.

NOTE: Read the whole **CTC Sentinel Newsletter** of Combating Terrorism Center at West Point in the Newsletter's website – CBRNE-CT Papers section

Luton bomber's secret accomplices: Where did 'lone wolf' terrorist get money and expertise to launch Sweden attack?

Source: http://www.dailymail.co.uk/news/article-2072498/Sweden-attack-Luton-bomber-Abdulwahab-Al-Abdalys-secret-accomplices.html#ixzz1gKgSy rDL

Terrorist: Iraqi-born student Taimour Abdulwahab Al-Abdaly killed himself and injured two others when he blew himself up on a Stockholm street

He appeared to be a 'lone wolf' suicide bomber, who blew himself up on the streets of Sweden in an act of solitary vengeance against the country's presence in Afghanistan.
But a fresh investigation into Luton bomber Abdulwahab Al-Abdaly's last 24 hours before his attack in Stockholm has exposed some glaring holes in the lone suicide bomber theory.
Swedish prosecutors, who examined evidence from December 11 last year, have questioned how the unemployed father-of-three was able to finance his mission.
Investigators spoke to 800 people, conducted searches of several premises, and recovered CCTV footage while retracing Al-Abdaly's final steps.
He arrived in the country to visit extended family a month before his attack, during which investigators believe he brought ingredients to make his homemade bombs.

Family man: Stockholm bomber Taimour Abdulwahab Al-Abdaly pictured woth his wife Mona Thwany

And arriving in Sweden the fundamentalist bought a white Audi which he used in his attack. It is not clear how he paid for the car.
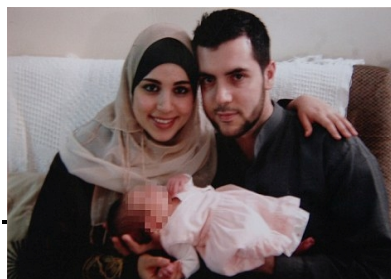
Agnetha Hilding Qvanstrom, a senior official in Sweden's Public Prosecutor's Office for National Security, told CNN: 'We don't know if he got help in Sweden.

CBRNE Terrorism Newsletter – Winter 2011

'What we do know, is that we really think he was alone this day in Stockholm, but we don't know if anyone tried to help him before to buy ingredients for bombs.'

Loving father: Mona Thwany and husband Taimour Abdulwahab Al-Abdaly

It has already been proven, like other terrorists in Europe, he had received bomb-making training in Iraq.
And according to British investigators al-Abdaly made and received a telephone call to a number in Iraq on the day of his attack.
He had two bombs, one inside his new car and another taped to his chest.

Prosecutors say the vehicle's GPS system helped Swedish investigators retrace his route, which included a stop at a petrol station where he paid for his fuel with his bomb strapped tightly to his chest.

Preparation: CCTV footage of Taimour Abdulwahab Al-Abdaly moments before the Swedish blast

Impact: Smoke billows out over the crowds after the December 11 explosion

The terrorist then parked in Olof Palme street and sent several e-mails in English: to a Swedish news agency, the Swedish security services, his wife back in Luton and his mother in Tranas, according to Qvanstrom.
'He said it [the bombing] was because of Lars Vilks and the Swedish presence in Afghanistan,' Qvanstrom, told CNN.
At 4:50 p.m. Stockholm police began receiving calls about a car on fire in central Stockholm. Qvanstrom told CNN: 'Our theory is that he put the car on fire to draw people close.'
Bomb: Firefighters tend to the car in Stockholm in December. A 30-year-old man has today been arrested in Glasgow in connection with the attack

Prosecutors believe he planned to draw people closer to the Audi before setting an explosive off via a walkie-talkie.
But the explosives in the car did not detonate. CCTV video showed that in a nearby street Al-Abdaly was trying to blow himself up for ten minutes he walked through the area, trying to make the device attached to his stomach work.
Magnus Ranstorp, research director at the Swedish National Defence College and a leading counter-terrorism expert, told CNN: 'My understanding is that there was a level of sophistication

CBRNE Terrorism Newsletter – Winter 2011

in the detonation mechanisms and the wiring, Swedish authorities say they continue to investigate whether Abdulwahab was linked to terrorists overseas, or received help in carrying out the attack.

They say he had traveled to Syria and Iraq in 2009 to receive training.

Nasserdine Menni faces charges at Glasgow High Court that he supplied money and that they conspired together 'and with others to further terrorist aims by criminal and other means.' Menni's next court appearance is in January.

Most affordable online degrees in homeland security

Source:http://www.homelandsecuritynewswire.com/bull20111208-most-affordable-online-degrees-in-homeland-security

According to a recent study, at $7,300 Fort Hays State University is the best place to earn your online Master's degree in criminal justice if you are looking for a bargain.

Last week GetEducated.com, a publisher of online college rankings and reviews, release dits rankings for the most affordable online degrees in homeland security, forensics, criminal justice, and security.

GetEducated.com calculated its rankings by comparing tuition and distance education fees at thirty universities across the United States that offered more than forty Master's degrees in homeland security-related fields.

New Mexico State University came in second at $10,318 followed by American Public University, Columbia College, and University of Central Missouri at $11,700, $12,060, and $12,060 respectively.

On the other end of the spectrum, Boston University was found to be the most expensive online program costing more than $31,800.

In total GetEducated.com found sixteen of the best online degrees for under $19,000. In contrast, the average cost for an online Master's degree in justice studies was slightly more than $19,700.

Most notably, the University of Phoenix, the largest for profit online U.S. college, did not make the list as its criminal justice program cost more than $25,700.

GetEducated.com also recently release dits rankings on the most affordable online Bachelor's degrees in homeland security related fields. According to their results, Western Carolina University was the most affordable at $13,937, while Fort Hays State University again made the list at number two with tuition costs of $21,576.

Thomas Edison State College, Waldorf College, and Arkansas Tech University rounded out the top five, with all three costing nearly $27,000 or less for in-state residents.

Brain's failure to appreciate others may permit atrocities

Source: http://www.homelandsecuritynewswire.com/dr20111215-brains-failure-to-appreciate-others-may-permit-atrocities

A person can become callous enough to commit human atrocities because of a failure in the part of the brain that is critical for social interaction; this function may disengage when people encounter others they consider disgusting, thus "dehumanizing" their victims by failing to acknowledge they have thoughts and feelings; this also may help explain how propaganda -- depicting Tutsi in Rwanda as cockroaches and Hitler's classification of Jews in Nazi Germany as vermin -- has contributed to torture and genocide.

A father in Louisiana bludgeoned and beheaded his disabled 7-year-old son last August because he no longer wanted to care for the boy.

For most people, such a heinous act is unconscionable. It may be, however, that a person can become callous enough to commit human atrocities because of a failure in the part of the brain that is critical for social interaction. A Duke University release reports that a new study by researchers at Duke University and Princeton University suggests this function may disengage when people encounter others they consider disgusting, thus "dehumanizing" their victims by failing to acknowledge they have thoughts and feelings.

This shortcoming also may help explain how propaganda depicting Tutsi in Rwanda as cockroaches and Hitler's classification of Jews in Nazi Germany as vermin contributed to torture and genocide, the study said.

"When we encounter a person, we usually infer something about their minds. Sometimes, we fail to do this, opening up the possibility that we do not perceive the person as fully human," said lead author Lasana Harris, an assistant professor in Duke University's Department of Psychology & Neuroscience and Center for Cognitive Neuroscience.

Harris co-authored the study with Susan Fiske, a professor of psychology at Princeton University.

Social neuroscience has shown through MRI studies that people normally activate a network in the brain related to social cognition — thoughts, feelings, empathy, for example — when viewing pictures of others or thinking about their thoughts. When, however, participants in this study were asked to consider images of people they considered drug addicts, homeless people, and others they deemed low on the social ladder, parts of this network failed to engage.

What is especially striking, the researchers said, is that people will easily ascribe social cognition — a belief in an internal life such as emotions — to animals and cars, but will avoid making eye contact with the homeless panhandler in the subway.

"We need to think about other people's experience," Fiske said. "It's what makes them fully human to us."

The duo's previous research suggested that a lack of social cognition can be linked to not acknowledging the mind of other people when imagining a day in their life, and rating them differently on traits that we think differentiate humans from everything else.

This latest study expands on that earlier work to show that these traits correlate with activation in brain regions beyond the social cognition network. These areas include those brain areas involved in disgust, attention and cognitive control.

The release notes that the result is what the researchers call "dehumanized perception," or failing to consider someone else's mind. Such a lack of empathy toward others can also help explain why some members of society are sometimes dehumanized, they said.

For this latest study, 119 undergraduates from Princeton completed judgment and decision-making surveys as they viewed images of people. The researchers sought to examine the students' responses to common emotions triggered by images such as:

— a female college student and male American firefighter (pride);

— a business woman and rich man (envy);

— an elderly man and disabled woman (pity);

— a female homeless person and male drug addict (disgust).

After imagining a day in the life of the people in the images, participants next rated the same person on various dimensions. They rated characteristics including the warmth, competence, similarity, familiarity, responsibility of the person for his/her situation, control of the person over their situation, intelligence, complex emotionality, self-awareness, ups-and-downs in life, and typical humanity.

Participants then went into the MRI scanner and simply looked at pictures of people.

The study found that the neural network involved in social interaction failed to respond to images of drug addicts, the homeless, immigrants and poor people, replicating earlier results.

"These results suggest multiple roots to dehumanization," Harris said. "This suggests that dehumanization is a complex phenomenon, and future research is necessary to more accurately specify this complexity."

The sample's mean age was twenty, with sixty-two female participants. The ethnic composition of the Princeton students who participated in the study was 68 white, 19 Asian, 12 of mixed descent, and 6 black, with the remainder not reporting.

— Read more in Lasana T. Harris and Susan T. Fiske, "Dehumanized Perception: A Psychological Means to Facilitate Atrocities, Torture, and Genocide?" Zeitschrift für Psychologie / Journal of Psychology 219, no. 3 (2011): 175-181

Upcoming Events

Michigan's Emergency Management Conference (October 10-12; Acme, MI) The theme of this conference, sponsored by the Michigan State Police (Emergency Management & Homeland Security Division) and the Michigan Emergency Management Association, is "Back to Basics." It will focus on the fundamental knowledge that all emergency management professionals should have in their arsenal of resources, such as damage assessments, understanding grant requirements, and knowing the latest in communication tools, sheltering regulations, and responder safety. *View event website*
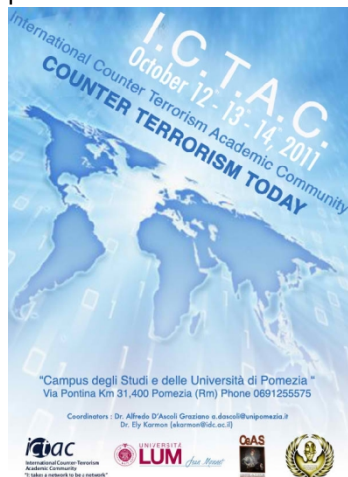
Counter-Terrorism Today (October 12-14; Rome) At this conference presented by the International Counter-Terrorism Academic Community, members of Parliament, heads of security agencies and police forces, professional experts, international organizations' officers, and prominent academics and researchers will examine counter-terrorism today and the effectiveness of current measures and identify which new measures can and should be implemented. *View event website*

American Board for Certification in Homeland Security (October 12-14; Branson, MO) The board's 2011 Executive Summit is a multidisciplinary event that will bring together professionals from the forensics, homeland security, psychotherapy, and integrative medicine disciplines with the common goal of learning. The presentations will cover the latest issues, science, and trends. *View event website*

(October 12-14; Singapore) This conference and exhibition emphasize the importance of implementing disaster prevention measures and present an extensive showcase of the most innovative range of specialized rescue and disaster management products and services designed to protect life and property. *View event website*

(October 13; Los Angeles) The Structural Engineers Association of Southern California will host this major earthquake loss reduction summit at the University of Southern California, a precursor to the Great California ShakeOut on October 20. Many building types in Southern California are at risk of significant damage in earthquakes, and this summit will present cost-effective ways to reduce this risk and bring building officials, owners, and engineers together to develop additional solutions. *View event website*

(October 13, New York; November 10, San Francisco) This conference addresses issues common to all aspects of disaster and emergency preparedness and management; it includes insightful and knowledgeable speakers while providing opportunities for training and networking with experts and practitioners in disaster management research, business continuity, emergency management, emergency

communications, emergency response, risk management, security, information technology, human resources, environmental and community planning, and the organizations that supply and service these professions. *View event website*

Forum on Metropolitan Public Safety (October 13-14; Shanghai, China) this forum is sponsored by the China chapter of the International Emergency Management Society in conjunction with its second annual meeting. The theme is "Building a Safer City." Officials, experts, and scholars from government authorities and emergency response institutions will offer extensive, in-depth discussion and exchange on exploring intelligent urban development samples focused on newest approaches, methods, and technologies that can be used in accident prevention and preparation, monitoring and early warning, relief and rescue, recovery, and reconstruction. *View event website*

Biomedical Advanced Research and Development Authority Industry Day (October 17-19; Boston) This meeting will focus on contracting for countermeasures. It will present the authority's perspective, mission, core services, capabilities, and programs; an industry perspective on working with the authority; opportunities for individual meetings; and more. *View event website*

International Counter-Terrorism Officers Association Conference (October 17-20; Las Vegas) This conference will cover "Jail & Prison Radicalization," "Al Qaida 2011," "Legal Rules to Deal With Emerging & Current Threats in the War on Terror," "Policing Jihad," "Dissolution of Mexico's Traditional Drug Cartels & the Emergence of Bandas Criminals," "Strategic Themes & Drivers in Islamic Law," and "Influence of the Shariah on Law Enforcement Investigations." *View event website*

Virginia Hazardous Materials Conference and Expo (October 17-21; Hampton, VA) This event is presented by the Virginia Association of Hazardous Materials Response Specialists in conjunction with the Virginia Department of Emergency Management. This year's theme is "Confronting New Challenges: Are We Ready?" *View event website*

Building Resilience (October 19-21; Ottawa) This Canadian Risk and Hazards Network Symposium sponsored by the University of Ottawa will explore how to build disaster resilience, concentrating on what has been learned about the multidimensionality and complexity of resilience and, in Canada, about what makes a resilient city and aboriginal community. *View event website*

(October 20) Already, 7.5 million people have signed up to participate in this year's ShakeOut. In 2010, more than 7.9 million Californians practiced "Drop, cover, and hold on" to practice how they will protect themselves during earthquakes and to increase their overall preparedness. *View event website*

NC Emergency Mgt. Assn. Fall All-Hazards Conference (October 23-28; Hickory, NC) The conference will include an update from FEMA Headquarters, firsthand accounts of the April tornadoes and the continuing wildfires, a look at a variety of terrorism issues in the state, and a legal authorities refresher. *View event website*

Coast Guard Innovation Expo (October 25-27; Tampa, FL) This event is sponsored by the National Defense Industrial Association with U.S. Coast Guard participation. This
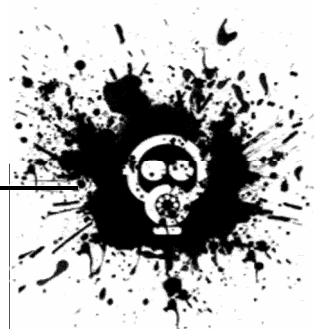
year's expo theme is "Innovation—Steering the Course for Enduring Excellence." "Coast Guard Innovators" will "resolve organizational challenges by showcasing their initiatives in a rich collaborative learning environment alongside other innovators throughout DHS and across Government, industry and academia." *View event website*

(October 26-27; Montgomery, AL) The Air Force Research Institute is organizing this symposium on threats in cyberspace to contribute to a better understanding of the structural sources of cyber security challenges and to identify a common methodology that will serve as framework for identifying solutions and better informed policies. The conference will serve as a forum for exchanging ideas and experiences among cyber professionals. *View event website*

World Maritime Day Observance and Coast Guard Missions Conference (October 27-28; Tampa, FL) This year's world maritime issue is piracy. The Coast Guard Mission Conference theme is "Stewardship, Security and Safety." *View event website*

CBRNe Asia 2012
Conference, Exhibition and Exercise
3rd – 7th September 2012
Plaza Athénée Bangkok, A Royal Meridien Hotel, Thailand

Book by 31st January and Save S$350

Organised by

ib·consultancy
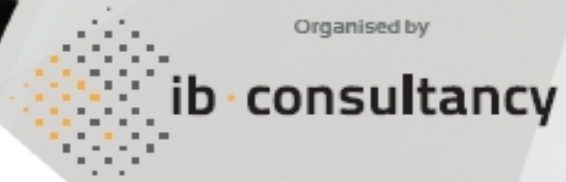
In Full Partnership with the Royal Thai Government
and is pending final endorsement from the Thai MoD

Connect with 300 delegates from over 30 countries

Be visible and be recognised as a key CBRNe player at the premier CBRNe event for the ASEAN community

Reach out and get your opinions across to the people that matter

Networking - 5 days of activities which include workshops, conference, 3 days of exhibition, Royal Thai Governemnt table top exercise day and the Thai National CBRN exercise make this the premier CBRNe event for networking in the world

Esteemed military and government speakers from Asia, Europe, USA, South America and the Middle East ensure that you will hear timely case studies from those at the forefront of current operations

CBRNe Asia 2012 is Asia's first and largest 5 day CBRNe event, exhibition and exercise and will bring together experts, end users, policymakers, industry and procurement staff.

The event will be held in conjunction with the annual Thai National CBRN Exercise, which will focus on a number of chemical and radiological scenarios, and will be fully accessible to all conference delegates.
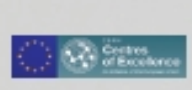
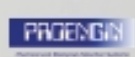Lead Exercise Sponsor:
BRUKER

Exercise Product Sponsor:
AirBoss

Delegate Bag Sponsor:
NBC sys

USB Sponsor:
SAFER SYSTEMS

Event Sponsor:
Centres of Excellence

Exhibitors:
bertin TECHNOLOGIES
CRISTANINI CBRN decontamination systems
Environics
MIRION TECHNOLOGIES
OWR

Paul Boyé TECHNOLOGIES
PROENGIN
proqares
Remploy Putting ability first
RSDecon
Thermo SCIENTIFIC

Endorsing Partners:
THAILAND

Official Media Partner:
CBRNe WORLD

To Keep up-to-date with the Latest Programme Updates, Developments and Announcements Visit:

CBRNeAsia.com

Maritime & Coastal Security Africa (October 26-28; Cape Town, South Africa) This conference focuses on modernizing and optimizing maritime platform capability, encouraging international cooperation, and advancing communication and collaboration among maritime industry bodies. It "will give attendees the tools to provide the necessary surveillance, monitoring and control to African seas and maritime borders as well as utilise the best strategies for port and vessel security." ***View event website***

The conference will bring together experts in the field during a day and a half of presentations in conjunction with an exhibition hall. ***View event website***

(October 27-30; Jakarta, Indonesia) This event aims to increase public knowledge in Indonesia in preparation for upcoming disasters, whether caused by nature or humans. It is also prepared to provide knowledge and education to the public about disaster with "edutainment" delivered in a way of "fun simulation and easy learning." ***View event website***

(October 30–November 1, 2011; Seattle) This conference of the Institute of Electrical and Electronics Engineers will gather scientists, engineers, technology professionals, academics, foundations, government and nongovernmental organizations, and individuals engaged in humanitarian work to discuss and develop solutions for present and future needs: health, medical technology, and telemedicine; disaster warning and response; and connectivity and communications technologies for remote locations—among other topics. ***View event website***

Emergency Management Association of Texas Symposium (October 30–November 2; Odessa, TX) This year's theme is "Pumping Up Preparedness!" This symposium will bring together emergency management professionals and stakeholders from around the state to share information and learn about best practices, new methodologies, and programs in the emergency management and homeland security fields and gain additional knowledge that will help them improve and enhance their emergency operations as they relate to all-hazards mitigation, preparedness, response, and recovery. ***View event website***

2011 National Symposium on Homeland Security and Defense (October 31–November 2; Colorado Springs, CO) The theme of this year's conference is "A 'Whole-of-Society' Approach to Homeland Security and Defense; It's Everybody's Job." This National Homeland Defense Foundation symposium is a public forum where leaders from various sectors of our society can come together to share information, ideas, and plans focused on securing our nation and our liberty. ***View event website***

This conference, hosted by the Integrated Research on Disaster Risk International Programme Office and the China Association for Science and Technology, will provide a platform from which to launch trans-disciplinary research alliances aimed at in-depth, practical disaster risk reduction studies. It will focus on characterization of hazards, vulnerability, and risk; understanding decision making in complex and changing risk contexts; and reducing risk and curbing losses through knowledge-based actions. ***View event website***

(November 1-3; New York) Security Week is an all-in-one mega-event in New York City, organized by the Security Industry Association, that will offer information and business opportunities related to all aspects of the security industry. Existing events—Securing New Ground, Security 500, the Tri-Association Awards Dinner, and ISC Solutions—for the first time will all work together to provide

attendees with new levels of value and convenience. ***View event website***

National Cyberterrorism Conference (November 1-3; San Diego) The conference will address the potential threat from terrorists' use of the Internet and technology to conduct or inspire attacks on small-town America and the nation's critical infrastructure as foreign terrorist organizations "increasingly seek to conduct asymmetric attacks on the U.S. from abroad." Foundry, the conference host, hopes to enhance the nation's ability to counter these threats by educating law enforcement, intelligence analysts, critical infrastructure personnel, the military, and policy makers. ***View event website***

Maritime Regional Resilience and Whole Community (November 3; Norfolk, VA) This forum presented by the Infrastructure Security Partnership will bring together leaders from several port regions to discuss strategies, priorities, and collaboration efforts to ensure maritime regional resilience. ***View event website***

Terror on Trial (November 3-5; Washington, DC) The theme of this conference sponsored by the Association for the Study of the Middle East and Africa is "Out of the Past, Into the Future: Reflections on the Middle East and Africa." It will feature a keynote address by Barham Salih, Prime Minister of the Kurdistan Region, along with presentations by top policymakers and scholars, roundtable discussions on "Turkey as a Democratic Ally Under the AKP [Party for Justice and Progress]" and "The Saddam Tapes, 1978-2001: The Inner Workings of a Tyrant's Regime," and panel discussions of the latest academic research in Middle Eastern and African studies and related disciplines. ***View event website***

(November 7-8; São Paulo, Brazil) The second Chief Security Officer Roundtable Latin America Summit, sponsored by the American Society for Industrial Security International, will cover critical business and security issues such as public-private collaboration during a crisis, dealing with cultural differences in a global organization, corporate security's role in preventing internal fraud, protecting executives and their families, and Brazil's security preparations for the World Cup and the Olympic Games. Last year's summit drew more than 100 security executives from around the world. ***View event website***

(November 7-9; San Diego) Border management professionals will come to learn effective practices to secure and protect the nation's borders. They will hear about technology needs and gaps directly from top border security officials, receive an up-to-date overview of 2012 procurement and acquisition strategies, and gain access to the latest border security technology. The conference and expo are being held in conjunction with UAV West and Maritime Homeland Security West. ***View event website***

Maritime Homeland Security Summit (November 7-9; San Diego) This summit will bring together departmental policy makers, uniformed service leaders, law enforcement, and industry partners to exchange and share best practices and opportunities to improve the security of the nation's maritime borders. The event will showcase anti-piracy strategies, small vessel security strategies, priorities in the Arctic, and the perspective from maritime operators. It also will focus on Homeland Security Department, Justice Department, Defense Department, industry, and law enforcement partnerships and cooperation. ***View event website***

Resilience, Business Continuity and Risk Conference (November 8-9; Adelaide, Australia) This conference will bring together policy makers, practitioners, and academics to consider current developments, including the availability and utility of

management tools, and to review research work and future initiatives to produce a better understanding of how risk management, business continuity, and organizational resilience work together, leading to a more secure and resilient society. *View event website*

Georgia Local Emergency Planning Committee Leadership Summit (November 8-10; Young Harris, GA) This summit provides workshops for local emergency management agencies to obtain tools and knowledge to increase disaster readiness and response capacity. The conference is free but registration is required. *View event website*

Emergency Medical Services Symposium (November 9-13; Norfolk, VA) This symposium sponsored by the Virginia Department of Health offers seminars, courses with continuing education credits, an exhibit hall, and a career fair. *View event website*

(November 11-17; Las Vegas) The International Association of Emergency Managers annual conference provides a forum for current trends and topics, provides information about the latest tools and technology in emergency management and homeland security, and advances the association's committee work. Sessions encourage stakeholders at all levels of government, the private sector, public health, and related professions to exchange ideas on collaborating to protect lives and property from disaster. *View event website*

Mercury Electronic Warfare Launch
New Portfolio of EW Courses

Mercury Electronic Warfare Ltd is a leading provider of EW consultancy, EW operational support and EW training design, development and delivery. With over 60 years of combined experience within the Defence industry and operational military environments, Mercury Electronic Warfare Ltd is at the forefront of operations and support. We specialise in Communications Intelligence (COMINT), Electronic Intelligence (ELINT), Electronic warfare Support (ES), Electronic Attack (EA), Electronic Protection (EP) and Counter-RCIED EW with ongoing specialist support in both technical and operational aspects of these EW disciplines.
We are pleased to announce our new programme of UK delivered EW courses scheduled for 2011 and Q1/Q2 2012. Moreover, UK or overseas organisations who have a requirement for bespoke EW training, or require any of the EW courses detailed below to be delivered outside of the UK can email info@mercuryew.com and we will be delighted to discuss your requirements in detail.
Our courses offer a fully portable and cost effective EW training solution and include the following:

_____

_____

Land Electronic Warfare (EW) Course
Course Dates | November 28 – December 2, 2011 | March 5 – 9, 2012
This five-day course addresses the key management functions regarding the planning, preparation, deployment and sustainment of Land Electronic Warfare capability in a deployed operational context. This includes the processes and procedures required to effectively manage EW capability. It will focus on the employment of EW assets and how best to utilise these assets in a variety of operational environments. There will be a detailed focus on Counter Radio Controlled Improvised Explosive Devices (RCIEDs) covering threats, equipments, technology cycle, interoperability and Tactics, Techniques and Procedures (TTPs). It will also address key subjects that EW has significant influences upon; ISTAR, Information Operations and Battlespace Spectrum Management as well as the roles and

responsibilities of military personnel involved in EW Equipment Procurement, specifically; Procurement Cycle, Capability Integration, Statements of Requirement, Requirements Capture and the various associated key document outputs. The course will also facilitate a number of practical based exercises designed around realistic deployed scenarios in order to consolidate student learning.

Click here for the full course syllabus.

Counter RCIED Workshop

Course Dates | December 6 - 7, 2011 | March 20 – 21, 2012

This two-day workshop addresses key areas regarding the planning, preparation, deployment and sustainment of Electronic Counter Measures used specifically to inhibit Radio Controlled Improvised Explosive Devices (RCIEDs) in a deployed operational context. This includes the processes and procedures required to effectively manage ECM capability. It will cover the RCIED threat; an historical insight into how devices have developed in different environments. Different types of IEDs will be discussed, focusing on the requirements of an RCIED. The workshop will focus in detail on the requirements of ECM equipment and the various methods of jamming that can be used to inhibit RCIEDs. It will also concentrate on the Technology Cycle; exploiting emerging threats and developing new waveforms or new equipment as a timely response to the threat. Interoperability between national and other nations ECM equipments will be addressed as well as ECM interoperability with communications. There will also include a session covering Tactics, Techniques and Procedures relating to ECM usage by both dismounted patrols and vehicle convoys. The workshop will also facilitate practical based exercises designed around realistic deployed scenarios in order to consolidate student learning.

Click here for the full course syllabus.

Radar Fundamentals Course

Course Dates | Janaury 9 - 13, 2012 | April 16 – 20, 2012

This five-day course addresses the key fundamentals of Radar. The course is designed to introduce delegates to the background, history and key operating principles used in modern Radar technology. A review of older legacy systems through to more advanced technology, delegates will be given an insight into how Radar has been, and still is, an important part of today's military and civilian life. The course will be delivered with a blend of theory and practical based lessons. The practical elements of the course will be conducted using state of the art Radar Design software that enables delegates to create theoretical Radar Systems using real world parameters. Using the theory based knowledge and practical application of the software, delegates will increase their understanding of the complex parameters used in modern Radar systems and how the changing of parameters and physical elements of a Radar system influences performance and operating capabilities.

Click here for the full course syllabus.

Battlespace Spectrum Management Course

Course Dates | February 14 – 16, 2012 | May 15 – 17, 2012

This three-day course addresses the key elements of spectrum management in a deployed operational context. This includes the organisation, policy, processes and procedures required to effectively manage the electromagnetic spectrum. It will address

the principles of effective spectrum management including acquisition, planning and deployment of spectrum dependent capability; the spectrum management process from mission preparation to deployment, sustainment and recovery; multinational doctrine and proposed national, joint and single service policy, doctrine, organisation and procedures; examples of good practice and operational anecdotes; practical exercises based on realistic deployed scenarios.

Click here for the full course syllabus.

ELINT Technical Analysis Course
Course Dates | March 26 – 30, 2012 | May 28 – June 1, 2012

This five-day course addresses key elements of ELINT Technical Analysis and will provide the delegates with a sound operational understanding and appreciation of ELINT and its role within modern warfare. The course will be delivered with a blend of theory and practical based lessons. The practical elements of the course will be conducted using a state of the art Pulse Analysis Tool and allows delegates to conduct Technical Analysis of real world parameters. Using the theory based knowledge and practical application of Pulse Analysis software; delegates will increase their understanding of the complex parameters used in modern Radar systems and the skills needed to produce effective and useful ELINT Data files.

Click here for the full course syllabus.

Maritime Electronic Attack Course
Coming soon....

This five-day course addresses the key fundamentals of Maritime EA. The course is designed to introduce delegates to the background, history and key operating principles used in a modern EA environment. A review of older legacy systems through to more advanced technology will give delegates an insight into how EA plays an important part in today's Maritime Warfare. The course will cover all key operational aspects and aims to increase delegates' understanding of EA and how it is applied within modern ASMD tactics.

Click here for the full course syllabus.

In association with Komcept Solutions Ltd, all our advertised courses will be delivered at Ridgeway Farm, Hartwell Road, Ashton, Northampton NN7 2JR, United Kingdom. You can find this location by searching Komcept Solutions Ltd via Google maps.

To download our booking form and full terms and conditions click here. Single delegate and discounted delegate costs for each of the courses are available on application. For more details email us at mailto:info@mercuryew.com

Mercury Electronic Warfare Ltd specialise in the provision of the following services:
• EW operational support and consultancy
• Design, development and delivery of bespoke, generic and EW equipment specific training
• EW academic accreditation at undergraduate and postgraduate levels
• Counter RCIED training, support and consultancy
• Counter Indirect Fire (C-IDF) operational support and consultancy
• EW project management

CBRNe Asia 2012

CBRNe Asia is Asia's first and largest CBRNe conference, exhibition and exercise. CBRNe Asia 2012 on **3-7 September in Bangkok, Thailand** will bring together experts, end users, policymakers, industry and procurement staff and is being organised in full partnership with the Royal Thai Government.

The five-day event will include a two-day conference with high level speakers from the Thai government, ASEAN and the NATO WMD Centre, among others. A special focus session will examine the Fukushima case and simultaneous stream sessions will examine themes including detect and decon, medical CBRN countermeasures, CBRN forensics and improvised chemical devices. The event will be held in conjunction with the annual Thai National CBRN Exercise, which will focus on a number of chemical and radiological scenarios, and will be fully accessible to all conference delegates. During the exercise, equipment made available by exhibiting companies will be used by the Thai Civil and Military authorities.

CBRNe Asia 2012 **Unique Benefits**
- Connect with 300 delegates from over 30 countries
- Be visible and be recognised as a key CBRNe player at the premier CBRNe event for the ASEAN community
- Reach out and get your opinions across to the people that matter
- Networking - 5 days of activities which include workshops, conference, 3 days of exhibition, Royal Thai Governemnt table top exercise day and the Thai National CBRN exercise make this the premier CBRNe event for networking in the world
- Esteemed military and government speakers from Asia, Europe, USA, South America and the Middle East ensure that you will hear timely case studies from those at the forefront of current operations

In full partnership with the Royal Thai Government

Monday 3rd September:
- Pre conference workshop at the Dutch Embassy and an Icebreaker Drinks Reception at Le Meridien Bangkok.

Tuesday 4th September and Wednesday 5th September:
- Two day conference with 40 high level military, government and industry presentations and case studies. Stream sessions will also run allowing you to pick the sessions of most relevance to you. Take the chance to see the latest products, technologies and solutions for the CBRNe community during the exhibition.

Thursday 6th September
- The Royal Thai Government will run a full day of table top scenarios exercises at the Plaza Athenee Bangkok whilst the industry exhibition goes on for a third day.

Friday 7th September

CBRNE-Terrorism Newsletter – Winter 2011

The Thai National CBRN Exercise will take place in Ayutthaya the old Capital of Thailand. All of the conference attendees will have free access to the Thai Military CBRN Exercise and coach transport will be provided from the conference venue.

Pre-Conference Icebreaker Drinks Reception on the 3rd, Le Meridien
Le Meridien Bamboo Chic Bar offers a relaxed atmosphere for unwinding over a drink and discussing your role in the CBRNe domain and the highlights of the next 4 days.

Conference, Exhibition and Royal Thai Government Table Top Exercise, 4th - 6th, Plaza Athenee Bangkok

Plaza Athenee Bangkok, A Royal Meridien Hotel is renowned for uncompromising service standards, world-class facilities, and refined cuisine, all in a unique style that blends the traditions of Thailand with European elegance making this the ideal location to host the CBRNe Asia 2012 conference, exhibition and full day table top exercise day. For more information on Plaza Athenee Bangkok please visit their website

Pre-conference workshop on the 3rd and the end of fourth day drinks reception on the 6th, Embassy of the Kingdom of the Netherlands
Embassy of the Kingdom of the Netherlands in Bangkok, close to the conference venue, will be hosting both the pre-conference workshop and the drinks reception (both will be invitation only). For more information on the Ducth Embassy please visit their website

The Gala dinner on the 4th, Restaurant Vertigo
The gala dinner on the 4th will be hosted at Vertigo Bangkok. This open air bar-cum-restaurant is 61 floors above the bustling streets of Bangkok; stylish, sophisticated, romantic and reaching for the clouds. Prepare for a memorable dinner of barbecued seafood and indulge in some of the world's finest champagne, exotic cocktails, wine-by-the-glass or non-alcoholic beverages in the bar area. The magical atmosphere makes for a memorable evening and a telescope is available for star-gazing, and there will be a live jazz band to accompany networking long into the night. For more information on Vertigo visit their website

The Thai National CBRN Exercise on the 27th, Ayuttaya
The Thai National CBRN Exercise will take place in Ayuttaya the old capital of Thailand. Ayuttaya was founded around A.D.1350 by a Prince of U-Thong. It used to be one of the richest cities in Asia by the 1600s, exporting rice, animal skins, ivory, amongst others. In 1767 the city was completely burned during the war.

INTEGRATED SAFETY & SECURITY 2012
The concept of the exhibition 2012 is an edifice reflecting an integrated comprehension of processes related to the further formation and improvement of the government system of Russia, prevention and liquidation of emergency situations of natural and anthropogenic character, creation of this system and its constant readiness of its forces from nowadays to 2020.
Taking into consideration the development of

the Russian Federation, which is directed to the transformation of the country into the social state and which, in full, provides inalienable right for safety in all spheres to the society, the events within ISSE should particularly clear reflect the social aspect of integrated safety and security provision. In addition this activity should be intensified at regional and municipal government levels.

Small Vessel Security Threats Conference

"The Small Vessel Security Threats Conference" brings together stakeholders from the public and private sectors of the maritime community to discuss the implementation of DHS's "Small Vessel Security Strategy" (SVSS). This forum will discuss the Small Vessel Security Strategy giving the audience an update and insight into the strategy and its' critical components.

Over the last year, HSOutlook with the help of the U.S. Coast Guard have hosted two conferences in Miami and San Francisco to address the SVSS and its' critical objectives. What has been highlighted through these two programs is the need to enhance coordination, cooperation, and communication between federal, state, local and the private sector as well as international partners. "The Small Vessel Security Threats Conference" Charleston will expand on the objective by bringing together stakeholders from the International, Federal, State, Local and Private to discuss how we can collaborate and share intelligence (open source and classified) to better secure the maritime domain from small vessel security threats.

The Four Objectives of the SVSS:

- Develop and leverage a strong partnership with the small vessel community, public and private sectors in order to enhance maritime domain awareness.
- Enhance maritime security and safety based on a coherent plan with a layered, innovative approach.
- Leverage technology to enhance the ability to detect, determine the intent, and when necessary, interdict small vessels.
- Enhance coordination, cooperation, and communication between federal, state, local and tribal partners and the private sector as well as international partners.

Counter IED India, 3-5 October 2012

IB Consultancy is proud to announce Counter IED India together with the Centre for Asia Studies, a major think tank in India. The three day event will take place in Mumbai, India on the 3rd – 5th October 2012 and will bring together Asia's leading experts in C-IED, EOD, Land EW and Counter Terrorism for three days of high

level conference, exhibition, workshops and demonstrations. Here is a chance for those in business to learn from experts, share their perceptions and learn the related issues of the most important form of threat to Indian and Asian cities, infrastructure and people.

The conference organizers invite you to submit papers for consideration at the conference. Please email our events team at info@ibcevents.com and visit www.c-iedindia.com for more information on the program, delegates' sales and sponsor opportunities.

Counter Terror Expo USA

Click **here** for more info