

How to defend against still-undefined CB attacks

CBRNE-TERRORISM Newsletter

Δελτίο ΧΒΡΠΕ-ΤΡΟΜΟΚΡΑΤΙΑΣ

Volume 3 - 2010



- Unit 731
- Cyborg insects sniff WMD
- Warlord, Inc.
- Home-made nuclear reactors
- 911 and miscarriages
- Do you love pigeons?
- Culture war maps

**Man infected himself
with computer virus**

www.RIEAS.gr

CBRNE-Terrorism Newsletter®
Δελτίο ΧΒΡΠΕ-Τρομοκρατίας
Volume 3
Copyright 2010

Editor: BG (ret) Ioannis Galatas MD
Contact e-mail: igalatas@yahoo.com

DISCLAIMER

The CBRNE-Terrorism Newsletter is a free online publication for the fellow first responders of both the civilian and military relevant field and relevant sources are provided.

All info provided herein is from open Internet sources. Opinions and comments from the Editor are not necessarily represent those of the RIEAS.

"Man has never had a weapon he didn't use,"

Ronald Reagan

'We Are Totally Unprepared'

Nine years after 9/11, a chilling complacency about WMD attacks.

Source: <http://online.wsj.com/article/SB10001424052748704312104575299082391565318.html>

By PEGGY NOONAN

The most important overlooked story of the past few weeks was overlooked because it was not surprising. Also because no one really wants to notice it. The weight of 9/11 and all its implications is so much on our minds that it's never on our mind. I speak of the report from the inspector general of the Justice Department, issued in late May, saying the department is not prepared to ensure public safety in the days or weeks after a terrorist attack in which nuclear, biological or chemical weapons are used. The Department of Homeland Security is designated as first federal responder, in a way, in the event of a WMD attack, but every agency in government has a formal, assigned role, and the crucial job of Justice is to manage and coordinate law enforcement and step in if state and local authorities are overwhelmed. So how would Justice do, almost nine years after the attacks of 9/11? Poorly. "The Department is not prepared to fulfill its role . . . to ensure public safety and security in the event of a WMD incident," says the 61-page report. Justice has yet to assign an entity or individual with clear responsibility for oversight or management of WMD response; it has not catalogued its resources in terms of either personnel or equipment; it does not have written plans or checklists in case of a WMD attack. A deputy assistant attorney general for policy and planning is quoted as saying "it is not clear" who in the department is responsible for handling WMD response. Workers interviewed said the department's operational response program "lacks leadership and oversight." An unidentified Justice Department official was quoted: "We are totally unprepared." He added. "Right now, being totally effective would never happen. Everybody would be winging it." The inspector general's staff interviewed 36 senior officials involved in the department's emergency response planning and summarized the finding: "It was clear that no person or entity is managing the overall Department's response activities." You could almost see them scratching their heads and saying, "No one's in charge here." The report reminded me of the CBS News reporter who, working the overnight and monitoring the wires, saw the first report in 1957 that the Soviet Union had launched the first satellite, Sputnik. He called the rocket launch site at Cape Canaveral for a reaction. "We're all asleep here!" a rocket scientist replied, according to lore. They certainly were. A year later NASA was born. There is one bright spot in the inspector general's report: the FBI, which was highlighted for its organizational seriousness about WMD readiness, including holding regular exercises and training sessions, and having an actual response plan with clear lines of responsibility. All credit to the bureau. The report was not the first of its kind. Six months ago, the bipartisan Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism gave both the Obama administration and Congress failing grades on preparedness for biological attack. It said, "the US is failing to address several urgent threats, especially bioterrorism." The administration soon announced it would speed up delivery of drugs that would be needed in the event of an attack. After the inspector general's report, Paul McHale, a former Democratic congressman from Pennsylvania who also served as an assistant secretary of defense under George W. Bush, told the Los Angeles Times: "There is a sense of complacency that has settled in nearly a decade after Sept. 11." The paper also quoted Randall Larsen, the former executive director of the commission that gave the government low marks in January: "They just don't see the WMD scenario as most likely," he said. They don't? They must be idiots. They must not be reading all the government reports of the past eight years, declaring terrorist attacks on

U.S. soil not only likely but virtually certain. There are many reasons for this, and just one has to do with something Ronald Reagan mused about in his office 25 years ago. "Man has never had a weapon he didn't use," he said, to a handful of aides. If you develop the atom bomb, it will be used, as it was. If man, in his darkness, can develop and deploy nuclear, biological and chemical weapons, they will be used, too. No one wants to think about it. I don't want to think about it. But you have to make plans. You have to imagine, you have to think about the worst case, and then



you have to plan for it—literally. We've had enough time, nine years since our unforgettable reminder that history is, among other things, and some of them quite wonderful, a charnel house. Our eye is off the ball. The public, in spite of what it knows in the day to day, assumes the government is on the case. And certainly the government is on the case with regard to prevention: Not being hit again since 2001 means something, and our antiterrorism professionals, intelligence and law-enforcement agents, do impressive work. In New York the past week they picked up two apparent would-be terrorists who won't be playing jihad anytime soon. But public awareness of prevention success gives the impression the government is similarly capable in terms of readiness and response. You can see a certain air of complacency even on government websites. On the front page of the House Committee on Homeland Security site there's a picture of Chairman Bennie Thompson, a Mississippi Democrat, then, below, an area devoted to something called "Business Opportunities Model" and an area for "DHS Business Opportunities." On the Homeland Security Department's website, the priorities seem equally clear: "Find Career Opportunities," "Use the Job Finder." There's little sense of urgency; it's government as employment agency, not crisis leader. A few days before the report on the Justice Department, Henry Kissinger spoke before the Senate Foreign Relations Committee in favor of the new Strategic Arms Reduction Treaty. His testimony was moving—the old vet shares his anxieties for the future—and pertinent. Asked to think aloud on the foreign-policy landscape, the former national security adviser and secretary of state's thoughts turned toward the facts of the age we live in. Suicide bombers, or those who might independently use WMDs, are unlike nations: "They do not calculate in any classic way." The moment we are living in is both dramatic and uncertain. "What happens if we woke up one morning and found that 500,000 people had been killed somewhere?" On 9/11 we were rocked but held together. In a second and more devastating attack, public safety and public unity would be infinitely more stressed. The event, having had a precursor, would be infinitely more painful. You'd think this would focus the government's mind. We may be witnessing again a failure of imagination, the famous phrase used after 9/11 to

capture why the U.S. government was caught so flatfooted and was so stunned that such a terrible thing could occur. They neglected to think of the worst thing that could happen, and so of course they did not plan for it. If agencies within the government now are having a second failure of imagination, it is not forgivable. We're not being asked to imagine a place we've never been, after all, we're only being asked to imagine where we've been, and how it could be worse, and plan for it.



CBRNE-TERRORISM Newsletter

Δελτίο ΧΒΡΠΕ-ΤΡΟΜΟΚΡΑΤΙΑΣ

Volume 3 - 2010

A photograph of a white military truck, possibly a Humvee, that has been severely damaged and is engulfed in a large, intense fire. The fire is bright orange and yellow, with thick black smoke rising from it. The truck is positioned in the center-left of the frame, and the fire is concentrated around its front and side. The background is a blurred, outdoor setting.

CHEM –News

TSI's M41 Protection Assessment Test System lets you test the fit and integrity of NBC protective masks, quickly and reliably.

At mask issue sites, mask training facilities, or even in the field under real-life conditions, you can test your troops in their own protective masks.

For current information
www.tsi.com



- Fully deployed by the U.S. Army, Air Force and Marine Corps, by the German Bundeswehr, and by OPCW field inspectors.
- Gives numerical indication of mask fit and mask integrity
- Verifies that personnel are getting the best possible protection from their assigned masks
- Provides highly sensitive detection of mask leaks
- Helps training personnel to quickly locate and correct problems with mask fit
- Offers results in minutes with no special test chamber
- Uses programmed exercises to simulate normal field activities
- Portable, easy-to-use unit operates almost anywhere
- Includes effective self-test functions

Russia Expands Its Chemical Arsenal, Exposing Treaty's Faults

Source: <http://www.wired.com/dangerroom/category/weapons-and-ammo/chem-bio-nukes/>

Seven years ago this week, Russian Special Forces killed 120 hostages trapped in a Moscow theater, after pumping the place full of a supposedly “non-lethal” knockout gas. Since then,



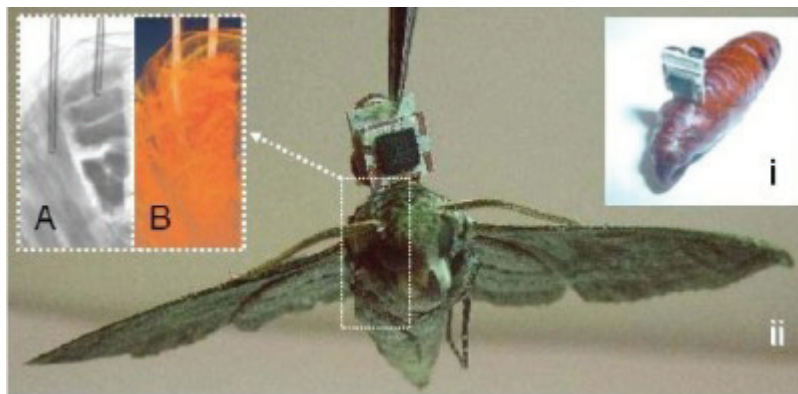
the Kremlin has only expanded its arsenal of these chemical agents, [a new report](#) reveals. And Russia isn't the only country expanding its stockpile. The report by Michael Crowley of University of Bradford's Non-lethal Weapons Research Project, is called *Dangerous Ambiguities*, and it highlights how the international treaties like the Chemical Weapons Convention are failing to curb the so-called “incapacitants” and “riot control agents” — from CS tear gas to fentanyl, the stuff used in the Moscow theater siege. Countries are supposedly prohibited from using these chemical agents as a “method of warfare.” But the term is so vague that it's essentially meaningless. And the Convention was drafted before some modern chemical agents even existed, making their legal status unclear. No wonder the chemicals have been used in a “variety of human rights abuses including suppression of the right to assembly, excessive use of force, ill-treatment and torture. In some instances misuse of RCAs, particularly in enclosed spaces, has reportedly resulted in serious injury or death.” Russia has the biggest arsenal of these non-lethal chemical munitions - everything from 120mm and 82mm mortar rounds to thousand-pound chemical cluster bombs and a “heliborne... dispenser of packages of sub-munitions filled with irritant-action pyrotechnic composition.” As the theater siege showed, the Russians are more than willing to use the agents. To some, the use of fentanyl was a resounding success; Crowley quotes a NATO report saying that “although it may seem excessive that 16% of the 800 hostages died from the ‘gas’ exposure still 84% survived. We do not know that a different tactic would have provided a better outcome. The use of a ‘sleeping gas’ or ‘calmative’ or ‘incapacitant’ agent in this setting is a novel courageous attempt at saving the most lives.” This is echoed in a Russian defense journal, which describes the advantage of this sort of weapon in the urban battlefield: “The irritants

temporarily disable a large number of people, detect an enemy and stabilize the situation without much injury to the local population.” As Crowley notes, the Russians have devoted a considerable amount of effort to this area and they may have other “non-lethal” surprises in store. The existing Chemical Weapon Convention is clearly not effective in limiting this type of chemical warfare, and it’s quite possible that the Russians might deploy such weapons on a large scale. An entire village could be blanketed with an agent in order to sort out the armed militants from civilians. And if 16% is an acceptable death rate, how about 26%... 36%? Other countries are developing their own brand of allegedly “non-lethal” chemical weapons. The Turkish company MKE, for instance, builds the 120mm CS gas mortar round (pictured). A mortar of this size is an artillery piece, a military weapon which is not used by police forces or for law enforcement. There is little doubt that the round is for use as “a method of warfare.” (Crowley mentions a 1999 incident when the Turkish army used CS gas against Kurdish militants in a cave. Twenty of them died, although it is “unclear whether they died from high concentrations of tear gas or whether they were shot when leaving the cave.”) As Crowley points out, the existing international legal framework is not adequate. He suggests a range of measures to improve the situation — from clarifying the existing Convention to launching investigations. But it’s hard to see where the political drive will come from: even the U.S. and U.K. have shown more than a little interest in developing “non-lethal” chemical agents of their own.

Pentagon Wants Cyborg Insects to Sniff WMD, Offer Free Wi-Fi

Source: <http://www.wired.com/dangerroom/category/weapons-and-ammo/chem-bio-nukes/>

The Pentagon is looking for better ways to prevent chemical weapon attacks. So military researchers are implanting insect larvae with WMD-detectors - turning them into cyborg-critters that specialize in tracking down mustard gas. Naturally. In 2005, the military trained honeybees to sniff out land mines. Then, Darpa’s [HI-MEMS program](#) started trying to machinize insects instead. So far researchers have implanted micro-mechanical components into larval moths and created remote-controlled beetles. Those initial HI-MEMS efforts



seemed designed for reconnaissance missions - this time, the Pentagon wants its modified bugs to detect and differentiate between chemical agents. The Pentagon has handed researchers at Agiltron Corporation a contract to implant larvae with “high

sensitivity micromechanical chemical sensors” that run on electric power collected with an embedded “electromagnetic harvester.” The implanted system would include muscle actuators, so different tics or twitches would signal the detection of different chemicals. In separate deals, the Pentagon is also backing research into an insect-mounted device powered by fuel cells, for a more reliable energy source. “This solution offers several advantages over the existing electromechanical methods; 50-100X higher power density, power-generation independent of insect species, and power generation in absence of insect motion,” according to the contract award. And to really bring the critters into the 21st century, the military wants to hook them up with their own wireless network - using chirps instead of Tweets. They’re funding two projects that would create “a mobile ad hoc network” for vocal insects like crickets and cicadas. Insects will be equipped with embedded MEMS transceivers that pick up modulated calling sounds from nearby insects. Once the information in a call is extracted by the transceiver, the information code is applied to an electromechanical device on board

the insect that modulates the insect calls, thereby retransmitting the information to another insect, and so on. The instant-insect message would then be transmitted to humans or computerized systems, which could decode the covert chirp. Sure, swarms of teeny biochemical detectors would be valuable in war-zones. But fly-swatters take note: project proposals reference “civilian and defense applications,” so your bug-squashing habit might soon make you a threat to national security.

Afghanistan: Gas attack targets third girls' school

Source: www.adnkronos.com

At least 30 schoolgirls were poisoned on Tuesday in the northern Afghan city of Kunduz, the third such attack on a girls' school in the city in less than a month, officials said. It is unclear who was behind the attacks. "A masked man, dressed in black, came into the classroom and



threw a small box at us. When we saw the box, we tried to run away, but I passed out. When I regained consciousness, I was in hospital," said 13-year-old Nafeesa, quoted by Pajhwok Afghan News. The girls who fell ill on Tuesday were taken to a local hospital. Some of them were unconscious and in a critical condition, head of the city hospital, Homayoon Khamosh,

told

Pajhwok.

He said

the cause of their sickness was a poisonous gas, similar to the one that had been used at Khodeja-ul-Kubra and Fatima-tu-Zahara girls' schools in Kunduz last month. Pajhwok quoted provincial police chief, Brig. Gen. Mohammad Razaq Yaqubi blaming the attacks on reactionaries who opposed education for girls. But Yaqubi said he did not think the Taliban was involved and no group has claimed responsibility. The Taliban banned



education for girls during their five-year rule of Afghanistan during the 1990s. In many rural areas, there are still threats against female teachers and families who allow their daughters to attend school. Blood tests taken from girls affected by the previous attacks have not yet yielded any results. Taliban spokesman, Zabihullah Mujahid, has strongly condemned the incidents. Last week, 22 schoolgirls and three



teachers fell ill after their school was targeted. In most cases the girls reported smelling something sweet, then fainting, dizziness and vomiting. Kunduz is the capital of surrounding Kunduz province.

teachers fell ill after their school was targeted. In most cases the girls reported smelling something sweet, then fainting, dizziness and vomiting. Kunduz is the capital of surrounding Kunduz province.

Satellite Photos Support Testimony That Iraqi WMD Went to Syria

Source: <http://pajamasmedia.com/blog/satellite-photos-support-testimony-that-iraqi-wmd-went-to-syria/?singlepage=true>

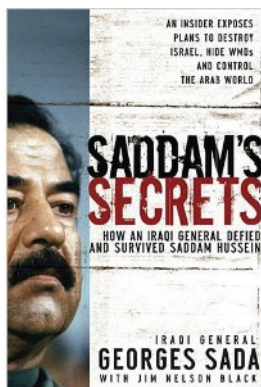
Ha'aretz has revived the mystery surrounding the inability to find weapons of mass destruction stockpiles in Iraq, the most commonly cited justification for Operation Iraqi Freedom and one of the most embarrassing episodes for the United States. Satellite photos of a suspicious site in Syria are providing new support for the reporting of a Syrian journalist who briefly rocked the world with his reporting that Iraq's WMD had been sent to three sites in Syria just before the invasion commenced. The newspaper reveals that a 200 square-kilometer area in northwestern Syria has been photographed by satellites at the request of a Western intelligence agency at least 16 times, the most recent being taken in January. The site is near Masyaf, and it has at least five installations and hidden paths leading underneath the mountains. This supports the reporting of Nizar Nayouf, an award-winning Syrian journalist who said in 2004 that his sources confirmed that Saddam Hussein's WMDs were in Syria. One of the three specific sites he mentioned was an underground base underneath Al-Baida, which is one kilometer south of Masyaf. This is a perfect match. The suspicious features in the photos and the fact that a Western intelligence agency is so interested in the site support Nayouf's reporting, showing that his sources in Syria did indeed have access to specific information about secret activity that is likely WMD-related. Richard Radcliffe, one of my co-writers at WorldThreats.com, noticed that Masyaf is located on a road that goes from Hamah, where there is an airfield sufficient to handle relatively large aircraft, into Lebanon and the western side of the Bekaa Valley, another location said to house Iraqi weapons. It



seems to be commonly accepted that Iraq did not have WMDs at all. The intelligence was obviously flawed, but the book has not been closed on what actually happened. The media blasted the headline that Charles Duelfer, the head of the Iraq Survey Group tasked with finding out if Saddam had WMDs, concluded

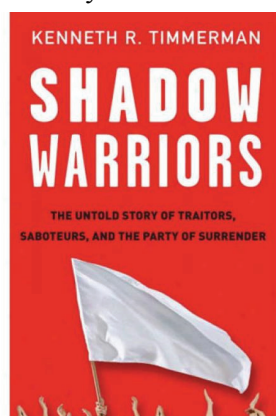
that a transfer did not occur. In reality, his report said they were “unable to complete its investigation and is unable to rule out the possibility that WMD was evacuated to Syria before the war” due to the poor security situation. Although no conclusion was made, Duelfer has since said that he is “convinced” that no WMD went to Syria. He is a competent and credible individual, but there is evidence that key information on this possibility was not received by the Iraq Survey Group, which had many of its own problems. On February 24, 2009, I went to see a talk Duelfer gave at the Free Library of Philadelphia to promote his book. He admitted there were some “loose ends” regarding the possibility that Iraqi WMD went to Syria, but dismissed them. Among these “loose ends,” Duelfer said, was the inability to track down the Iraqis who worked for a company connected to Uday Hussein that sources said had driven “sensitive” material into Syria. A Pentagon document reveals that an Iraqi dissident reported that 50 trucks crossed the border on March 10, 2003, and that his sources in Syria confirmed they carried WMD. These trucks have been talked about frequently and remain a mystery. During the question-and-answer period and during a follow-up interview, Duelfer made several interesting statements to me that reinforced my confidence that such a transfer occurred, although we can not be sure of the extent of it. General Georges Sada, the former

second-in-command of the Iraqi Air Force, claimed in his 2006 book that he knew two Iraqi pilots that flew WMD into Syria over the summer of 2002, which came before a later



shipment on the ground. I asked Duelfer if Nizar Nayouf or the two Iraqi pilots were spoken with. “I did not interview the pilots nor did I speak with the Syrian journalist you mentioned,” he said. “We were inundated with WMD reports and could not investigate them all. ... To narrow the problem, we investigated those people and places we knew would have either been involved or aware of regime WMD activities.” He then told me that the lack of testimony about such dealings is what convinced him that “a lot of material went to Syria, but no WMD.” He cited the testimony of Naji Sabri, the former Iraqi foreign minister, in particular. “I knew him very well, and I had been authorized to make his life a lot better, or a lot

worse,” he told me. He said that Sabri’s position would make him aware of any such deal between the two countries. However, in his book, Duelfer said that Sabri had nothing to do with any of Iraq’s WMD efforts at any time. “His statements on WMD from an intelligence perspective would have been irrelevant,” Duelfer wrote. “Someone among the people we interviewed would have described this,” Duelfer said. However, such testimony does exist. Don Bordenkircher, who served as the national director of jail and prison operations in Iraq for two years, told me that he spoke to about 40 Iraqis, either military personnel or civilians assigned to the military, who talked about the WMDs going to Syria and Lebanon, with some claiming they were actually involved. Their stories matched and were not contradictory, he said. Another military source of mine related to me how an Iraqi intelligence captain in Al-Qaim claimed to have witnessed the movement of suspicious convoys into Syria between February and March 2003. I also asked Duelfer if he was aware of the intelligence provided by the Ukrainians and other sources that the Russians were in Iraq helping to cleanse the country shortly before the invasion. His facial expressions before I even finished the question showed he genuinely had never even heard of this. As explained in detail in Ken Timmerman’s book *Shadow Warriors*, high-level meetings were held on February 10-12, 2004, involving officials from the U.S., the UK, and Ukraine. Among the attendees were Deputy Undersecretary of Defense John A. Shaw, the head of MI6, and the head of Ukrainian intelligence, Ihor Smeshko. The Ukrainians provided all the details of the Russian effort, including the dates and locations of meetings to plan the intervention and even the names of the Russian Spetsnaz officers involved. Shaw also worked with a British source that ran an intelligence network in the region and provided substantiation and additional details. The former head of Romanian intelligence during the Cold War, Ion Pacepa, has provided supporting testimony. He says that he had personal knowledge of a Soviet plan called “Operation Sarindar” where the Russians would cleanse a rogue state ally of any traces of illicit activity if threatened with Western attack. The plan’s purpose was to deny the West of



any evidence incriminating Russia or its ally. The presence of Russian advisors in Iraq shortly before the invasion, some of whom received medals from Saddam Hussein, is a strong indication that this plan was followed. Dave Gaubatz, who was the first civilian federal agent deployed to Iraq, told me that he saw intelligence that “suggested that some WMD had been moved to Syria with the help of Russian intelligence.” Iraqis personally confirmed to him that there was a Russian presence before the American soldiers arrived. Amazingly, Duelfer seems to have never been informed of this intelligence. “This does not mean ... that it was not passed on to ISG [Iraq Survey Group],” he said to me

later. The fact that the head of the WMD search was never even made aware of this indicates

something went seriously wrong. In Timmerman's book, Shaw says that Smeshko complained about the CIA's station chief in Kiev not being cooperative. Timmerman researched the station and chief and found that he was very close with other people in the intelligence community who were doing their best to fight Bush administration policies. Duelfer actually provides information that supports this account. He confirmed that Russia was helping Iraq's illegal ballistic missile program and had close ties to Saddam's regime. "Russians were present in Iraq for many activities. ... Russian officials regularly met with Iraqi officials. ... Russian KGB officers were in regular contact with the regime at very senior levels. ... Russian businessmen were all over Baghdad trying to secure a variety of deals. And of course Russians, including very senior Russians, were in receipt of lucrative oil allocations under the UN Oil-For-Food Program," Duelfer told me. The theory that Iraq's WMD went to Syria is not a fringe conspiracy theory. John Loftus, a former Justice Department prosecutor known for his wide-ranging contacts in the intelligence community, said in an interview we did that "every senior member of a Western, European or Asian intelligence service whom I have ever met all agree that the Russians moved the last of the WMDs out of Iraq in the last few months before the war." General Tommy Franks and General Michael DeLong, the top two officials in CENTCOM when the invasion began, have spoken of credible intelligence supporting the theory. General James Clapper, President Obama's pick to replace Dennis Blair as director of national intelligence, has previously stated his belief that the weapons went to Syria and took part in the meetings organized by Shaw. Obviously, it is impossible to prove and we do not know exactly what went to Syria, but **the history books on this issue shouldn't be written just yet.**

CBRNE-TERRORISM Newsletter

Δελτίο ΧΒΡΠΕ-ΤΡΟΜΟΚΡΑΤΙΑΣ

Volume 3 - 2010

A photograph of a white military truck, possibly an ambulance or medical transport, that has been severely damaged by a large fire. The fire is intense, with bright orange and yellow flames rising from the front and side of the vehicle. The truck is parked on a paved surface, and the background is a plain, light-colored wall. The overall scene is one of destruction and emergency.

BIO –News

Cougar CBRN Protection Suit

The Cougar CBRN Protection Suit provides the very latest in technological solutions to an ever changing CBRN threat. Cougar delivers adaptive solutions to wearer comfort and needs enabling optimum efficiency and protection within an active operational environment.

Lightweight, by design, the Cougar is tough and versatile, facilitating low physiological burden. Cougar can be worn as an over garment or as a stand alone ensemble, delivering a highly effective quick don solution to the CBRN threat.

The outer material of Cougar comprises of a rip stop polyester cotton material for increased tear resistance and enhanced abrasion. The material is water repellent and flame resistant. The inner layer is a lightweight knitted carbon, which is both durable and comfortable to the wearer. Both layers can be laundered, prolonging operational usage.

Features Include:

- High performance permeable fabric – cut, tear and abrasion resistant poly/cotton ripstop, with pyrophobic, fluorocarbon and IRR finishes
- Lightweight
- Two piece hooded jacket and trouser combination
- Jacket incorporates – drawcord adjustment at waist and hem (inhibiting 'bellowing' effect of chemical vapours), elasticated hood: ensuring tight integration with the respirators, modified velcro fastenings on sleeves for optimum integration with gloves
- Trousers incorporate – zip fly, adjustable braces, waist adjuster straps, velcro fastening bottoms for optimum integration with boots
- Guaranteed shelf life of 10 years
- Tested and approved by two leading test houses
- Manufactured to ISO accredited production units located in the UK
- Washable up to 10 times without degradation
- Low level of physiological burden in high humidity environments
- Vacuum packed
- Reusable – retains continuous protective barrier when worn and laundered up to 10 times
- Storage – Long shelf life of up to 10 years (in hermetically sealed packaging)



Research Challenge: How to Defend Against Still-Undefined Chemical, Biological Attacks

Source: <http://www.nationaldefensemagazine.org/archive/2010/June/Pages/DefendAgainstStillUndefinedChemBioAttacks.aspx>

Military scientists are often criticized for not working fast enough and for not pushing technologies into the field more expeditiously. Those working in chemical and biological sciences are no exception. At the Defense Threat Reduction Agency, researchers are finding ways to compress the cycle so they can respond to future attacks that could come in the form of deadly viruses or toxic agents. They worry that advances in biological and chemical



sciences are making it easy for would-be terrorists to wield nature's compounds and bugs for deleterious purposes. Last year's H1N1 pandemic demonstrated how a highly transmissible virus could wreak havoc in a matter of weeks. "It is clear that a pandemic contagious disease is an enormous threat to this country and the world," said Bill Huff, chief of the chemical and biological operations division at the Defense Threat Reduction Agency. "We cannot take our eye off the biological or chemical attack," said Huff. "We have to continue to be vigilant in that arena and continue to develop the technologies that will enable our forces to withstand and operate and successfully defeat a chemical or biological attack." Keeping up with next-generation chemical agents and bioengineering threats is a constant burden. "There's an awful lot of work that needs to be done," said Huff. Developing the technologies to counter the unforeseeable remains the biggest challenge, he added. "What if we get hit with an unknown? How do we rapidly respond?" Army Col. Michael O'Keefe, acting director of the chemical and biological technologies directorate, said the agency is also looking for talent outside the government. Reaching out to scientists who may not be working on chem-bio defense projects per se can be a challenge. But the connections are being made and some are yielding benefits to ongoing projects. Take Omar Yaghi for example. The University of California-Los Angeles chemistry professor probably never thought of his research as having a defense application. He is working on chemical compounds to improve hydrogen storage capabilities for fuel cell-powered cars. DTRA tapped into his research on compounds that soak up chemicals. These compounds, called metal-organic frameworks, have tiny spaces where

chemical agents can be absorbed. Then they can be decontaminated or destroyed by reactive elements. “That type of cutting-edge science could end up in a protective suit the war fighter wears,” said O’Keefe. Troops today have to don a bulky suit that merely absorbs chemicals. In the future, their field uniforms may incorporate Yaghi’s compounds, which would allow the fabric to absorb chemical agents, self-detoxify and automatically report that a reaction has occurred, he explained. “We’re probably within a handful of years of being able to have technology that could feed into that,” said O’Keefe. “The technology is closer than it’s ever been.” Metal-organic frameworks are not limited to fabrics and materials; they could be incorporated into a powder that could be spread on the ground to decontaminate items and areas or used in filtration systems for buildings. The government wants to leverage the work that non-defense researchers are doing, said Eric Moore, chief of the basic and supporting science division. “Many times that requires science managers to look at areas of research that they normally wouldn’t invest in to see if there are some pearls over there, some gems that they could pull into the program,” he said. Ngai Wong, the senior science and technology manager for detection in chemical and biological defense, has an annual budget of \$60 million. “The leveraging that I do between other government agencies would bring the value into the quarter-billion dollar range.” The chem-bio technologies directorate is shifting focus from protecting against known chemical and biological agents to defending against future, still unidentified threats, said O’Keefe. In the past, defense programs focused on conventional chemical weapons, such as mustard gas, VX and sarin. Now it’s time to worry about emerging threats, said John Harvey, principal deputy for the assistant to the secretary of defense for nuclear, chemical and biological defense programs. Wong said the intent is to be able to detect an organism or chemical and ascertain whether it’s a potential menace. His team is working with the National Institutes of Health in human genome sequencing and applying it to chem-bio detection capabilities. “The goal here is a handheld genomic device that’s a very accurate detection device,” said Richard Pate, deputy chief of the physical science and technology division. A major concern is making sensors small and reliable enough



for military use. “That’s where a lot of our resources end up going. It’s not so much in the development of the science itself, but to make sure that the technology actually works the way we think it will,” said Wong. It could take a decade to miniaturize a system, but some capabilities could be fielded sooner. “It will not be handheld, but it will still increase by orders of magnitude what we’re doing today,” said Wong. The division is collaborating with the Energy Department’s national laboratories to build a

10- to 20-year roadmap of how scientists would apply nanoscience to miniaturize various devices. “It’s a big effort to keep current with the ongoing science,” said Pate. In bio-warfare research, scientists have traditionally focused on agents such as anthrax. But in recent years, the emphasis has shifted to infectious diseases, Huff said. Medical programs are stressing pre-symptomatic diagnostics rather than diagnosing patients with a disease after they show up with initial symptoms. “That allows us to open up windows of intervention, before people become ill,” said O’Keefe. “That’s a harder challenge. It involves looking for unique bio-markers that could indicate exposure, and we’re employing things like systems biology to help us search for relevant bio-markers.” Richard Hedstrom, deputy of the medical science and technology division, said there’s a movement to accelerate the development of new products. The so-called translational medicine has been a huge change. “It’s caused basic scientists to think more carefully, to think about how to get this science into a product, something useful that physicians can use to treat people,” he said. In the 2006 Quadrennial Defense Review, the Pentagon called for investments in capabilities to respond to bio-engineered pathogens and emerging infectious diseases. The Defense Department set up the Transformational Medical Technologies Initiative in order to develop therapeutics that could

be applied to multiple threats, said Harvey. This “one drug for many bugs” concept has taken off and yielded two products that were accepted for trials by the Food and Drug Administration a year ago, said David Hough, director of the program. One drug treats Ebola and the other Marburg, both hemorrhagic fever viruses. Those are moving into clinical trials early next year, said Hough. The Defense Department has added funds in fiscal 2010 and 2011 to strengthen that program, said Harvey. When the H1N1 outbreak began last year, government officials took samples of the virus and sent them to Columbia University as part of a rapid-response exercise. The lab was able to identify and characterize the pathogen in less than 24 hours. The sequencing information was sent on to AVI BioPharma, a company in Corvallis, Ore. Its “antisense platform” forms the basis of the two investigational drugs that the government is moving into clinical trials. “They were able to modify that in 72 hours and give us a hospital medical countermeasure, which we took to animal testing and showed that we could knock out 99.9 percent of viral titer using this particular drug,” said Hough. Viral titer is the level of live virus in a fluid or tissue sample. A second test involving an unknown pathogen and four laboratories also proved out the rapid-response capability to identify the sample. All four labs were able to interact with a database set up at Wright-Patterson Air Force Base, Ohio. “That was proof that the mechanics worked. Even the electrons flowed and we were able to share information,” said Hough. In August, the team plans to conduct a similar exercise in South Korea. It will take a clinical sample of a dead virus, transport it back to the United States and see how rapidly the labs can identify or characterize it, and then determine the best course of treatment. “In the three and a half years of the program, we’ve had some pretty good successes and we’re moving forward rapidly into some new areas,” said Hough. “We’re maturing that rapid-response capability and our medical countermeasure development, depending more on systems biology now than ever before. It’s a major change.” DTRA is working with the Food and Drug Administration to get approval for the antisense backbone, said Hough. Developing a therapeutic against an emergent pathogen could take anywhere from five to 10 years. “Our goal is to do it in a matter of weeks,” he said. Hough also oversees a Defense Advanced Research Projects Agency program that is called the accelerated manufacturing of pharmaceuticals. New processes and technologies to manufacture vaccines may speed up production time to days instead of months.

Chem-Bio Defense Budgets Set to Increase In Coming Years

Source: <http://www.nationaldefensemagazine.org/archive/2010/June/Pages/ChemBioDefenseBudgetsSettoIncreaseInComingYears.aspx>

The Obama administration has made no secret of its support of chemical and biological defense programs. The Defense Department in its fiscal 2011 budget requested \$1.5 billion



for chem-bio defense programs — \$370 million for procurement, \$812 million for advanced development and \$396 million for science and technology. “That shows continued commitment to these programs,”

said John Harvey, principal deputy for the assistant to the secretary of defense for nuclear, chemical and biological defense programs. Chem-bio defense programs over the next five years are poised to grow from \$1.5 billion to \$1.8 billion. Defense Secretary Robert Gates has directed the department to rebalance its capabilities to support six key missions. One of the missions is countering weapons of mass destruction, Harvey noted. The goal is to fund activities that cover a wide range of needs, including prevention, attribution, response and consequence management, he said. “We’re trying to develop a systems analytic approach to managing risk and understanding whether the investments we’re making are the right investments. And two, whether there are things that we’re not doing that we should be doing,” said Harvey. “When we get our arms wrapped around this, I think we’ll have a better

opportunity to understand how to target our investments and that's what we're going to be trying to do over the next year."

Biological warfare tests by British WW2 scientists revealed in secret files

Source: <http://www.telegraph.co.uk/science/science-news/7732442/Biological-warfare-tests-by-British-WW2-scientists-revealed-in-secret-files.html>

Cholera, dysentery, typhoid and foot-and-mouth disease were all trialled as potential weapons of war, according to previously secret files released to the National Archives. The list revealed in the new documents demonstrates the breadth of the British research into biological weapons during the conflict, which was already known to have included experiments with anthrax. Experts recognised that "biological warfare" was against the 1925 Geneva protocol, but still carried out a number of tests, the majority of them at Porton Down, near Salisbury, and Pirbright in Surrey. They gave reports to the War Cabinet's Porton experiments subcommittee, which recognised that "bacteriological warfare" was against the 1925 Geneva protocol, The Guardian reported. The minutes were classified as "secret" and "to be kept under lock and key". The use of biological weapons was not seen as "likely to achieve a decisive effect" but preparation was thought to be necessary in order to defend against similar enemy attacks and as a "means of retaliation". Scientists encountered problems when attempting to examine the effect of diseases on cattle because the animals refused to eat cakes containing infections or cut glass. Experts wrote: "Observations have shown that cattle are rather suspicious of any new type of food."

Growing public interest in genetic science sparks some bio-security concerns

Source: <http://www.nationaldefensemagazine.org/archive/2010/June/Pages/GrowingPublicInterestInGeneticScience.aspx>

"When it comes to the knowledge and tools required to launch a bio-terrorism attack, the 'genie is out of the bottle,' experts have warned. The know-how, the equipment and the laboratories needed to genetically manipulate DNA is 'out there,' and the building blocks that could be used to make these potentially devastating diseases occur in nature. There is no need to enrich uranium or stockpile tightly regulated chemicals. Anthrax [spores], for example, could be found in a cow pasture. Now, a growing movement of hobbyists who are carrying out biology experiments in garages, basements and community labs has drawn some interest from the FBI. There have not been any cases of these amateur scientists doing anything illegal, but the potential is there, said one agent. 'We're looking at advances in technologies,' said Edward H. You, supervisory special agent at the FBI's weapons of mass destruction directorate. 'That barrier to do various acts -- and even just cause mischief -- is getting lower and lower and lower, so that risk is growing.'

Expert confirms 3,000 victims at Japan's Unit 731

Source: http://www.chinadaily.com.cn/china/2010-05/14/content_9849909.htm

"An expert confirmed that he and his fellow researchers have uncovered new archives proving at least 3,000 people died from human experiments carried out more than 60 years ago by Japan's infamous Unit 731, china.com.cn reported Friday. Jin Chengmin, an expert on Unit 731 from the Harbin Academy of Social Sciences in Northeast China's Heilongjiang province, said they have gotten the names of the more than 3,000 victims who died from biological experiments at Unit 731 in the Pingfang district of Harbin during China's War of Resistance against Japanese Aggression from 1937 to 1945. Besides the victims' names, the files also include their ages, occupations, places of birth, education levels, and some even contain their

photographs. The list of the victims' names will be displayed in a museum that shows the evidences of crimes of Unit 731."



Wisconsin researcher punished for unauthorized research on bioterror agent

Source: <http://homelandsecuritynewswire.com/wisconsin-researcher-punished-unauthorized-research-bioterror-agent>

A university of Wisconsin researchers conducted unauthorized research on bioterror agent; the researcher developed antibiotic-resistant variants of brucellosis and tested them on mice; the University of Wisconsin was fined \$40,000 by the National Institutes of Health, and the professor was ordered to stay out of a lab for five years. The University of Wisconsin-Madison had ordered a veterinary researcher to stay out of a lab for five years after he performed research on a potential bioterrorism agent without receiving proper approval, the Wisconsin State Journal reported Tuesday. Professor Gary Splitter failed to receive authorization from local or federal authorities before his laboratory no later than 2007 produced antibiotic-resistant variants of brucellosis and tested them on mice. The work was a "major action violation," according to the National Institutes of Health (NIH), and earned the university a \$40,000 penalty. Brucellosis is a disease that generally infects livestock or other animals but can spread to humans through several means, including consumption of milk contaminated with the bacteria. Symptoms include fever, headache, and back pain and the disease can produce "severe infections" of the central nervous system or heart lining, according to the Centers for Disease Control and Prevention (CDC). The disease is not among the agents most likely to be used in an act of bioterrorism, "in part because it results in a high morbidity, but low mortality," according to a fact sheet from Saint Louis University. "However, it remains a threat because the disease process is long and incapacitating." An antibiotic-resistant version of the disease could be harder to treat than a more standard form, according to the newspaper. Global Security Newswire reports that one laboratory staffer was infected with the disease, but it was not clear whether that was linked to the strain involved in Splitter's work. The staffer apparently suffered no permanent effects. "These are extremely dangerous compounds," according to university provost Paul DeLuca. "They are very highly regulated and we want to be in full compliance with federal laws." Splitter said that graduate students performed the research in question and that it had not been brought to his attention. Scientists have also not received adequate guidance from the university on work involving antibiotic-resistant forms of disease, he argued. "The University of Wisconsin failed to provide the right education," he said. "The bottom line is that this wasn't just an investigation of one individual. It was a major meltdown by the university." The university probe into the

case, which began in 2008, uncovered information that indicated that Splitter was aware of the research, officials said. In 2007 a scientist at the university was reported to have received approval to conduct Ebola research in a facility with a lower security level than mandated for that work. The research was ultimately relocated to a higher-security facility. The university over the last twelve months has brought on a new biological safety director and five officers. Splitter is due to receive laboratory privileges again in December 2013, five years after his work area was closed. “Gary Splitter is one terrific scientist,” DeLuca said. “He’s had an excellent career and done really excellent work, however that does not excuse doing experiments with select agents that are not approved.”

And man made life

Artificial life, the stuff of dreams and nightmares, has arrived

Source: http://www.economist.com/opinion/displayStory.cfm?story_id=16163154



TO CREATE life is the prerogative of gods. Deep in the human psyche, whatever the rational pleadings of physics and chemistry, there exists a sense that biology is different, is more than just the sum of atoms moving about and reacting with one another, is somehow infused with a divine spark, a vital essence. It may come as a shock, then, that mere mortals have now made artificial life. Craig Venter and Hamilton Smith, the two American biologists who unravelled the first DNA sequence of a living organism (a bacterium) in 1995, have made a bacterium that has an artificial genome—creating a living creature with no ancestor. Pedants may quibble that only the DNA of the new beast was actually manufactured in a laboratory; the researchers had to use the shell of an existing bug to get that DNA to do its stuff. Nevertheless, a Rubicon has been crossed. It is now possible to conceive of a world in which new bacteria (and eventually, new animals and plants) are designed on a computer and then grown to order. That ability would prove mankind’s mastery over nature in a way more profound than even the detonation of the first atomic bomb. The bomb, however justified in the context of the second world war, was purely destructive. Biology is about nurturing and growth. Synthetic biology, as the technology that this and myriad less eye-catching advances are ushering in has been dubbed, promises much. In the short term it promises better drugs, less thirsty crops, greener fuels and even a rejuvenated chemical industry. In the longer term who knows what marvels could be designed and grown? On the face of it, then, artificial life looks like a wonderful thing. Yet that is not how many will view the announcement. For

them, a better word than “creation” is “tampering”. Have scientists got too big for their boots? Will their hubris bring Nemesis in due course? What horrors will come creeping out of the flask on the laboratory bench? Such questions are not misplaced—and should give pause even to those, including this newspaper, who normally embrace advances in science with enthusiasm. The new biological science does have the potential to do great harm, as well as good. “Predator” and “disease” are just as much part of the biological vocabulary as “nurturing” and “growth”. But for good or ill it is here. Creating life is no longer the prerogative of gods.

Children of a lesser god

It will be a while, yet, before lifeforms are routinely designed on a laptop. But this will come. The past decade, since the completion of the Human Genome Project, has seen two related developments that make it almost inevitable. One is an extraordinary rise in the speed, and fall in the cost, of analysing the DNA sequences that encode the natural “software” of life. What once took years and cost millions now takes days and costs thousands. Databases are filling up with the genomes of everything from the tiniest virus to the tallest tree. These genomes are the raw material for synthetic biology. First, they will provide an understanding of how biology works right down to the atomic level. That can then be modelled in human-designed software so that synthetic biologists will be able to assemble new constellations of genes with a reasonable presumption that they will work in a predictable way. Second, the genome databases are a warehouse that can be raided for whatever part a synthetic biologist requires. The other development is faster and cheaper DNA synthesis. This has lagged a few years behind DNA analysis, but seems to be heading in the same direction. That means it will soon be possible for almost anybody to make DNA to order, and dabble in synthetic biology. That is good, up to a point. Innovation works best when it is a game that anyone can play. The more ideas there are, the better the chance some will prosper. Unfortunately and inevitably, some of those ideas will be malicious. And the problem with malicious biological inventions—unlike, say, guns and explosives—is that once released, they can breed by themselves.

Biology really is different

The Home Brew computing club launched Steve Jobs and Apple, but similar ventures produced a thousand computer viruses. What if a home-brew synthetic-biology club were accidentally to launch a real virus or bacterium? What if a terrorist were to do the same deliberately? The risk of accidentally creating something bad is probably low. Most bacteria opt for an easy life breaking down organic material that is already dead. It doesn't fight back. Living hosts do. Creating something bad deliberately, whether the creator is a teenage hacker, a terrorist or a rogue state, is a different matter. No one now knows how easy it would be to turbo-charge an existing human pathogen, or take one that infects another type of animal and assist its passage over the species barrier. We will soon find out, though. It is hard to know how to address this threat. The reflex, to restrict and ban, has worked (albeit far from perfectly) for more traditional sorts of biological weapons. Those, though, have been in the hands of states. The ubiquity of computer viruses shows what can happen when technology gets distributed. Thoughtful observers of synthetic biology favour a different approach: openness. This avoids shutting out the good in a belated attempt to prevent the bad. Knowledge cannot be unlearned, so the best way to oppose the villains is to have lots of heroes on your side. Then, when a problem arises, an answer can be found quickly. If pathogens can be designed by laptop, vaccines can be, too. And, just as “open source” software lets white-hat computer nerds work against the black-hats, so open-source biology would encourage white-hat geneticists. Regulation—and, especially, vigilance—will still be needed. Keeping an eye out for novel diseases is sensible even when such diseases are natural. Monitoring needs to be redoubled and co-ordinated. Then, whether natural or artificial, the full weight of synthetic biology can be brought to bear on the problem. Encourage the good to outwit the bad and, with luck, you keep Nemesis at bay.

WTC Workers Suffer Long-Lasting Sensory Loss

Source: <http://www.medicalnewstoday.com/articles/189097.php>

New research from the Monell Center and collaborating institutions reports that workers exposed to the complex mixture of toxic airborne chemicals following the 9/11 disaster had a decreased ability to detect odors and irritants two years after the exposure. "The nose performs many sensory functions that are critical for human health and safety," said lead author Pamela Dalton, PhD, MPH, an environmental psychologist at Monell. "The sensory system that detects irritants is the first line of defense to protect the lungs against airborne toxic chemicals. The loss of the ability of the nose to respond to a strong irritant means that the reflexes that protect the lungs from toxic exposures will not be triggered." Individuals involved in rescue, recovery, demolition and clean-up at the World Trade Center (WTC) were exposed to a complex mixture of smoke, dust, fumes, and gases. In the study, reported online in the journal *Environmental Health Perspectives*, Dalton and collaborators studied 102 individuals who worked or volunteered at the WTC site on 9/11 and during the days and weeks afterward to determine whether this exposure affected their ability to detect odors and irritants. Forty-four percent of the workers reported being in lower Manhattan on 9/11 and 97 percent worked on the site during the week after the buildings' collapse. Two years after the exposure, the WTC workers had decreased sensitivity to odors and irritants as compared to similar workers with no WTC exposure. Twenty-two percent of the WTC workers had a diminished ability to detect odors and nearly 75 percent had an impaired ability to detect irritants. Workers exposed to the dust cloud immediately after the buildings' collapse had the most extreme loss of sensitivity to irritants, with an almost complete inability to detect the nasal irritant used in the study. Almost none of the individuals tested recognized that their ability to detect odors and irritants was compromised. Health screenings of WTC workers had documented the effects of inhaled exposure on the lungs and respiratory function, but little was known about the impact on sensory systems of the nose. These sensory systems include the olfactory system, which detects odors, and the somatosensory system, responsible for detecting irritants, chemicals that cause pain, tingling, burning, stinging, or prickling. The inability to detect irritants and odors is a critical safety concern, especially since the workers were not aware of their impairment. "Odors also serve a protective function, such as the ability to identify smoke from a fire, leaking gas, or spoiled food," said Dalton. The authors suggest that the ability to smell and detect irritants should be evaluated regularly in WTC responders and other workers having pollutant exposures. Future studies will attempt to follow the workers to assess recovery and identify factors associated with more complete recovery.

Universal Vaccines: Hope for the Future

Source: <http://mbio.asm.org/content/1/1/e00042-10.full.pdf+html>

While vaccines have proven invaluable in the quest to control infectious diseases, certain microbes—exemplified by the influenza virus—have defied long lasting control because their antigenic structure mutates, creating moving targets for vaccines. For years, researchers have sought to develop an influenza vaccine that could be given once (or at least infrequently) and that would provide protection from all or most strains of influenza. Such a “universal vaccine” could greatly limit the disease burden of seasonal influenza and reduce the threat of an influenza pandemic. In the April 2010 issue of the journal *mBio*, Cassone and Rappuoli review the topic of universal vaccinations for influenza and several other infectious diseases. Asserting the importance of this approach in controlling infectious diseases, the authors call for further development of universal vaccines.



Influenza Virus Exemplifies Need for Universal Vaccine

Each year as influenza season approaches, the seasonal flu vaccine is refined to best match the strains predicted to be circulating during that season. The vaccine is often a good match, but there have been occasions when mismatches occur, resulting in more widespread disease secondary to decreased vaccine efficacy. Mismatches also can have the long lasting effect of diminished confidence in the flu vaccine. The emergence of a pandemic strain, as in 2009, necessitates the rapid development, manufacture, and distribution of a novel vaccine. While some influenza vaccines provide limited cross-reactivity between some strains, which may be boosted by adjuvants; however, this cross-reactivity is hardly a universal vaccine. The search for a universal influenza vaccine is currently focused on identifying a structure that is present in all influenza strains and is not affected by antigenic shift and drift. Such a structure is coded for by a “conserved domain” of the virus’s genome. To date, several targets have been discovered:

- Stalk of the hemagglutinin molecule
- Nonglobular portion of the hemagglutinin molecule close to or containing the fusion peptide
- Nucleoprotein
- M2 protein

Restricted and Unrestricted Universal Vaccines

- Cassone and Rappuoli divide universal vaccines into 2 broad conceptual categories:
- Restricted—directed against related microbes (eg, influenza, pneumococcus)

Unrestricted—may be effective against genetically disparate microbes (eg, a vaccine targeted both *S. aureus* and *E. coli*)

Fascinating examples of vaccines with unrestricted universality are discussed, including the unrestricted vaccine mentioned above, which targets poly-N-acetylglucosamine and is protective against the gram negative bacterium *E. coli* and the gram positive bacterium *S. aureus*. Other approaches in development include a vaccine that is protective against both *Candida* and *Aspergillus* and a vaccine that targets the prokaryote bacterium *S. aureus* as well as the eukaryote fungi *Candida*.

Universal Vaccines Represent a Paradigm Shift

The employment of universal vaccines in the battle against infectious microbes represents a major paradigm shift that has the potential to revolutionize the field of vaccinology and improve the health of the human species. Targeting microbes that have defied easy vaccination solutions and decreasing the vaccination burden by elucidating universal antigenic components (Pathogen-Associated Molecular Patterns, PAMPS) will provide a 21st century solution to a problem present since the dawn of the human race.

References

Cassone A, Rappuoli R. Universal vaccines: shifting to one for many. *mBio* 2010; e00042-10. <http://mbio.asm.org/content/1/1/e00042-10.full.pdf+html>. Accessed May 25, 2010.

Scientists voice concern over health risks from full body scanners

Source: http://www.gsnmagazine.com/article/20791/scientists_voice_concern_over_health_risks_full_bo

No longer is it just bloggers, activists and anti-government conspiracy theorists that are concerned about full body scanners in our nation’s airports. Now, a group of worried scientists from the University of California at San Francisco (UCSF) have called upon the White House to take a close look at these X-ray scanners. In a letter sent to the Office of Science and Technology, the scientists -- who are experts in the field of biochemistry, biophysics, imaging, cancer and crystals -- raise serious concerns regarding the safety of full body scanners. The technology being used puts people at increased risk of cancer, the scientists believe, among other health problems. This is especially true, according the

scientists, for older travelers, women who are expecting and individuals with weak immune systems. The UCSF group, which includes Dr. Marc Shuman, John Sedat, David Agard and



Robert Stroud, have asked that the President put together an independent panel to look into the possible risks. Even guest columnists who have contributed their musings to GSN: Government Security News have voiced their concern over the scanners. On May 6, Rafi Sela, President of AR Challenges, wrote in an editorial featured in GSN's Homeland Security Insider entitled, "Airport security and body scanners – a new paradigm?" in which he points out that the body scanners "do not solve the whole threat [of terrorism], only a part of it. Such systems make lines longer

and no one really knows yet if the radiation emitted is safe." Officials at DHS say the scientists' concern is misplaced. Dr. Alexander Garza, the assistant secretary for health affairs and chief medical officer for the department, said he has no qualms about putting his own family through the airport scanners when they travel. "The risk is so low it's almost negligible," he said, adding that all passengers have the right to forgo the scanner and instead undergo a full-body pat-down search. By the end of next year, the Transportation Security Administration (TSA) hopes to have up to 1,000 full-body scanners to screen passengers at airports across the U.S. The letter from the California university scientists comes on the heels of a new Programmatic Environmental Assessment (PEA) report issued by the Customs and Border Patrol that studied "the environmental effects of using truck-mounted and stationary High Energy X-ray systems to inspect cargo containers at U.S. seaports and land ports of entry, and [which] concluded that 'there will be no significant, adverse effects to the human environment as long as identified mitigation measures are followed,'" as GSN: Government Security News reported on May 25.

Distress of 9/11 may have led to miscarriages, research says

Source: <http://edition.cnn.com/2010/HEALTH/05/25/9.11.miscarriage.bereavement/>



The shock and stress felt by pregnant women after the terrorist attacks on September 11, 2001, may have contributed to an increase in miscarriages of male fetuses in the United States, according to a study recently released. Researchers found the male fetal death rate increased in September 2001 and subsequently affected the ratio of boys born in a later

month, according to the study published in the journal BMC Public Health. The authors hypothesized that this might be a case of "communal bereavement." Even without direct relationships with the deceased, pregnant women may have been distressed by the attacks, resulting in miscarriage, according to the research. "A huge population saw the consequences and carnage onscreen," said lead author Tim Bruckner, who is an assistant professor of public health at University of California Irvine, about the effects of 9/11. He examined this topic "because pregnancy is sensitive to stressors. I wondered whether pregnant women might have a physiological reaction to witnessing harm." Bruckner examined only miscarriages of boys, because male fetuses are believed to be more sensitive than females to stress hormones. Previous studies have suggested that the percentage of male births drops after natural disasters, economic decline or catastrophes. A 2005 study found the health of the Swedish economy affected the ratio of male-to-female births. A 1998 study from Japan found a decline in male births after the Kobe earthquake in January 1995. With fetuses, Bruckner said, "We have very little understanding why males respond more sensitively to stressors than females. ... Physiologically we don't have a grasp on this when we look at how pregnancies respond to stress. In particular, when we look at sex ratios, fewer males are born after population stress. Females remain relatively unaffected." It's a striking finding, said Thomas O'Connor, professor of psychiatry and psychology at the University of Rochester Medical Center, but the scientific literature has not been clear whether male fetuses are more affected by stress hormones. It's possible that male fetuses react differently to the stress hormones, said Dr. Sarah Berga, a professor and chairman of the department of gynecology and obstetrics at the Emory University School of Medicine. "We do know that the cellular machinery of males [and] females is more different than we used to think," she said. "We're in the cusp of beginning to understand it." Male babies born prematurely tend to encounter greater health problems such as respiratory distress and developmental delays than females, she said. High stress during pregnancy can cause complications including pre-eclampsia (high blood pressure after 20 weeks), preterm labor, low birth weight and congenital malformations. The 9/11 incidents induced "widespread social and economic disruption, leading to high levels of stress and anxiety," wrote the research authors. Bruckner and his two co-authors used data from the National Vital Statistics System that contained records of 23 million births to determine the number of fetal deaths reported in the United States between 1996 and 2002. They found the average fetal deaths in the month of September in those years. The mean monthly number of male fetal deaths was 995. But for the month of September 2001, the number spiked to 1,115, according to the research, and the actual number of miscarriages was likely higher because of under-reporting, Bruckner said. In the following December, the ratio of male-to-female births fell by 0.8 percent. While that appears small, Bruckner said it's still significant. "The sex ratio of live births, it's very stable. It doesn't jump up and down that much. It's very rare to have a sex ratio to change more than 1 percent," he said. "It's statistically meaningful," he said. "The sex ratio is responding to 9/11." This could mean that the number of males died before their expected delivery in December 2001. There were no statistically significant variations in the sex ratio eight, nine or 10 months after the terrorist attacks. "In terms of the take-home message, we know very little about what affects fetal loss," Bruckner said. "There's very little research on it. This paper suggests that we can identify these population stressors that can affect the likelihood of male fetal loss." More epidemiological research should be done on stressors, such as economic downturns and events that have a ripple effect in the population, Bruckner said. The idea that a collective traumatic event could affect pregnancy is plausible, said Berga. "There's nothing more contagious than emotion. If something bad happens, you have a negative contagion. Having something really bad happen, it strikes me it would resonate through a population," she said.

Underground terror[ism]

Source: http://www.ntnews.com.au/article/2010/06/20/157481_ntnews.html

"A deadly terrorist weapon could be buried in the backyards of Darwin's northern suburbs,

United States scientists fear. US authorities say melioidosis - commonly known as Nightcliff Gardeners Disease - is [caused by] a potential bioterror[ism] threat. The US Government believes the tropical disease, caused by soil-dwelling bacteria, could become the next anthrax-style bioterrorism threat. Melioidosis caught the attention of the US Government when it realised the naturally-occurring bacteria had the potential to be used as biological weapon. Australian and American scientists are now on the verge of a breakthrough in the early diagnosis of the disease which killed 10 people in the Northern Territory in the wet season. Professor Bart Currie, who works in the infectious diseases department at Royal Darwin Hospital and is the melioidosis project manager at Menzies School of Health Research, said interest in the bacteria from countries outside the endemic regions had grown dramatically in the past 10 years, particularly since the 2001 anthrax attacks [sic] in the US."

Survival rate up to 100% for late stage treatment of anthrax infections

Source: <http://www.prnewswire.com/news-releases/survival-rate-up-to-100-for-late-stage-treatment-of-anthrax-infections-96879099.html>

"IQ Therapeutics B.V., Groningen, the Netherlands, announced this week that in collaboration with the University of Texas Medical Branch it has obtained outstanding results for the treatment of inhalation anthrax. In a rabbit model up to 100% survival could be achieved with extended time to treatment (48h post infection) with a combination of two specific monoclonal antibodies developed by IQ Therapeutics. This has significant potential for saving lives of infected people who have no immediate access to treatment. IQ Therapeutics' Chief Scientific Officer Herman Groen states: 'The results obtained in the recent studies are unprecedented. We have demonstrated in a rabbit model that we can achieve up to 100% survival after treatment with a single dose of two antibodies (anti-PA [anti-Protective Antigen] and anti-LF [anti-Lactoferrin]), at 48 hours after the infection. Our advanced stage treatment is unique and has a tremendous advantage in real life settings where an infected person might not immediately be aware of the infection or does not have immediate access to proper treatment. Especially in those cases, IQ Therapeutics' dual antibody approach can in the future help saving lives, as there is currently no cure available for that stage of disease."

Israel to develop new nonconventional missile siren

Source: <http://www.jpost.com/Israel/Article.aspx?id=179021>



"In face of a potential war that could involve chemical and biological attacks against Israel, the IDF [Israeli Defense Force] Home Front Command is planning to develop a special siren for non-conventional missiles, The Jerusalem Post has learned. The possibility of using two different sirens during a future conflict - one for conventional missiles and the other for missiles carrying non-conventional warheads - came up during the nationwide civil defense exercise that was held last month called Turning Point 4. Since the Second Lebanon War in 2006, the IDF Home Front Command has invested in improving Israeli warning systems and has doubled, the number of sirens stationed throughout the country to a whopping 3,100. The command is currently working on installing sirens in military bases as well."

How bacteria make syringes to infect host cells

Source: <http://www.nano.org.uk/news/625/>

Scientists reconstruct bacterial transport channel in the test tube



Shigella flexneri, the causative agent of dysentery (orange), establishes contact with a human host cell (blue). The bar corresponds to a micrometer or a thousandth millimeter, respectively.

Image Credit: Volker Brinkmann, Diane Schad and Michael Kolbe.

For a successful infection, bacteria must outwit the immune system of the host. To this aim, they deliver so-called virulence factors through a transport channel located in the bacterial membrane. In some bacteria this transport channel is formed like a syringe, enabling them to inject virulence factors directly into the host cell. Scientists from the Max Planck Society and the Federal Institute for Materials Research and Testing have now succeeded for the first time in elucidating basic principles of the assembly of this transport channel. This is an important starting point for the development of new drugs that might interfere considerably earlier than antibiotics in the course of infection. (Nature Structural & Molecular Biology, 13 June 2010). Every day the human organism is confronted with a huge variety of pathogens. Most of them are fended off by our immune system. To execute a successful infection, bacteria must therefore manipulate the host to ensure their survival. They secrete virulence factors through a transport channel located in the bacterial membrane. Some bacteria, such as the causative agents of dysentery, food poisoning, typhoid fever, and pest, have developed a specialized transport mechanism called the Type three secretion system. Electron microscopy reveals that this structure is formed like a syringe: the base of the syringe is imbedded in the bacterial membrane, and the needle protrudes out of the bacteria. With this apparatus bacteria can inject virulence factors directly into the host cell. So far, little has been known about how bacteria build this nano-syringe. Scientists from the Max Planck Institute for Infection Biology in Berlin, the Max Planck Institute for Biophysical Chemistry in Göttingen, and the Federal Institute for Materials Research and Testing have now succeeded in elucidating fundamental principles of the needle assembly. This was made possible by reconstitution experiments which allowed them to study the assembly of proteins into a needle in the test tube. The close observation of these events revealed how the proteins are assembled into a syringe: the bacterium synthesizes the proteins in the cell interior, transports them through the syringe to the outside, and stacks them one after the other onto the tip of the growing needle. The scientists could also show that the proteins change their three-dimensional structure during the assembly process. They were able to pinpoint the exact structural changes down to the single amino acid level. These results provide new perspectives in the development of medications that might interfere very early in the course of infection. These so-called anti-infectives could inhibit the assembly of the needle and the injection of virulence factors into the host cell. This would be a major advantage over antibiotics, which have to travel through the membrane into the bacteria to be able to kill it. Furthermore, antibiotics cannot distinguish between good and evil, i.e. disease-causing bacteria, often leading to unwanted side effects. Lastly, the use of anti-infectives would circumvent the problem of antibiotic resistance development. The change of the three-dimensional structure of the proteins during the needle assembly was analyzed by X-ray structural experiments at BESSY in Berlin and ESRF in Grenoble and complementary NMR-spectroscopic experiments in liquid and solid phase at the Max Planck Institute for Biophysical Chemistry in Göttingen (Department Griesinger). The scientists compared the three-dimensional structure of the needle protein before and after

the needle assembly. BESSY (Berlin Electron Storage Ring Society for Synchrotron Radiation) and ESRF (European Synchrotron Radiation Facility, Grenoble): research facilities in which scientists from all over the world can use x-rays for structural analysis.

Bird and Animal Diseases

Source: <http://www.allstateanimalcontrol.com/diseases.php>

Safety precautions are necessary when working with pigeons, particularly if their droppings will be disturbed. Many pigeon diseases are transmitted through spores and fungus that grow in their feces. Pigeons are notorious disease carriers, earning them the nickname “flying rats”. They potentially carry Histoplasmosis, salmonella, Cryptococcosis, Psittacosis, pseudo-tuberculosis, and West Nile Virus, to name a few. Many of these pigeon diseases are not communicated by contact with the birds themselves, but rather with their droppings. Fungi and spores grow and multiply in and on their waste. When the droppings are disturbed,



such as when they are scraped up or swept up during cleaning, the spores and other dangerous particles become airborne and are potentially inhaled. This is the beginning of respiratory illness. Symptoms of Histoplasmosis include fatigue, fever and chest pains, and symptoms may be very mild or quite severe. One of our Allstate technicians contracted Histoplasmosis from pigeon droppings and developed the worst cough of his life which lasted for 3 months. The violent coughing also led to uncontrollable vomiting. He lost 15 pounds while ill and thought he would die. Fortunately he recovered, although he has since developed asthma as a result of the disease and occasionally has difficulty breathing. Pigeon diseases are nothing to sneeze at. They can cause serious repercussions and negatively affect quality of life. If you have a nuisance bird problem or a bird mess to clean up, don't take the risk of getting a pigeon disease. Find a professional to do the cleanup, one who has the proper equipment and protective devices to prevent the contamination from spreading. Allstate Bird and Animal Control has all the right gear for trapping and removing nuisance birds, and for cleaning up their droppings, feathers, and general mess. We can sanitize, deodorize, and disinfect any

affected areas, and can help you develop a long-term solution to the problem and avoid pigeon diseases. Build up of pigeon waste is not only unsightly, it is also a serious health hazard.

World War II Canadian lab made anthrax bombs: documentary

Source: http://www.google.com/hostednews/afp/article/ALeqM5jMuLO_MB1RuzCXQLUyM9z8-V7jdw

A top secret military lab set up in Canada developed biological weapons for the Allies during World War II, according to a new documentary film aired late Tuesday by Radio-Canada. In 1943 on Grosse-Ile, a small island in the Saint Lawrence seaway, Canadian scientists produced vast quantities of anthrax to be used in the fabrication of biological bombs. The so-called Project N was one of three great secrets of the war, equal in scope to the Allies'



cracking of German signal codes and the development of an atomic bomb, filmmakers Vincent Frigon and Yves Bernard opined. During this period, the Allies were preparing to wage a biological war against Germany and British Prime Minister Winston Churchill sought to obtain 500,000 anthrax bombs. After a few missteps, the lab was closed in August 1944 after producing some 70 billion deadly doses -- enough to wipe out the world's population 30 times over -- and the research was moved to the United States. Only 5,000 anthrax bombs would be sent to England before the end of the war. "The (leftover) batches were mixed with solvents, left to sit for awhile and then dumped at the bottom of the Saint Lawrence seaway," one of the researchers who worked on the project, Thomas Stovell, said in the film.

CBRNE-TERRORISM Newsletter

Δελτίο ΧΒΡΠΕ-ΤΡΟΜΟΚΡΑΤΙΑΣ

Volume 3 - 2010

A large, intense explosion is the central focus of the image, with bright orange and yellow flames and a thick plume of white smoke rising from the ground. In the background, a white fire truck is visible, its front end partially obscured by the explosion. The scene is set outdoors on a paved surface. A black rectangular box with white text is overlaid on the right side of the image.

RAD-NUKE –News

ANV S2 Radiation Detection & Monitoring for Ships and Submarines



The solution for radiological threat detection.

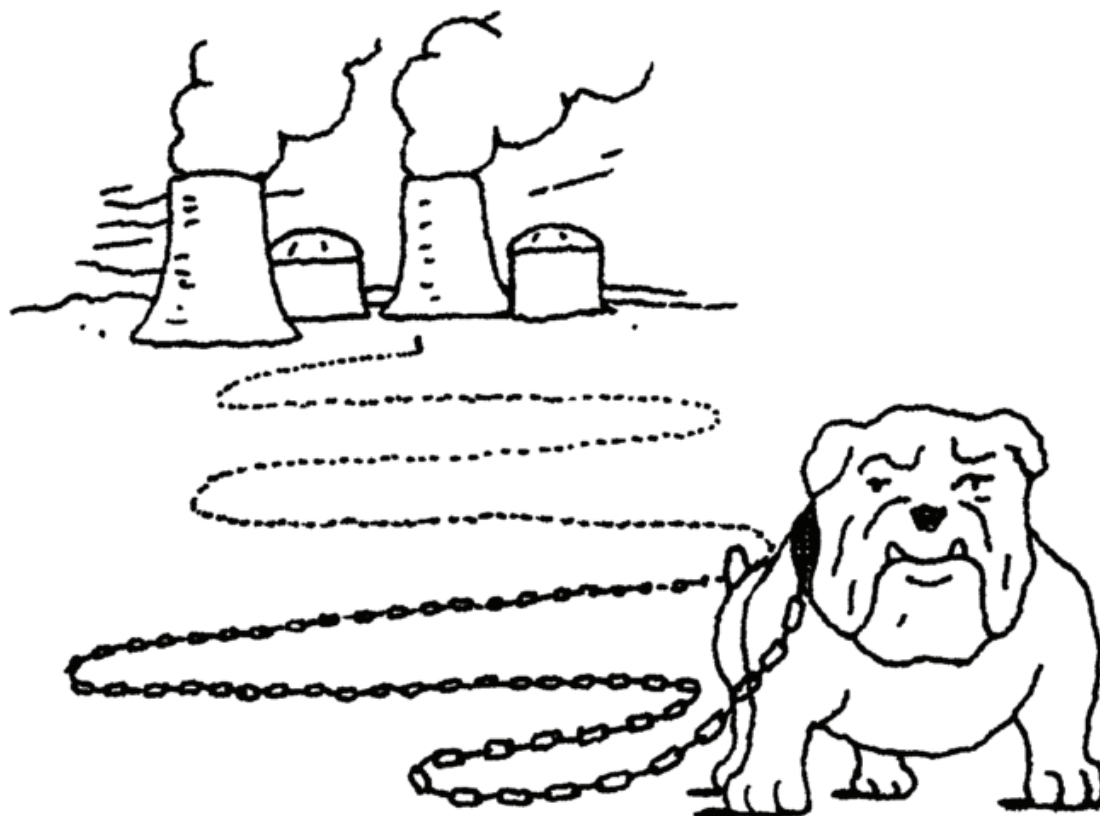
www.ultra-ccs.com

Ultra
ELECTRONICS

Al Qaeda's Nuclear Plant

Source: www.nytimes.com

ALL eyes are on Faisal Shahzad, the man charged with the attempted bombing in Times Square on Saturday. But perhaps we ought to be concerned a bit less with Mr. Shahzad, a failed terrorist now in custody, and significantly more with Sharif Mobley — a New Jersey native, a former high school wrestler and, until shortly before he moved to Yemen to allegedly join Al Qaeda, a maintenance worker at five nuclear power plants along the East



Coast. Since his arrest by Yemeni security forces in March, American law enforcement officials have taken pains to emphasize that Mr. Mobley's low security clearance makes it unlikely that he passed crucial details about American nuclear-plant security to Al Qaeda. But it doesn't take top-level clearance to know how to set off a nuclear meltdown. All it takes is information on perimeter security — information Mr. Mobley possesses about every plant where he worked. A nuclear power plant is very different from a coal- or gas-burning plant. If something goes wrong at such a plant, boilers can be quickly shut down, averting disaster. But there's no way to quickly shut off a reactor: the heat that builds up inside it is so intense that even if something goes wrong, cooling water must continue to circulate through its systems for days before it is safe. If the cooling system malfunctions, even if the rest of the plant is operating safely, the heat will literally melt the reactor and its concrete containment shell, releasing radioactive gas into the atmosphere — in other words, a partial nuclear meltdown like that at Three Mile Island in Pennsylvania in 1979. And it turns out that damaging a reactor's cooling system is a lot easier than getting to the core. You don't have to obtain access to the nuclear fuel, get into the control room or penetrate the containment shell. Most of the critical components of the cooling system, including pumps and water intake pipes, sit unprotected outside. If you can get a car bomb or a team with demolition charges near these components, you can shut off the cooling water to the reactor, and physics will take care of the rest. Even low-level employees at a nuclear plant would have the information necessary to pull off such an attack, like the number of guards, their weapons and procedures

at entry gates — even someone as low-level as Sharif Mobley. We don't yet know what kind of plant-security information, if any, Mr. Mobley passed on to Al Qaeda. But we do know that the organization has been interested in attacking American nuclear plants for years; it even considered including a plant on its Sept. 11 target list. For now, we have no choice but to assume that Mr. Mobley did in fact pass on details about plant security, and we need to take immediate steps to head off any possible terrorist attack. Defensive schemes at the plants where Mr. Mobley worked need to be significantly changed so that his information is no longer of value to any potential attacker. Guard procedures, for example, must be altered. Where such changes cannot adequately compensate for the potential risk Mr. Mobley presents, then defenses need to be strengthened. Security perimeters need to be widened. And more barriers must be put in place against car bombs. Once we have dealt with the plants where Mr. Mobley worked, we need to institute similar procedures at the remainder of the nuclear plants in the United States, because the unfortunate truth is that the defensive schemes at these sites are essentially all alike. For too long we've assumed that a nuclear plant is safe as long as its reactor is protected. Sharif Mobley knew better. Now, chances are, so does Al Qaeda.

Iraqi technicians dismantling Hussein's nuclear plants

Source: <http://edition.cnn.com/2010/WORLD/meast/05/16/iraq.nuclear.legacy/>

"The shell of former Iraqi strongman Saddam Hussein's efforts to produce a nuclear bomb is being slowly dismantled along the banks of the Tigris River, but its radioactive legacy lingers on. The Tuwaitha research complex, about 18 kilometers (11 miles) southeast of Baghdad, was bombed by Israel in its 1981 air strike on Iraq's Tammuz 1 research reactor. It was bombed again during the Persian Gulf War of 1991, and it was looted extensively after the 2003 U.S. invasion that ousted Hussein. Now, engineers and technicians are working to dismantle the laboratories and equipment at the site, but the extensive contamination left behind complicates their work. 'It is difficult because of the destruction,' said Anwar Ahmed, the project manager at Tuwaitha. 'This facility was bombed in 1991. Now, finally the decision was made to decommission all the destroyed facilities.' Workers and visitors have to wear protective suits and masks around the facility, where about 20 people are at work so far. Iraq's ministry of Science and Technology said it is training more specialists to decommission the facility, but acknowledged the cleanup could take decades."

The Effects of a Nuclear Detonation in LA: Must See Video for all First Responders

Source: <http://jennihesterman.blogspot.com/2010/05/effects-of-nuclear-detonation-in-la.html>

What if the bad guys are somehow able to defeat us and set off a nuclear weapon in downtown LA? Not a dirty bomb, but an actual 10 kiloton nuclear device that results in the stereotypical mushroom cloud over the city. How should first responders plan for this attack? What are the key actions that should be taken in the first hour, the second hour and beyond? How can we educate our public on what to do in the event of this attack? This briefing was conducted at the Radiological or Nuclear Incident & Clinical Application Seminar. It is presented by Brooke Buddemeier from the Lawrence Livermore National Laboratories and Global Security. Buddemeier works with DHS on preparation of cities for a nuclear detonation. He is a Certified Health Physicist and radiation safety specialist. I think you will agree this is an eye opening presentation. I encourage you to watch it from beginning to end



and absorb some critical information we don't often see in the public domain.

Some key points:

Technical:

- A 10 KT detonation gives off the light of 1,000 midday suns up to a mile away for about 15 seconds
- A 10 KT detonation is the equivalent of 5000 Oklahoma City attack truck bombs
- Creates a 600 foot crater
- 3 miles out of from the epicentre, glass will break in buildings - 800,000 people in LA affected within this 3 mile circle
- But, it's not all bad news - if you can get to shelter you could survive the fallout and there is particle decay as time goes by.

Planning:

- There is apathy in planning - most feel that if a nuclear weapon goes off response doesn't matter, we're all casualties, it's every man for himself. Or it is overwhelming to think about first response to such an event, therefore there are no plans.
- There are no regional response plans for a nuclear detonation
- There is a misunderstanding about local and federal response and responsibilities
- There is a lack of understanding about the technical aspects of a detonation and the right way to respond
- The first hours are critical and doing the right thing could mean saving hundreds of thousands of lives - or, doing the wrong thing could lead to the death of hundreds of thousands

It seems we don't want to wrap our minds around this type of an attack, but we must. The threat exists - al Qaeda has expressed interest in obtaining nuclear material and building a device; Hezbollah's sponsor Iran is a nuclear State; radical Islamist terrorist groups in Pakistan could get access through an attack on a facility, planting a mole, or a from a sympathetic scientist or engineer. We must plan as first responders. How do we communicate when the radios, cell-phones and computers go down as a result of an electromagnetic event? Do we rush out to help (first instinct) or shelter, survive, then help? Where are our shelters and is the public aware? Do we practice for this type of event and if so, is it realistic? We have to better educate our citizens. An educated populace is less fearful and their will to survive a detonation will be much higher armed with some knowledge than just operating from a position of fear. We can't be afraid to have this conversation with our public, they deserve to know and prepare. They shouldn't over rely on the government during times of crisis, as we've seen time and time again in the past. It strikes me that the generations before us were much more prepared - they knew the location of fallout shelters, for starters. Remember when the bank, the schools, etc in your hometowns had those black and yellow shelter signs? Our parents and grandparents had canned food and water as rations, a radio with batteries, a rallying point and safe area in their homes. There were civil preparedness drills and videos on TV about what to do in the event of a nuclear detonation or related emergency. It was a part of every day life that a nuclear attack was possible - not inevitable, but possible. This is our reality today, as well, although the average person probably gives it no thought at all.

Hope you find this video helpful in your planning efforts at work, in the community and in your home.

http://client.blueskybroadcast.com/Landauer/1282010/landauer09_v10/index.html

Report says Italy's nuclear wastes a terror risk

Source: <http://www.poten.com/NewsDetails.aspx?id=10446647>

Italy's dumps of nuclear waste and other radioactive material are vulnerable to terrorists and should be kept under strict security, a terrorism report released Monday said. The report by a private Italian foundation looks at the causes of Islamic terrorism and the evolution of al-Qaida and other terror groups since 9/11, with a particular eye to Italy. Analyzing the dangers



of an attack with nuclear weapons or radioactive "dirty bombs," the report says the fight for non-proliferation is bound to have a central role in anti-terror efforts and will require stricter cooperation among nations. Italy has a dozen sites where radioactive material is temporarily stocked, according to the report. These sites, the stocked material and their transfers "are vulnerable to terror attacks" and require measures to protect them from any terror risks. The report did not elaborate on the security measures currently in place. Italy closed nuclear plants after a referendum banned nuclear power in 1987. But the report says that the plants have produced 55,000 cubic meters of waste. There is also 2,000 cubic meters of other radioactive material coming from health and medical products, as well as waste produced by hospitals and chemical and other companies. Another risk, the report said, stems from the fact that there are active nuclear plants in nearby or neighboring countries. The report called for stricter coordination between local officials and the government, as well as between countries.

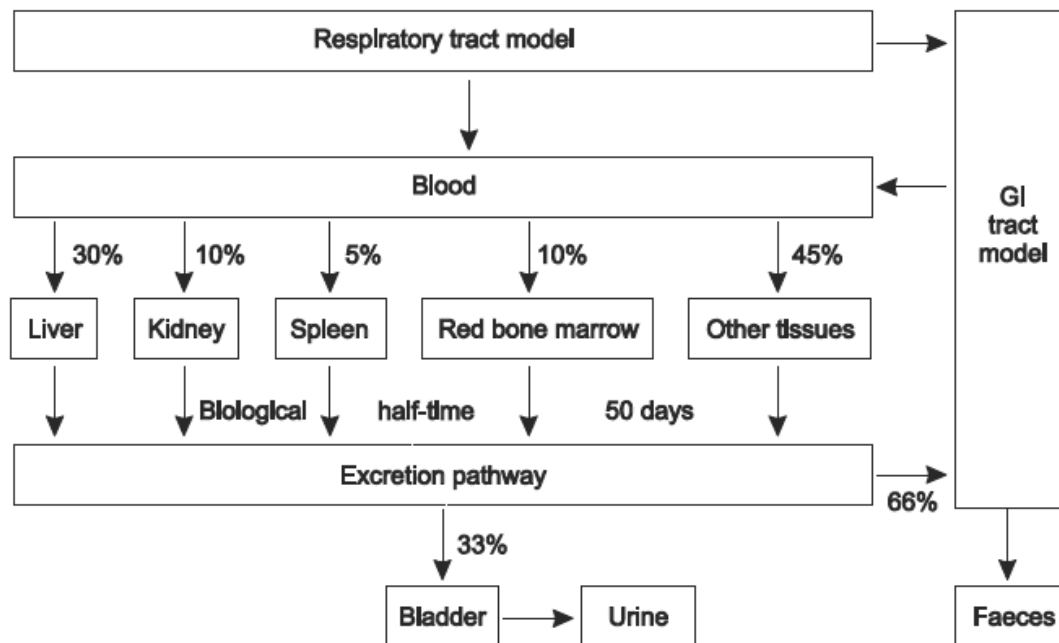
The report presented in Rome was the first one by the ICSA Foundation, a private body that analyses potential threats to national security and seeks counter strategies. For Italy, another threat comes from illegal immigration. This threat comes especially from North Africa, home to the group called al-Qaida in the Islamic Maghreb, or AQIM.

HPA-RPD-067 - Individual Monitoring Conducted by the Health Protection Agency in the London Polonium-210 Incident

Synopsis



The alleged poisoning of Mr Alexander Litvinenko with polonium-210 was an extraordinary event that presented some unique public health challenges. Environmental polonium-210 contamination was found at a number of locations in London, including parts of two hospitals, several hotels, restaurants, and office buildings. An extensive programme of individual monitoring of potentially exposed persons was rapidly initiated, based on urine sampling. At each location, risk assessments were undertaken to identify persons with significant risk of contamination with polonium-210. These individuals were invited to provide samples, not only to enable a direct assessment to be made of their own exposure, but also to inform decisions on whether others connected with the site should also provide samples or could be reassured. Urine samples from 753 people were processed: about 500 during the first month, another 250 up to the end of May 2007, and a further three up to August 2007. Of these, 139 measurements were above the Reporting Level set by the Health Protection Agency for this incident of 30 mBq d-1, showing the likely presence of polonium-210 from the incident. Committed effective doses were assessed for measurements above the Reporting Level. Most were less than 1 mSv, with thirty-six in the range ≥ 1 mSv and <6 mSv, and seventeen ≥ 6 mSv, with the highest about 100 mSv.



Drug Mitigates Toxic Effects Of Radiation In Mice

Source: <http://www.unc.edu>

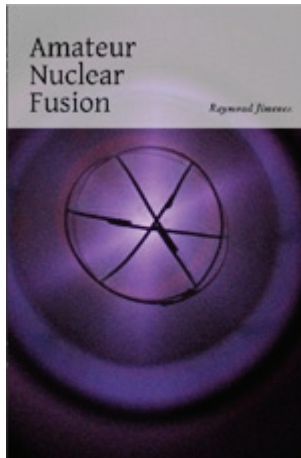
The most important acute side effect of radiation poisoning is damage to the bone marrow. The bone marrow produces all the normal blood cells, and therefore a high dose of radiation can lead to low blood counts of red cells, platelets and white blood cells. Humans that receive a lethal dose of radiation as in the setting of an accidental exposure die of bone marrow failure. While there are a few drugs that will decrease toxicity when given before exposure to radiation (“radioprotectants”); currently, no effective therapy exists to mitigate bone marrow toxicity of radiation when given after radiation exposure (“radiomitigants”). The identification of successful human radiomitigants is a top research priority of the U.S. Department of Homeland Security and National Institutes of Health. In a study published today in the *Journal of Clinical Investigation*, a team led by UNC Lineberger Associate Director for Translational Research, Norman Sharpless, MD, provides a first example of successful radiomitigation in mammals. The investigators found that oral treatment of mice with a drug that inhibits enzymes involved in cell division caused certain groups of bone marrow cells to temporarily stop dividing (which they termed ‘pharmacological quiescence’ or PQ). Several decades of work have shown that cells which are not dividing are resistant to agents that damage DNA, like radiation. Workers in the Sharpless lab were then able to show that the induction of PQ immediately before or up to 20 hours after radiation exposure were able to protect mice from a lethal dose of radiation. PQ protected all the normal cells of blood, including platelets, red cells and white cells. “We believe this study is really exciting. We have identified a simple, non-toxic pill that decreases radiation toxicity even when given after radiation exposure. We believe this approach could be of use in humans who are accidentally or intentionally exposed to lethal doses of radiation,” said Sharpless, who is an associate professor of medicine and genetics at UNC’s School of Medicine. PQ relies on the use of potent and selective inhibitors of cellular enzymes called CDK4 and CDK6. Related drugs have been used extensively in humans with cancer, and CDK4/6 inhibitors are currently being tested in humans. Importantly, these drugs can be given as a pill, are chemically stable and have little toxicity. Therefore, such compounds could be stockpiled for use in the setting of an unexpected radiological disaster. The group showed that structurally different versions CDK4/6 inhibitors provided protection from radiation, whereas other types of kinase inhibitors did not. Sharpless believe PQ may have a role in treating patients with cancer. Radiation is used in cancer therapy, and therefore PQ might benefit such patients. Also, several commonly used chemotherapy drugs cause bone marrow toxicity by damaging DNA, and therefore PQ might protect from chemotherapy toxicity in addition to radiation toxicity. A concern is that PQ might also protect a patient’s tumor from the toxicity of therapeutic DNA damaging agents, but the Sharpless group showed that at least some types of cancer were not protected by inhibitors of CDK4/6. Bone marrow protection is a major issue in medical oncology, with billions of dollars of growth factors used annually in the US alone for this problem. In particular, PQ protects platelets and red cells, which are largely unmet needs in current clinical oncology. UNC has filed patents related to these discoveries, which have been licensed to an RTP-startup company called G-Zero Therapeutics, which was co-founded in 2007 by Sharpless and researchers in Boston and San Francisco.

Web developer builds nuclear reactor in Brooklyn warehouse!

Source: http://news.yahoo.com/s/ynews/20100623/sc_ynews/ynews_sc2797

It sounds like the premise of an especially geeky comic book: Web developer by day, trailblazing nuclear engineer by night. Mark Suppes is a Web developer for the fashion house Gucci, but in his off-hours, he tinkers with his homemade nuclear-fusion reactor in a Brooklyn warehouse, unknown to his neighbors. In a video interview with BBC News' Matthew Danzico, Suppes cheerfully shows the reporter how his reactor works, warning him to step back as the machine activates and emits a small amount of radiation. The reporter is heard laughing nervously in the background, telling Suppes to be careful. Suppes' is the **38th homemade reactor built by an independent amateur scientist**, according to Fusor.net. On

that website, "fusioners" discuss attempts to create a nuclear-fusion reactor that produces as much energy as it consumes, a problem that has plagued some of science's greatest minds. Though several Brooklyn locals expressed unease to the BBC at the idea of hosting a fusion



startup in their neighborhood, the process is entirely legal in the United States. As scientists explained to the BBC, experimental fusion devices don't actually use fissionable materials like uranium. Instead, fusion reactors seek to force together the nuclei of atoms at high temperatures — a procedure that releases energy as the combined atoms form larger nuclei. Perhaps the most salient question about Suppes' hobby, then, is whether it's a waste of time. Government-led research of fusion technology is funded on a far more lavish scale than Suppes' \$35,000 DIY project. (Fusion energy is the holy grail of green technology, since it produces no nuclear waste or greenhouse gases.) "I won't say something that puts these guys down, but it's a tricky situation because there is a great deal of money and time and a lot of very experienced scientists working on fusion at the moment," said

Neil Calder, spokesman for Iter, a multinational project focusing on fusion power. Not that Suppes is expecting his fusion dreams to be contained in his Brooklyn warehouse space. He says he's hoping to raise millions of dollars to scale up the reactor. Still, a do-it-yourself, door-to-door fundraising approach probably isn't advisable in this case. "I would have thought there would be some sort of rules and laws about messing around with nuclear fusion in your apartment," Brooklyn resident Stephen Davis told the BBC. "I'm not sure I'd like that living right next to me."



CBRNE-TERRORISM Newsletter

Δελτίο ΧΒΡΠΕ-ΤΡΟΜΟΚΡΑΤΙΑΣ

Volume 3 - 2010

A photograph of a white military truck, possibly an ambulance or transport vehicle, that has been severely damaged and is engulfed in a large, intense fire. The fire is bright orange and yellow, with thick black smoke rising from it. The truck is positioned in the center-left of the frame, and the fire is concentrated around its front and side. The background is a blurred, outdoor setting.

CYBER –News

Versatility and reliability are the cornerstones of the TASER Shockwave system. To ensure complete reliability no matter when called upon, each TASER Shockwave unit contains a lithium battery pack that can be kept in a constant state of readiness via recharging from the Control Box.

The TASER Shockwave is an operator controlled, six-shot device that covers a 20-degree arc with 25 foot cartridges. When activated, the Control Box will initiate the simultaneous discharge of all six cartridges delivering a five-second TASER Neuro Muscular Incapacitation (NMI) effect.



Covers a 20-degree arc

TASER International is an industry leader in products, training, and support to law enforcement agencies in more than 40 countries throughout the world. Our **innovative** technologies and systems have revolutionized law enforcement by providing the tools they need to **protect** themselves and the public as they keep our communities **safe**.

TASER CUSTOMER SERVICE

17800 North 85th Street
Scottsdale, AZ 85255

Toll Free: 800 978 2737
Direct: 480 991 0797
Fax: 480 991 0791

Email: Sales@TASER.com



When the TASER Shockwave system is deployed in a stacked configuration, each activation of the trigger commands a sequential deployment of TASER cartridge rows via an intelligent networking system. This allows each unit to know where it is in the array of multiple systems. As a protective measure when waves of target sets are encountered, additional five-second exposures are administered to already expended rows with every additional deployment. The TASER Shockwave keeps previously targeted personnel down and incapacitated while subsequent target sets are engaged – a truly scalable defense in depth capability.



Vehicle Mountable



www.TASER.com

MPC0054 Rev: A

©2009 TASER International, Inc. TASER, Shockwave, and the Lightning Bolt logos are trademarks of TASER International, Inc. All rights reserved.



Area Denial and Force Protection System

Fully Modular System

The TASER® Shockwave™ system is designed as a fully modular system, allowing the end user complete flexibility to deploy as needed to achieve the desired objective. Multiple TASER Shockwave units can be stacked together either horizontally in order to extend area coverage, or vertically to allow multiple salvo engagements; or daisy chained together to maximize either area coverage or cartridge pattern density. These features provide the capability to project Area Denial from a secure location.

Remote Area Denial Technology

The TASER Shockwave system is the first generation of new TASER Remote Area Denial™ (TRAD) technology allowing for both increased safety and stand-off capability during hostile situations through the innovative use of TASER International's field-proven TASER® X26™ Neuro Muscular Incapacitation (NMI) technology.

Stand-off Distance

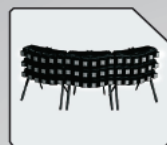
The TASER Shockwave system minimizes risk as the system can be activated with the push of a button on the Control Box at a safe stand-off distance of up to 100 meters. The TASER Shockwave unit deploys its cartridges up to 25-feet, to instantaneously incapacitate multiple personnel within the field of coverage.

Multiple Deployments

The TASER Shockwave device has the ability to de-escalate/defuse violent crowd/riot situations, with the only safer response to resistance Area Denial incapacitating device, by deploying multiple TASER cartridges that are oriented across a wide area arc.

Ease of Operation

The TASER Shockwave system is easily set-up and operated by trained personnel. Training certification can be accomplished in a matter of hours.



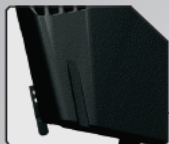
Intelligent Networking System

An intelligent networking system gives each TASER Shockwave the ability to know where its position is within an array of multiple systems.



Multiple Unit Configuration

The TASER Shockwave can be arranged in vertical and horizontal configurations with up to 12 units on a single control box, allowing up to three salvos.



Manual Sighting System

Ensures user accuracy.



Self-Supporting Leg System

The TASER Shockwave system can be deployed in virtually any terrain.



Unit Payload

Each single TASER Shockwave unit has a payload of six TASER cartridges, allowing for multiple person incapacitation through Area Denial.



Versatile Mounting System

The TASER Shockwave can be mounted on a variety of objects, such as vehicles, or fencing.



Computer program turns complex data into brilliant images

Source: <http://www.ksl.com/>

The future of computers is here, and University of Utah scientists keep pushing the envelope.



They have developed new imaging programs that turn complex data into brilliant pictures you can view on your iPhone or iPad. [ImageVis3D Mobile](#) became available last fall, and new applications are emerging. The latest is an app that simulates a nuclear reaction. The colorful, clear, 3-D images are created by ImageVis3D. The program takes abstract phenomena and data and turns it into something we can see and better understand. Those pictures help

with teaching college students and with collaboration among professionals. They also point to the future of computers for all of us. ImageVis3D, developed by Jens Krueger and Tom Fogal at the Scientific Computing and Imaging Institute at the University of Utah. "The average computer user can now visualize and look at their data in real time, regardless of how large it is," says Fogal. "That's what motivated us to develop the software in the first place." The user can manipulate a wide range of 3D images of medical, scientific and engineering data. Scientists can study anatomy, climate, fuel efficiency. The user assigns colors to specific pieces of data. "I want 19 to be red. I want green to show up for the numbers 32 through 36. And, by doing that and iterating over that process, they can bring out the features of their data set that they're interested in," says Fogal. This technology helps teach a new generation of

computer-savvy, visually-oriented students. Tatjana Jevramovic is the Director of the Utah Nuclear Engineering Program. She used the technology in her classroom this semester and says the students loved it. "So, if I show to them in the classroom something like this, very attractive with a lot of colors, they are very capable to understand easily and much faster abstract phenomena," says Jevramovic. Abstract phenomena like a fission reaction in a nuclear reactor: There's a new app for that. Jevramovic can display complex simulations of a nuclear reactor's core on an iPod, iPhone or iPad. The technology also helps researchers look at nuclear power plants and share performance information. So, what does all of this mean to the average computer user? In the future, Fogal says, it means we'll all be able to download more complex material onto even smaller computer devices. "This is stuff they would need a supercomputer for ten years ago," says Fogal. "So, I'm kind of thinking the things that we're doing on supercomputers now, I'll be doing in the palm of my hand in 10 years."



Jevramovic agrees. "Not everyone can have supercomputers at home, nor will that be the future," she says. "But, that could be the future, really," she says pointing to her iPhone. Whatever that future brings, computer scientists and their collaborators from other departments plan to stay on the cutting edge. The reactor simulation software is not available commercially, but you can get ImageVis3D free at the Apple iTunes Store.

The cybersecurity boom

Source: www.washingtonpost.com

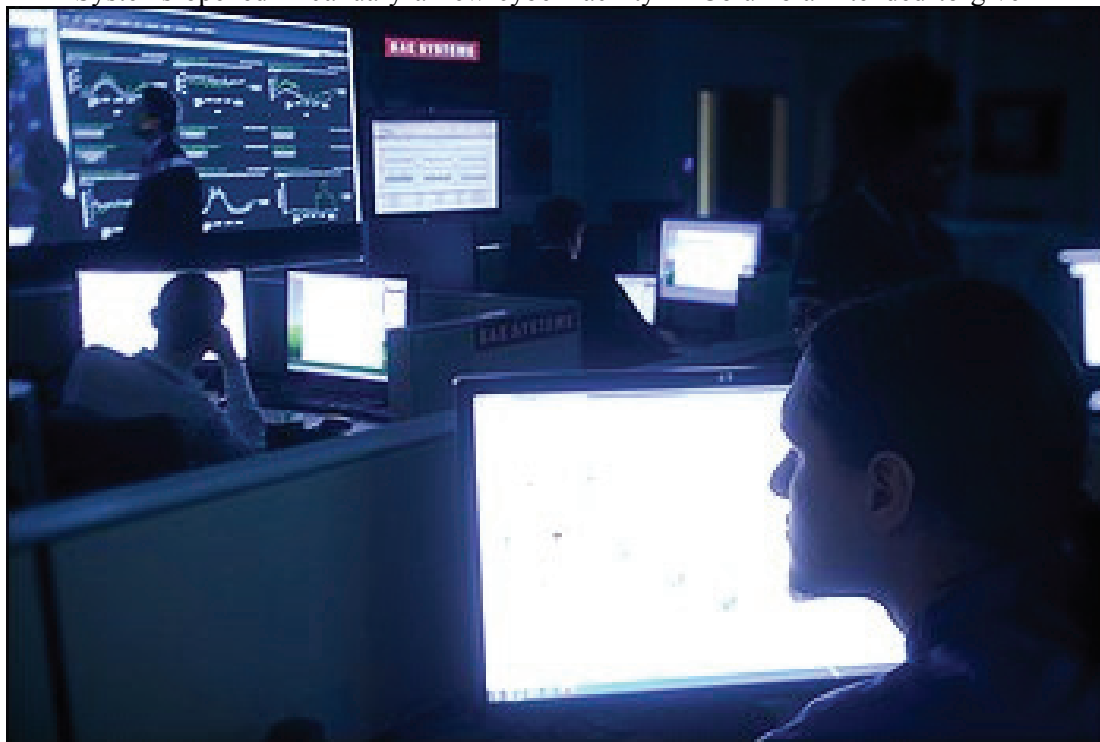
When cybersecurity firm Triumfant was founded in late 2002, it developed software meant to assist help desks in managing information technology problems. The company soon found a more valuable use for its software: detecting malicious acts on networks of computers and



making automatic fixes. Earlier this year, the small Rockville-based firm, which has fewer than 20 employees, announced it is partnering with Fairfax-based SRA International, a major government contractor, to beef up SRA's cybersecurity product. The company -- which today works exclusively in the cybersecurity field -- is just one of the beneficiaries of what analysts say is a growing boom in cybersecurity work. From small, recently-established firms

all the way up to the well-known defense contracting giants, local companies are building up their cyber credentials. There's plenty of reason for the surge. The increasing number and intensity of cyberattacks has attracted the attention of the Obama administration and Congress, which have begun steering new dollars to the problem. And much of that new spending is focused on the Washington region, as the federal government consolidates many of its cybersecurity-focused agencies in the area. With the National Security Agency, the soon-to-be-relocated Defense Information Systems Agency and the newly-founded U.S. Cyber Command at Fort Meade; the Department of Homeland Security set to move to Anacostia; and the Pentagon just across the river, a region known for information technology is fast becoming a cybersecurity capital. "There's this gravitational pull in Washington," said Philip Eliot, a principal at the D.C. private equity firm Paladin Capital Group. David Z. Bodenheimer, a partner at law firm Crowell & Moring in Washington who leads the firm's homeland security practice and specializes in government contracts, said the unclassified portion of the federal government's cybersecurity work is estimated at \$6 to \$7 billion annually. The classified portion is likely just as large -- and potentially bigger, he said. "I think it is a real growth opportunity in coming years," Bodenheimer said. "The market is still rather fragmented and in flux, but is developing with a speed that it is attracting both the major defense and homeland security contractors who are establishing independent business units to pursue these opportunities, and it is also a real opportunity for the smaller players who have niche products." As start-ups and others rush to stake claims, some wonder if a bubble of sorts is beginning to inflate. Roger Novak, founder of Novak Biddle Venture Partners, recalled that many venture firms in the early 2000s chased similar prospects. "A lot of the early people made significant money, but there were a lot of 'me too' companies," he said. "So a lot of people in the investment community probably absorbed losses in the space and began to move on." But now, he said, the administration's focus is once again piquing venture interest and spurring larger companies to pursue acquisitions of companies that already have cybersecurity footholds. Novak is bullish on the sector; after all, his firm invested in Triumfant in 2006. Eliot said key opportunities right now are in securing mobile devices, protecting against Web-based attacks that come from reputable Web sites, and fending off internal threats. Those are problems "that to date don't have good solutions," he said. One reason the field is attracting so many companies is that the barriers to entry are low -- at least relative to other defense industries. "The strictly defense markets largely have strictly defense suppliers," said David L. Rockwell, a senior analyst at the Teal Group. "In

cybersecurity -- so far you [have] had a lot more variety in who's able to get contracts, and I think we can expect that to continue." The big defense contractors are moving quickly to protect their turf. Lockheed Martin in late 2009 opened what it calls the NexGen Cyber Innovation and Technology Center, a research and development center, in Gaithersburg. The center brings together 14 companies -- including Hewlett-Packard, Intel, McAfee, Microsoft and Symantec -- that make up a cybersecurity technology alliance formed at the same time. BAE Systems opened in January a new cyber facility in Columbia intended to give BAE a



"world-class analytical capability," said John Osterholz, the company's vice president for cyberwarfare and cybersecurity. Staffed by 20 to 25 people, the office helps BAE quickly understand and characterize threats. And Chantilly-based TASC, divested from Northrop Grumman last year, has named a new lead executive for its cyber business, said TASC's president and chief executive, Wood Parker. "I'm sure that every company says that they are interested or they have a cyber business," he acknowledged. "I can tell you that TASC has a robust cyber business today." The largest IT and defense contractors are keenly interested in helping the government manage its computer networks. Lockheed Martin, Boeing, General Dynamics, ManTech International, Northrop Grumman and SAIC (which recently acquired CloudShield Technologies) are all competing in the space. Smaller companies see more opportunity in creating products that can protect networks or help the government keep tabs on threats -- especially if that gear and software can be deployed across agencies and departments. A key player in shaping future business is likely to be the Commerce Department, chiefly via the National Institute of Standards and Technology in Gaithersburg. NIST has been systematically revising its extensive collection of guidance documents for network security. It is including industry and military experts in these revisions in an attempt to unify approaches taken by the federal government broadly. NIST figures prominently in legislation making its way through Congress. A major bill, reported out in late March by the Senate Commerce, Science and Transportation Committee, chaired by John D. Rockefeller IV (D-W.Va.) would create a cybersecurity advisory panel with the White House, designate the Commerce Department as the clearinghouse for cyberthreat information, and strengthen NIST's authority to set cybersecurity standards for federal contractors and grant recipients. The bill, S 773, would also give the National Science Foundation new authority to establish what it calls a Federal Cyber Service: Scholarship for Service program. On the House side, the Homeland Security, Science and Technology Authorization Act would double the money available to DHS for cybersecurity research and development.

Buying a Cyberattack

Source: <http://www.nationaldefensemagazine.org/archive/2009/December/Pages/BuyingaCyberattack.aspx>

Together, thousands of computers can perform complex tasks that would crash a single machine. When used for good, these linked machines are called a grid computer. When used



for evil, they're called a botnet. Parabon Computation, a Virginia-based technology company, is using its grid computer to simulate the destructive effects of a botnet. This allows Parabon's clients to analyze their networks' abilities to withstand potential cyberattacks. Such an attack occurred in August, when cyber-criminals paralyzed Twitter.com, rendering the social-networking website inaccessible for hours. These criminals typically use spam emails and other tactics to spread malicious software to thousands — sometimes millions — of computers. The linked computers form a botnet, and the criminals can instruct them to log onto a specific website, overloading the site with traffic and shutting it down. The tactic, called a

denial-of-service attack, is used for political and monetary gain — or just to wreak havoc. "After testing our clients' systems, we'll work with them to develop remediation plans," says Steven Armentrout, Parabon's founder and chief executive officer. "There are various challenges to guarding against denial-of-service attacks. You have to find IP addresses that are generating tons of traffic and divert them." Parabon leases idle space on unused computers at university laboratories, and the company links them into a grid that can process high-volume information. For instance, the Defense Department uses Parabon's 10,000-computer grid to analyze its contract data, Armentrout says. Parabon is now marketing its denial-of-service simulator, called Blitz, to government agencies and businesses that are likely targets for Internet criminals. With Blitz, Parabon's thousands of linked computers log onto clients' websites simultaneously. They overload the sites with traffic, and the clients then analyze their networks' resiliency. Armentrout demonstrated Blitz for National Defense. He instructed the program to hit one of his company's websites 2,000 times per second. At first, the site loaded instantly. A minute later, the site wouldn't refresh at all.

Car hackers can kill brakes, engine, and more

Source: <http://www.autosec.org/>

University researchers have taken a close look at the computer systems used to run today's cars and discovered new ways to hack into them, sometimes with frightening results. In a paper set to be presented at a security conference in Oakland, California, next week, the security researchers say that by connecting to a standard diagnostic computer port included in late-model cars, they were able to do some nasty things, such as turning off the brakes, changing the speedometer reading, blasting hot air or music on the radio, and locking passengers in the car. In a late 2009 demonstration at a decommissioned airfield in Blaine Washington, they hacked into a test car's electronic braking system and prevented a test driver from braking a moving car -- no matter how hard he pressed on the brakes. In other tests, they were able to kill the engine, falsify the speedometer reading, and automatically lock the car's brakes unevenly, a maneuver that could destabilize the car traveling high speeds. They ran their test by plugging a laptop into the car's diagnostic system and then controlling that computer wirelessly, from a laptop in a vehicle riding next to the car. The point of the research isn't to scare a nation of drivers, already made nervous by stories of software glitches, faulty brakes and massive automotive recalls. It's to warn the car industry that it needs to keep security in mind as it develops more sophisticated automotive computer systems. "We think this is an industry issue," said Stefan Savage, an associate professor with

the University of California, San Diego. He and co-researcher Tadayoshi Kohno of the University of Washington, describe the real-world risk of any of the attacks they've worked out as extremely low. An attacker would have to have sophisticated programming abilities and also be able to physically mount some sort of computer on the victim's car to gain access to the embedded systems. But as they look at all of the wireless and Internet-enabled systems the auto industry is dreaming up for tomorrow's cars, they see some serious areas for concern. "If there's no action taken on the part of all the relevant stakeholders, then I think there might

Experimental Security Analysis of a Modern Automobile

Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, and Tadayoshi Kohno

Department of Computer Science and Engineering

University of Washington

Seattle, Washington 98195-2350

Email: {supersat,aczeskis,franzi,shwetak,yoshi}@cs.washington.edu

Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and Stefan Savage

Department of Computer Science and Engineering

University of California San Diego

La Jolla, California 92093-0404

Email: {s,dlmccoy,brian,d8anders,hovav,savage}@cs.ucsd.edu

be a reason to be concerned," Kohno said. Neither he nor Savage would name the maker of the car they conducted their tests on. They don't want to single out any one auto-maker, they said. That probably comes as a relief to whoever made the car the researchers probed, as they found it pretty easy to hack. "In starting this project we expected to spend significant effort reverse-engineering, with non-trivial effort to identify and exploit each subtle vulnerability," they write in their paper. "However, we found existing automotive systems—at least those we



tested—to be tremendously fragile." To hack the cars, they needed to learn about the Controller Area Network (CAN) system, mandated as a diagnostic tool for all U.S. cars built,

starting in 2008. They developed a program called CarShark that listens in on CAN traffic as it's sent about the onboard network, and then built ways to add their own network packets. Step-by-step, they figured out how to take over computer-controlled car systems: the radio, instrument panel, engine, brakes, heating and air conditioning, and even the body controller system, used to pop the trunk, open windows, lock doors and toot the horn. They developed a lot of attacks using a technique called "fuzzing" -- where they simply spit a large number of random packets at a component and see what happens. "The computer control is essential to a lot of the safety features that we depend on," Savage said. "When you expose those same computers to an attack, you can have very surprising results, such as you put your foot down on a brake pedal and it doesn't stop." Another discovery: although industry standards say that onboard systems are supposed to be protected against unauthorized firmware updates, the researchers found that they could change the firmware on some systems without any sort of authentication. In one attack that the researchers call "Self-destruct" they launch a 60 second countdown on the driver's dashboard that's accompanied by a clicking noise, and then finally warning honks in the final seconds. As the time hits zero, the car's engine is killed and the doors are locked. This attack takes less than 200 lines of code -- most of it devoted to keeping time during the countdown. Hacking a car isn't for the faint-hearted. At several points the team worried it might have come close to permanently damaging the two identical-make cars it experimented with, but that never happened, Kohno said. "You really don't want software to accidentally change critical parts of the transmission," he said.

Man infects himself with computer virus

Test shows possible security issues about chip use in medical devices

Source: http://www.msnbc.msn.com/id/37360942/ns/technology_and_science-security/

University of Reading researcher Mark Gasson has become the first human known to be infected by a computer virus. The virus, infecting a chip implanted in Gasson's hand, passed into a laboratory computer. From there, the infection could have spread into other computer chips found in building access cards. All this was intentional, in an experiment to see how simple radio-frequency identification (RFID) chips like those used for tracking animals can host and spread technological diseases. The research from the British university shows that as implantable bionic devices such as pacemakers get more sophisticated in the years ahead, their security and the safety of the patients whose lives depend on them will become increasingly important, said Gasson. "We should start to think of these devices as miniature computers," Gasson said. And just like everyday computers, they can get sick.

Down with disease

Gasson had a relatively simple chip implanted in the top of his left hand near his thumb last year. It emits a signal that is read by external sensors, allowing him access to the Reading laboratory and for his cell phone to operate. He and his colleagues created a malicious code for the chip. When the lab's sensors read the code, the code inserted itself into the building computer database that governs who has access to the premises. "The virus replicates itself through the database and potentially could copy itself onto the access cards that people use," Gasson said. The experiment showed that implants which wirelessly communicate with other computers can infect them and vice versa. Gasson said he knows of no instances to date of bionic devices having been contaminated by computer viruses. But the threat will grow with the number and complexity of these devices. Besides pacemakers for people with heart trouble, other modern bionic devices include cochlear implants for the hearing impaired and deep brain stimulators — a "brain pacemaker" — for neurological conditions such as Parkinson's disease. Years ahead, this surgically implanted hardware may not only be for people with medical conditions. Bionic enhancements, much like today's cosmetic surgery, could boost memories and IQs. A side effect mentioned in cases of deep brain simulation is patients who have experienced greater creativity, Gasson said.

Wash your digital hands

To fight communicable diseases caused by bacteria, viruses and fungi, we take precautions such as washing our hands. To counter threats of technological agents, Gasson said we are quite accustomed to keeping our computers updated with antivirus software and exercising caution online. A similar degree of hygiene and awareness may be necessary to keep the devices in our bodies clean as well. "I don't think for us that (infectious technological agents) would be a particularly new concept, but implants in our bodies will make it a lot more real," Gasson told TechNewsDaily. "A denial-of-service attack on a pacemaker, if such a thing were possible, would of course be very detrimental."

University of Arizona Researchers Combat Terrorism in Cyberspace

Source: <http://computerfreesoftware.co.cc/?p=91>

The U.S. has no deficiency of renowned colleges and universities. Americans may not be aware, though, of one university's reply to the post-9/11 War on Terror that is uniquely patriotic and beneficial. For years now, top-level computer scientists at the University of Arizona's artificial intelligence lab have been working with focused determination to collect and analyze terrorist Internet content, their response to the ubiquitous concern that the United States does not lose the War on Terror on the Internet. Their project has resulted in the creation of an exclusive resource available to all approved terror-fighting bodies, the Dark Web Project. In their work on the Dark Web Project, the individual University of Arizona staffers have promoted their team to the status of being pre-eminent authorities in the mechanisms and technology available for uncovering and tracking terrorists where they foment their violence – in cyberspace. Terrorists' use of the Internet to foment, recruit, and finance their violence is an increasing problem. In 2006, one leading Israeli scholar, Dr. Gabriel Weiman of the University of Haifa, believed there were approximately 5,000 terrorist websites. However, in 2007, researchers in the artificial intelligence lab at the University of Arizona revealed that there were likely 10 times that number – 50,000 terrorist web sites – based on five years of their web spiders moving throughout the Internet and bypassing passwords to gather and document the Dark Web terrorist content in the Web 2.0 environment. In 2008, PC Magazine Online reported that terrorists were disseminating directives and tutorials to followers on how to upload videos of successful attacks to Google's YouTube video sharing site. Indeed, a crucial portion of online terrorist videos relate to IEDs (improvised explosive devices). Those who know anything at all about terrorist forces in the world understand that the Internet has long been exploited as a recruiting and radicalizing instrument as well as a fund-raising tool. Members of the University of Arizona's Dark Web Project team reported in early 2010 that they had collected more than 1 million still images and 15,000 videos from terrorist sites and saved them to their servers. These files, as well as written content by terrorist/extremist authors (e.g. blog posts, forum chitchat, and social networking posts) are available to approved users (the military or intelligence community, for example) via a searchable portal or interface. In creating the Dark Web Project, Dr. Hsinchun Chen and his research team of computer and information scientists at the University of Arizona's artificial intelligence lab have responded to what they believe is the "dire danger" of the U.S. and its allies losing the War on Terror in cyberspace. Funded by the National Science Foundation and some other government agencies and private sources, the Dark Web Project team utilizes a wide variety of software package tools they have developed or adapted to document and identify sources of terrorist content. Using strategies within the discipline of artificial intelligence, the software programs seek to unmask and make sense of the terrorists' world for the benefit of intelligence agencies and military leaders. First and foremost, the Dark Web team uses hacking techniques to send spiders and web crawlers to collect content and trace web interactions. In 2010, the Dark Web researchers claimed to periodically collect the complete contents of about 300 terrorist forums, with some large radical sites boasting more than 30,000 members and nearly a million messages. They had also exposed a terrorist presence in at least 30 virtual world sites. The team focuses on known Al Qaeda sites as well

as some home grown terror cells in Europe. They believe they have the largest open-source terrorist aggregation in the world, although (like everyone else) they have no idea what the U.S. intelligence or defense agencies are doing. These University of Arizona researchers, who identify themselves as more “computationally oriented” than other anti-terrorism strategists and analysts, have invented and implemented a wide array of analytical tools that each contributes to an integrated understanding of how terrorism on the Web is evolving, and yields specific information that can be used by anti-terrorism forces fighting our enemies in the real world. Identities and connections are just a commence point for what the computer scientists are able to discern about the Dark Web. One forensic linguistics tool they developed, Writeprint, identifies unique authors of terrorist rhetoric and hate speech with 95 percent accuracy, enabling the U.S. and its allies to take action against them. Dr. Chen led the team that developed the Writeprint program, the name alluding to “written fingerprint.” Its sophistication and multi-language capability make it very difficult for terrorists to scam this invention to bypass the anti-terrorism efforts of the U.S. and its allied Western nations. If it were possible to outsmart the Writeprint program, every terrorist would essentially need to be an expert linguist, consciously altering his usual composition pattern and style as he would post his hate speech to forums or blogs in one of the tool’s languages. (But then, wouldn’t the “altered” text bear its own Writeprint?) Writeprint identifies unique authors of anonymous content by analyzing four aspects of written communications: lexicon (vocabulary richness); syntax (writing style with respect to punctuation and function words); structural features (sentence duration, paragraph length, capitalization, and style rules); and content features (keywords and themes). The software establishes and codes an author’s background characteristics from an initial sample, and then is able to actively see similar background characteristics while processing batches of written material, further refining the unique author’s profile with a high degree of accuracy (95 percent). The program will also detect and integrate unusual idiosyncrasies of an author if any are present in the writing sample. In civilian or peacetime applications, Writeprint has also been used to determine the true authorship of some great works of literature and historical documents. In addition to Writeprint, the Dark Web Project team uses their computer software to analyze the structure of social networks, to distinguish the degrees of connections between terrorist web sites and forum postings, and to visualize or map their relationships. The research team also analyzes and codifies the web site or web page content by selected categories (such as enlisting, training, propaganda, etc.). Another aspect of analysis pertains to the technical sophistication of each web site, measuring attributes such as media richness, interactivity, technical capabilities (e.g., with respect to forms, tables, and multimedia files). The point of the web metrics study is to judge and track the “web savvy-ness” of each of the Dark Web site owners and to integrate these findings with other results to arrive at a more complete profile. Since not all sites are equally radical, the Dark Web researchers have designed an analysis tool to measure a site contents’ message sentiments and affect to offer insight into how infective the content is and how much of a radicalizing upshot it might produce. The Dark Web team also focuses on analyzing the videos that are collected. They have found that a large percent of the videos originate from a just a small number of sites. The researchers who have analyzed the IED videos particularly have created a organization of unique signatures for the videos with respect to their sources. According to the Dark Web team, the main purpose of collecting the training videos and the violent IED videos is the hope that the U.S. military is analyzing them further to implement findings for the benefit of our own troops and their training prior to being deployed. Artificial intelligence, as a discipline within the computer sciences, seeks to advance the integration of analyses to mimic diverse aspects of human intelligence, such as language processing, social intelligence, and creativity. The Dark Web Project researchers have not only created the software (spiders) to hack in and collect the content of our enemies’ password-protected web sites and email, they have also implemented a collection of analytical tools to discern the structures, groups, and subgroups of the enemies of the United States from the content they’ve accumulated. Some of these new inventions, such as Writeprint, have enabled the Dark Web team and other users of the Dark Web Project to identify and track unique authors who are influential and/or who are active terrorist leaders. The researchers’

goal is to provide information and insight to the soldiers on the front lines as well as to the agents who have infiltrated the enemies' ranks. In doing so, they have also generated significant academic findings. In addition to creating a unique resource with clever analytical software, Dr. Chen and other Dark Web computer scientists at the University of Arizona's artificial intelligence lab are committed to the ongoing training of researchers who will be prepared to win the War on Terror's battle in cyberspace for years to come.

Army wants to build a massive virtual world to train soldiers

Source: <http://www.rdecom.army.mil/STTC/index.html>

The Army wants to develop a massive virtual world populated by 10,000 avatars that are managed by artificial intelligence and operate over a 32-mile square simulated landscape. Officials at the Army Research, Development and Engineering Command's Simulation and Technology Training Center said they want a systems integrator to put together a virtual




world that includes soldiers, vehicles and weapons that can move around a landscape built from Defense Department digital terrain elevation data. The Simulation and Technology Training Center also said in its request for information that it wants to incorporate technologies used in massively multiplayer online games and offer classified and unclassified versions. The Army is looking for the contractor to create avatars that have the same kind of Web 2.0 communications found in the real world, including chat, instant messaging and links to smart phones. Based on the requirements, the Army is likely to choose a closed world open only to its personnel, and not a public world such as Second Life, which is open to everyone, said Dan Frank, managing partner for Three Wire Systems, a virtual world developer in Vienna, Va., which placed first in this year's Federal Virtual World Challenge. While the Army did not clearly define what kind of operations it planned to conduct in the virtual world, Frank said the proposal indicated it would replicate operations in areas such as Kandahar, Afghanistan, where the service emphasizes peacekeeping missions as well as traditional

military operations. The requirement for the use of massively multiplayer online game technology also indicates the Army might want to replicate Microsoft's Xbox Live experience, where thousands of players worldwide vie against each other inside a virtual world. The service wants avatars to be able to handle thousands of simultaneous connections. The Army is following the lead of the Air Force, which set up MyBase in Second Life in February 2008, said Jacque Davison, president of Davison Associates and a retired Army helicopter pilot who has nearly three decades of experience in the construction of 3-D objects and virtual worlds. Davison Associates is a virtual world company that placed third in the Federal Virtual Worlds Challenge. Gen. William Loomey III, commander of the Air Education and Training Command, said in a white paper that MyBase will cater to cyber savvy young airmen "who have been living in a digital world their entire lives and are better prepared than any other generation to operate in this environment. It is imperative that we understand their needs and expectations, and develop an enterprisewide system that fosters learning and captures their most critical asset -- knowledge." Davison said he believes all the military services eventually will set up cradle-to-grave virtual worlds that will start with recruitment, provide knowledge management during active duty, and then keep retirees connected when they leave a service.

CBRNE-TERRORISM Newsletter

Δελτίο ΧΒΡΠΕ-ΤΡΟΜΟΚΡΑΤΙΑΣ

Volume 3 - 2010



EXPL –News

DEFENCE & SECURITY

SYSTEMS INTERNATIONAL

Vol. 1 2010 £5.95 €8.00 \$8.95



www.defence-and-security.com

WAR GAMES

**How military commanders are changing
the rules of engagement**

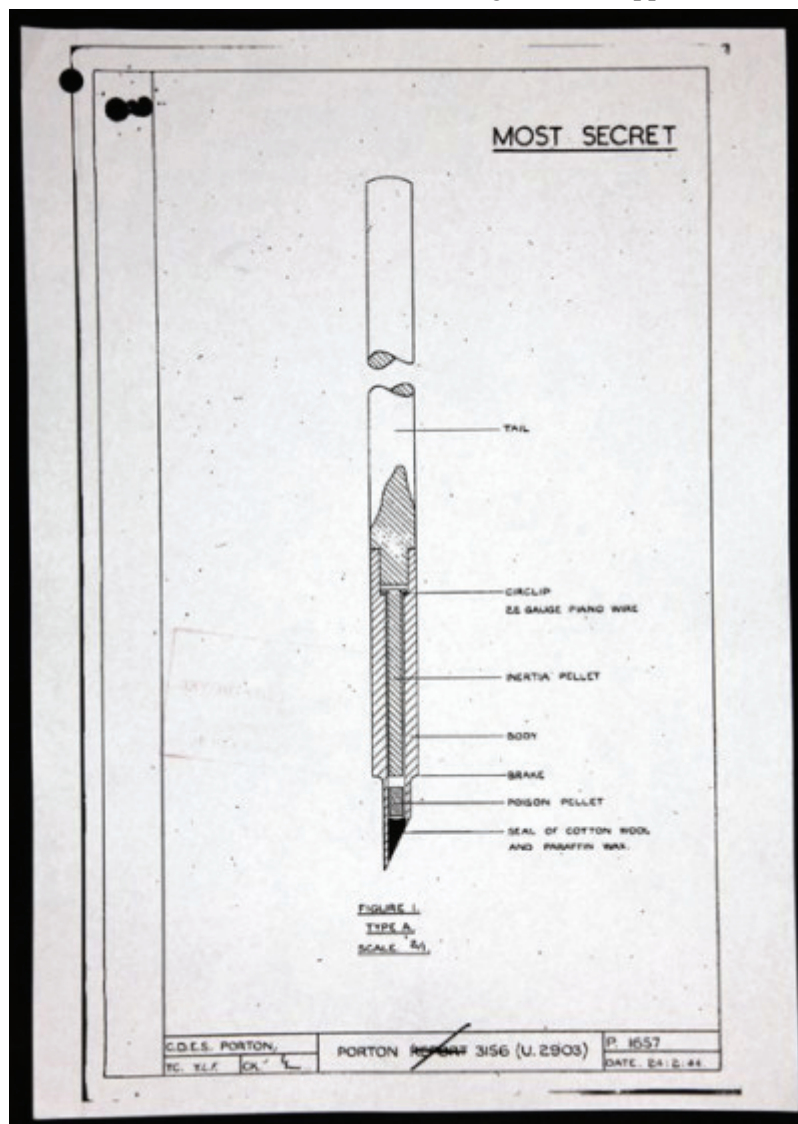


CHINESE AMBITIONS ■ GLOBAL LOGISTICS MANAGEMENT ■ AEROSPACE CHALLENGES

WWII's Secret Sewing Needle Bomb

Source: <http://www.wired.com/dangerroom/category/weapons-and-ammo/chem-bio-nukes/>

During World War II, British scientists developed a new and extremely lethal secret weapon: a bomb which released a cloud of sewing needles, tipped with deadly poison.



is disclosed in the latest release of declassified documents from the UK's National Archive. It was developed at Porton Down, which is now home to Defence Science and Technology Laboratory — but remains notorious for testing chemical and biological weapons on unsuspecting troops during the Cold War. Work on the darts was carried out with the assistance of Canadian and American researchers. Each dart consisted of a hollow steel needle with a paper tail. The tip of the needle was filled with toxin and a dense 'inertia pellet' above it. When the needle struck a target, the pellet kept going and forced the toxin out of the needle. Breaking the skin was enough to inject a lethal dose. The needles were tested on sheep and goats under "realistic"

conditions, sometimes covered with two layers of clothing and protected by trenches. Researchers concluded that if a needle "penetrat[ed] into the flesh, it will cause death if not plucked out within thirty seconds." Even if the needle was removed, it would cause "cause disablement by collapse." Media reports (including the BBC) claim that the chemical agent was mustard gas; this is extremely unlikely as the dose required would be much too high. Realistically, it would be one of the new nerve agents that were first fielded during WWII. The lethal dose for Sarin is 30 micrograms per kilogram of body weight, so three milligrams would kill most people. For Mustard gas, the dose needed would be about two hundred times higher. The effects reported on animal subjects (twitching and convulsions followed by death) also strongly suggest a nerve agent. The program called for the production of thirty million darts. This would require a large number of specially-made needles; the head of the British project contacted the obvious source: the Singer Sewing Machine Company, in a letter apologizing that: "It is a little difficult to explain what I want sewing machine needles for..." The reply from Singer was helpful, if baffled: "From your remarks it would seem the needles are required for some purpose other than sewing machines. In any case, we should like to help

you, if at all possible.” The weapon never went into production, possibly because the darts had very little penetrating power. As soon as its effects were known, scientists said that people would start to take cover under trees or in buildings or vehicles, which would make the rain of darts ineffective. The report also notes that the dart bomb would have been a “highly uneconomical weapon.” That may have sealed its fate. These days, nobody in a western military would dream of using poison darts. But darts filled with a nonlethal “calmative” agent are another matter. British researchers were looking at non-lethal dart guns for crowd control back in 1972 ; it wouldn’t take much imagination to turn that into a non-lethal artillery round. I wonder if they still have the quote from Singer?

U.S. Terror Concentrated In N.Y. City; Bombs Weapon Of Choice

Source: <http://www.medicalnewstoday.com/>

Terrorist attacks in the United States over the past four decades have centered on New York City - the vast majority of them involving bombs or explosives, says a new report from the University of Maryland-based National Consortium for the Study of Terrorism and Responses to Terrorism (START). The research is based on data from the Center's Global Terrorism Database (GTD), the world's most comprehensive, unclassified collection of terror incidents. "Explosives are by far the weapon of choice for terrorists in New York City," says Gary LaFree, who directs START and the GTD. "Of all terror attacks in New York City from 1970 to 2007, 70 percent involved bombs or explosives." La Free adds that "Car bombs have played a small but deadly role in U.S. terrorism." Of the ten terrorist car bomb attacks in the U.S., six have taken place in New York City. The most costly in the city involved the 1993 truck bomb attack on the World Trade Center, which killed six and injured a thousand people.

Among the other trends noted in the report covering the period 1970 to 2007:

- New York City is, by far, the most frequent site of terrorism in the United States;
- It has suffered more attacks than the next four most frequently target cities combined (Miami, 70; San Francisco, 66; Washington, D.C., 59; Los Angeles, 54);
- 284 terror attacks occurred in New York's five boroughs between 1970 and 2007;
- Nearly three-fourths of these attacks took place in the 1970s, followed by less frequent, but often more deadly, incidents including the 1993 and 9/11 World Trade Center attacks;
- Businesses and government facilities are the most frequent targets - not only in New York City, but throughout the United States.
- "While al-Qaeda has launched the deadliest attacks on New York City targets, almost 40 other identified groups engaged in terrorism in this city from 1970 to 2007, representing a range of different ideologies, backgrounds and goals, with changing actors over time," the report says.
- Puerto Rican separatists, the Jewish Defense League and an anti-Castro group were the most active in the 1970s, with their attacks tapering off through the 1980s.

The Optical Dynamic Detection (ODD) Solution Provides A New And Better Way To Detect Explosives

Source: <http://www.medicalnewstoday.com/>

For anyone who has spent a significant amount of time in an urban setting, the scene of a bomb squad responding to a report of a suspicious package might be all too familiar. But just how is it determined that the lunchbox left under the park bench is just leftovers - or a lethal weapon? The most common way is spectroscopy. "Spectroscopy is good, but it only gets you so far," says Eric Houser, a program manager in the Explosives Division of the Department of Homeland Security's Science and Technology Directorate (S&T). The wave of the future may lie in a technology called optimal dynamic detection (ODD), which overcomes many of

spectroscopy's limitations. Spectroscopy uses the color spectrum to shed light on a package's makeup. Since it uses visible light only, spectroscopy can't see through a lunchbox, but what it can see is microscopic residue on the box's outer layer, which can provide telltale clues about what's inside. Using spectroscopy, bomb squad personnel will beam a laser at the package, then compare the reflected "light signature" - an optical fingerprint - against a library of known signatures for chemical compounds, such as nitroglycerin. If there is nitro inside, chances are that some of it will be found in the package's residue. This method presents two problems. First, there's distance. Many threat detection methods require either the person or the detector to be physically near the bomb, making spectroscopy extremely dangerous. Second, approaches like spectroscopy, which rely on reflected light, often are not sensitive or selective enough, especially in the real world where chemical signatures may overlap or be contaminated. Think of light signatures as fingerprints. Capturing a fingerprint from a clean surface is not especially difficult. But in real life, surfaces are anything but clean, and dust, grease, or even ink stains can cause a backpack or lunch pail to bear small deposits of several different chemicals, each with a unique optical fingerprint. To minimize false alarms, a detector must be both sensitive and selective. The ODD project began in the summer of 2008, when researchers from Princeton University and Los Alamos National Laboratory pitched the concept to S&T. As a result, the Directorate signed a contract to fund research at the two labs for a proof of concept. A year and a half later, after several rounds of successful tests, researchers have successfully demonstrated the science of ODD. The goal now: to develop a portable prototype in the next three years that can be field-tested. But the real eye-opener is the science. "At this risk of oversimplifying, this is quantum control applied to explosives detection," warns Houser. Here's how ODD works: A bomb technician beams a "raw" laser pulse toward a suspicious bag, looking for a specific explosive. The pulse passes through an electro-optical filter, gaining clarity as it is bent through lenses, reflected by mirrors and amplified by chips. When the technician tunes the laser to a new frequency, the filter reshapes the laser's pulse. As it is bent, reflected, and electronically processed, the pulse changes amplitude. The shaped pulse hits the chemical environment around the lunchbox and excites the energy state of the material of interest, emitting an energy "signature." Since the pulse was precisely defined, so is the signature. A second laser, called an analyzing "probe," is beamed through the excited molecules, measuring its spectrum. The probe beam passes into an electro-optical detector stationed on the other side of the target. The pulse laser's final shape is stored and analyzed. If the signature looks like that of an explosive, it can conclusively be traced to the explosive molecules that emitted it, which may be found on the bag's fabric or zipper. In this way, ODD reduces background signals, which interfere with the identification process of a potential bomb, and amplifies the return signal, which illuminates the threat. The light energy going in is precisely defined, which makes it easier than spectroscopy to read the energy coming out. "In evaluating a potential bomb, you're looking for a needle in a haystack," explains Houser. "ODD helps bring the needle to the forefront." In a word, ODD offers control. And with greater control comes greater accuracy. The result may well save precious minutes when a minute saved can mean scores of lives also saved.

New Imaging Technology Brings Trace Chemicals Into Focus

Source: <http://www.medicalnewstoday.com/>

Arizona State University scientist N.J. Tao and his colleagues at the Biodesign Institute have hit on a new, versatile method to significantly improve the detection of trace chemicals important in such areas as national security, human health and the environment. Tao's team was able to detect and identify tiny particles of the explosive trinitrotoluene or TNT - each weighing less than a billionth of a gram - on the ridges and canals of a fingerprint. "We can easily detect the TNT traces because we combine the strength of optical microscopy, which gives spatial resolution, with the high sensitivity and selectivity of electrochemical detection," he said. Results of this research appear in the March 12 issue of Science.

Tao's work involves the application of a hybrid technique - called electrochemical imaging microscopy - developed in his lab. "We don't use electrochemistry alone," said Tao, director of Biodesign's Center for Bioelectronics and Biosensors and electrical engineering professor in the Ira A. Fulton Schools of Engineering. "We combine electrochemical sensing with other techniques, including optical detection." The technique has several advantages over more conventional methods of detection, and is a more powerful tool than either optical or electrochemical sensing alone. It is rapid and non-invasive to the chemical system it explores, and provides a detailed map of the surface under study, revealing the chemicals present at every location. Although Tao's published results highlight the power of electrochemical imaging microscopy to uncover explosive residues, he notes that the method can be usefully applied to a full assortment of detection applications. His group is currently using electrochemical imaging microscopy to monitor the activities of living cells, as well as to detect protein biomarkers - early warning beacons that can alert clinicians to pre-symptomatic signs of disease. This could offer improved speed and a lower cost for biomarker discovery when compared with current microarray approaches. Other potential uses include detection of heavy metal ions in drinking water. The technique dispenses with the traditional microelectrode used for chemical sensing. "The key idea here," Tao explains, "is to convert an optical signal into local electrochemical current." This is accomplished thanks to a phenomenon known as surface plasmon resonance. In an electrode - a metal conductor through which electric current is passed - electrons move freely and oscillate in a wavelike fashion called a plasmon. Shining light on the surface plasmon causes the electrons to absorb energy and enter an excited state. Tao notes that the plasmon is exquisitely sensitive to any changes occurring near the electrode's surface. If, for example, an electrochemical reaction involving oxidation or reduction takes place (where electrons are lost or gained, respectively), the plasmon registers this change as a reflection of light (electrochemical current can be inferred from the changes in optical signals detected). The technique allows for the resolution of trace chemicals down to a small fraction of a micron in diameter. The TNT experiments were carried out by first depositing a fingerprint on the surface of an electrode. The raised ridges of the fingerprint formed a delicate layer of protein that blocked the flow of electrochemical current, whereas the grooves allowed current to flow, providing the contrast to reveal the fingerprint in vivid relief when an electrical potential was applied. Next, the applied potential was lowered to correspond to the specific reduction potential of TNT, at which point spots of the explosive particles appeared, providing both visual and chemical confirmation. Remarkably, the technique could successfully detect the grains of TNT, even if they were mixed with other species of particles, including traces of dust, airborne particulate matter or wax. The research was supported through a National Science Foundation Special Creativity award. Co-authors of the study are: Xiaonan Shan, Urmez Patel, Shaopeng Wang, and Rodrigo Iglesias.

Mobile Simulators Give Soldiers Early Roadside Bomb Training

Source: <http://www.nationaldefensemagazine.org/archive/2010/April/Pages/MobileSimulatorsGiveSoldiersTraining.aspx>

High on a simulated hilltop in Afghanistan, a team of four Taliban fighters wait to spring an ambush using a roadside bomb. Their objective is to kill as many U.S. soldiers as possible. As the wind blows, and a sheep herder passes by in the valley below, the sound of two armored humvee engines can be heard winding their way up the mountain pass. In this interactive game, four U.S. soldiers play the part of a typical improvised explosive device emplacement team. There is a leader, a triggerman, a security man who wields a rocket propelled grenade launcher, and a cameraman to record the attack for propaganda purposes. As the humvee comes into view, the triggerman hits a red button and the humvee is destroyed. This all happens in the mobile counter-IED interactive trainer, a four-trailer system of lessons that are designed to give soldiers a first look at the world of roadside bombs. It's one of two new simulators that expose ground forces to the hazards they may face before they arrive in Afghanistan or Iraq. When the soldiers playing the parts of insurgents managed to

destroy the humvee, they earned points on their final score. Unfortunately, there were four soldiers in another part of the trailer who were in mock humvees driving up the mountain pass. They lost points when they failed to spot the warning signs of a roadside bomb. If the second humvee had been following too close and had been caught in the bomb blast, that driver may have had more points knocked off. If they had panicked and shot the goat herder, they would have lost more points. “It teaches them muzzle awareness and trigger control.



Because there are goat herders in this scenario all over the place,” said Lance Pylant, a trainer for the system. The Joint Improvised Explosive Device Defeat Organization and the University of Southern California’s Center for Creative Technologies developed the trainer. There are currently three versions of it at different training facilities with another seven being built. Although funding comes from JIEDDO, it was not an idea pushed from the top down, said Dave Saffold, deputy director of JIEDDO’s joint center of excellence. It was noncommissioned officers from the 1st Army who came up

with the concept. They wanted a training environment that could be quickly adaptive. New lessons can be downloaded via satellite on a secure military network. “If you are going to a certain sector in Afghanistan, we will tailor a package that will represent that training environment,” Saffold said. Having soldiers play the part of the red team gives them insight on how an IED cell works. They can choose their own hiding places and plant the various types of IEDs wherever they want. That includes placing themselves among the goat herders. Since all of the choices are made by the red and blue teams, “there is no scripting in this whatsoever,” Pylant said. The victims will have a shot of revenge, though. The two teams switch sides so all participants can have the same experiences. There are urban and small town scenarios as well. Army Lt. Gen. Michael Oates, JIEDDO director, said having soldiers play the enemy in a competitive environment is a “powerful learning tool.” “If you know anything about soldiers, they will compete over anything,” he told reporters. “Even who can spit the farthest ... They are thinking about where they hide the explosives. ‘How do I gain the most advantage? How do I attack the friendly forces?’” Prior to this final exercise, soldiers go through three other trailers that give them an overview of the IED problem. For example, what they look like, spots where they might be hidden and the different triggering devices. There is also a section on counter remote-controlled IED electronic warfare devices that are used to jam radio signals that set off the bombs. Videos of actual IED attacks taken from the inside of vehicles bring home the reality and seriousness of the problem. One trailer is a reproduction of an IED workshop where insurgents put the devices together. It comes complete with real tools employed to make the bombs, and has the smell of common chemicals used to make the explosives. At the end of each trailer, there is a quiz. Those results, along with the final simulation, are put together for a final score. Trainers or senior officers can see where a soldier may be lacking in knowledge and go over what they are missing, Pylant said. Another four-trailer system helps route clearance specialists train on their complicated trucks before they reach war zones. The virtual route clearance trainer, developed by Raydon Corp. of Daytona Beach, Fla., simulates missions in Afghanistan or Iraq. Currently, the three trucks used in these special missions are in high demand and are shipped overseas as soon as they come off assembly lines, said Cory McAndrew, simulations systems specialist at Raydon. The Army wanted something to train soldiers on the vehicles that they will be using before deploying. Up to eight operators at a time can train on the Buffalo mine protected clearance vehicle, which has a manipulator that is used to probe for suspected roadside bombs. There are also simulators for two Husky vehicle mounted mine detection systems, four RG-31 medium mine protected vehicles, which provide security for

the teams, one joint EOD rapid response vehicle and a Talon robot. While soldiers watch a simulation in a virtual world on a screen, they are sitting in replicas of the vehicles' cabs. The dashboards, seats, steering wheel and all the other controllers are the real thing, McAndrew said. The RG-31 gunner sits in a turret that rotates 360 degrees. "These are all from the actual vehicles, so they are getting their hands on the actual equipment they would be training on in real life," he said. One of the four trailers is devoted to classroom lessons and after-action reviews. Trainees first practice their skills separately, but at the end of the 40-hour course, they come together and go through different scenarios as a team. Up to 16 participate in the final simulation, which starts with a mission briefing. The drivers, operators and explosive ordnance disposal teams then work together to clear roads. The various scenarios can include bombs exploding, and medical evacuations. Scenes are based on real roads in Iraqi cities such as Tikrit. For Afghanistan, the data is based on Kandahar. Raydon is working on adding artificial intelligence to the simulations "so if you beep a horn, a car will most likely get out of your way," McAndrew added. The Army is asking for more realism, so the company is looking into adding force feedback to make the steering wheel respond the way it would if it were hitting rough patches on the road, and vibration under the seats to give drivers and passengers the same sensation. "The military would like motion platforms but that is very expensive to do," he said. Adding these features is meeting the goal halfway, he said.

Letter bomb

Source: http://en.wikipedia.org/wiki/Letter_bomb



A letter bomb, also called parcel bomb, mail bomb or post bomb, is an explosive device sent via the postal service, and designed with the intention to injure or kill the recipient when opened. They have been used in terrorist attacks such as those of the Unabomber. Some countries have agencies whose duties include the interdiction of letter bombs and the investigation of letter bombings. The letter bomb may have been in use for nearly as long as the common postal service

has been in existence, as far back as 1764 (see Examples).

Description

Letter bombs are usually designed to explode immediately on opening, with the intention of seriously injuring or killing the recipient (who may or may not be the person to whom the bomb was addressed). A related threat is mail containing unidentified powders or chemicals, as in the 2001 anthrax attacks.

Examples

One of the world's first mailbombs is mentioned in the 18th century diary of Danish official and historian Bolle Willum Luxdorph. His diary mainly consists of concise references to news from Denmark and abroad. In the entry for January 19, 1764 he writes the following: Colonel Poulsen residing at Børglum abbey was sent by mail a box. When he opens it, therein is to be found gunpowder and a firelock which sets fire unto it, so he became very injured. The entry for February 15 same year says: Colonel Poulsen receives a letter in German, [saying] that soon the dose will be increased. It is referring to the dose of gunpowder in the box. The perpetrator was never found. In a later reference Luxdorph has found a mention of a similar bomb being used, also in 1764, but in Savona in Italy.

POLICE.

At Marylebone, EDWARD RICHARD WHITE, aged 61, an artist, living at 10, Percy-road, Shepherd's-bush, was charged on remand before Mr. de Rutzen with causing to be received by Mr. John Theodore Tussaud at the exhibition in the Marylebone-road a certain explosive, with intent to do him grievous bodily harm. Mr. Grain, barrister, appeared to prosecute; and Mr. Bowker, solicitor, defended. Mr. Grain now said that some time ago Messrs. Tussaids were in financial difficulties and the waxwork exhibition was sold to Mr. Poyser, who formed a company. Notice was given to the men engaged in the exhibition that their engagements would cease on the 7th of February last, and that the matter of the re-engagement of some of them would then be considered. The prisoner had been engaged to execute the work of inserting the hair in the faces of the wax figures and had been paid at the rate of from £6 to £8 a week. Having referred to the delivery of the box at the exhibition, Mr. Grain produced the box, a small cigar-box, and showed that besides about half a pound of gunpowder found in it there was also some rough glass-paper attached to the lid, which, if the box had been opened quickly, would have caused two fuses to rub against the glass paper, when an explosion would have followed. Counsel then called Mr. Edwin Josiah Poyser in support of his statement. Witness said that as soon as he suspected that the box, from which some dark grains had fallen, contained an explosive he sent for the police, and it was found that the box contained a quantity of gunpowder. The parcel was fastened with a piece of gold lace cord such as was used for dressing the wax figures in the exhibition. Frederick Baker, a lad employed by the London Parcel Delivery Company at Rolls-buildings, Better-lane, said that on the 22d last, a man called and said that he wanted a parcel sent. He had already recognized the prisoner as the man who sent the parcel. A further remand at this point was asked for, which Mr. de Rutzen granted. The magistrate consented to admit the prisoner to bail in two sureties of £100 each.

- Edward White, formerly an artist at Madame Tugelignitessauds, was alleged to have sent a parcel bomb to John Theodore Tussaud in June 1889 after being dismissed.
- A Swedish man named Martin Ekenberg used a mailbomb August 20, 1904, targeting CEO Karl Fredrik Lundin in Stockholm. It was made of a box loaded with bullets and explosives.
- In 1915, Vice President of the United States Thomas R. Marshall was the target of an assassination attempt by letter bomb.
- Austrian Nazi war criminal Alois Brunner was sent a letter bomb by the Israeli intelligence services Mossad, to which he lost an eye and several fingers.
- Ruth First, a South African communist anti-apartheid activist was killed by a parcel bomb mailed by the South African government to her home in Mozambique.
- In the 1960s, 1970s and early 1980s, several terrorist organizations organizations in Argentina such as Montoneros and ERP included letter bombs into their weaponry.
- Theodore Kaczynski, the "Unabomber", killed three and injured 23 in a series of mailbombings in the United States from the late 1970s to the early 1990s.
- In August 1985, a woman in Rotorua, New Zealand, Michele Sticovich, was instantly killed and a close friend of hers seriously injured after she opened a parcel addressed to her containing a number of sticks of gelignite. Mrs Sticovich's estranged husband, David Sticovich, was arrested and ultimately pleaded guilty to her murder.
- Robert Smith Vance, a U. S. federal judge, was killed instantly upon opening a letter bomb in the kitchen of his home in Birmingham, Alabama, with his wife, Helen, seriously injured. Walter Leroy Moody was later convicted of killing both Vance and Georgia attorney Robbie Robertson by use of letter bombs delivered through the mail.
- Franz Fuchs, Austrian mailbomber, killed four and injured 15 with mailbombs and improvised explosive devices in the mid-1990s.
- Singer Björk was sent a letter bomb charged with explosives and hydrochloric acid by fan Ricardo López in 1996. The bomb did not reach Björk, having been randomly intercepted by London Police.
- In February 2007, a series of mailbombings in the United Kingdom injured nine people, though none of them were critically hurt.

- In January and February 2007, a bomber calling himself "The Bishop" sent several unassembled bombs to financial firms in the United States, and was arrested in April 2007
- In August 2007, a Lebanese immigrant was charged in connection with a letter bombing in the Toronto-Guelph, ON area; he was responsible for injuring 1 person. He was also responsible for the precautionary closing of a portion of the Don Valley Parkway in Toronto on August 31, 2007
- On October 19, 1986, [Dele Giwa], a [Nigeria]n journalist and editor of the [Newswatch] magazine was killed with a mail bomb, claimed to be sent by Nigeria's former dictator, Gen. [Ibrahim Babangida]. The general has never admitted complicity, remaining mute on the issue.

Patentability

Letter-bombs, along with anti-personnel mines, are typical examples of subject-matter excluded from patentability under the European Patent Convention, because the publication or exploitation of such inventions is contrary to the "ordre public" and/or morality (Article 53(a) EPC).

Scanmail 10K Electronic Mailscanner

Scanmail 10k is a compact desk-top electronic mail-scanner for letters and small packages.



it will automatically find highly explosive letter-bombs and other suspect items of mail such as razor blade letters and cutting devices whilst reliably ignoring office clutter such as paperclips and staples. over 10,000 units used in government, police, high security locations and corporate mailrooms. Scanmail 10k is used throughout the world in high security locations as well as in private residences and royal palaces. scanmail was also the machine that saved the life of one of the unabomber's intended victims by successfully intercepting one

of his postal devices. Unlike some other metal detector imitations. it is the only unit that will scan mail is not simply a metal detector, it is an intelligent device with advanced discrimination that allows you to reliably find a small battery while discriminating against paperclips and staples. no other unit can reliably do this and should be deemed unsafe. It can be used alone or with an x-ray machine as the first line of defence against postal bombs. no special training and no expensive maintenance or radiation checks required.

Features

- compact and portable
- screens parcels up to 6cm (2½") thick (telephone directory size)
- fast and reliable
- automatic detection of suspect items
- visual and audio alarm
- no calibration, simply plug in and use
- will not damage magnetic media or camera film
- no false alarms on paperclips and staples etc
- low maintenance requirements

Detects

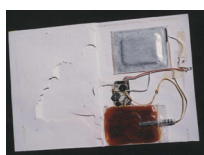
- bomb making components such as batteries, detonators, timers, circuitry regardless of what type of explosive is used
- cutting devices such as razor blade letters or mouse trap devices

Bypasses

- ordinary office clutter such as paperclips, staples and treasury tags

Additional features

- back up battery for use where power supply is absent. recharge by simply plugging into the mains
- back up circuitry in case of malfunction
- all parts modular and easy to replace
- no calibration. simply plug in and use



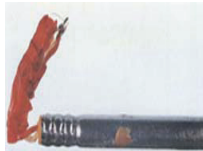
Scanmail automatically detects highly explosive mail devices such as musical greetings card devices



Scanmail will find razor blade letters, a common form of hate mail



Scanmail will reliably detect batteries (the power source of a mailbomb)



Scanmail will detect all known detonating mechanisms



Scanmail will reliably ignore office clutter such as paperclips and staples

Taliban Reportedly Adding HIV-Infected Needles to Explosive Devices

Source: http://www.thesun.co.uk/sol/homepage/news/campaigns/our_boys/3005443/Taliban-using-HIV-bombs.html

Taliban fighters are burying dirty needles with their bombs in a bid to infect British troops with HIV, *The Sun* reported Wednesday.



Hypodermic syringes are reportedly hidden below the surface of explosive devices, pointing upwards to prick bomb squad experts as they hunt for devices. The needles are feared to be contaminated with hepatitis and HIV. And if the bomb goes off, the needles



become deadly flying shrapnel. The tactic, used in the Afghan badlands of Helmand, was exposed by British ex-Army officer Patrick Mercer. "Are there no depths to which these people will stoop? This is the definition of a dirty war," Mercer said. Razor blades are also being used. All Royal Engineer and Royal Logistic Corps bomb search teams have been issued with protective Kevlar gloves.

CBRNE-TERRORISM Newsletter

Δελτίο ΧΒΡΠΕ-ΤΡΟΜΟΚΡΑΤΙΑΣ

Volume 3 - 2010

A photograph of a white military truck, possibly an ambulance or transport vehicle, that has been severely damaged by a large fire. The fire is intense and bright orange, consuming the lower half of the truck. The background is a hazy, outdoor setting.

TERR –News

UGV-platforms...
*highly mobile, reliable,
in service world wide*



www.telerob.de

24 Ιουνίου 2010

ΕΠΕΣΕ ΣΤΟ ΚΑΘΗΚΟΝ ΥΠΕΡ ΠΑΤΡΙΔΟΣ
Αστυνομικός Υποδιευθυντής Γιώργος Βασιλάκης, 52 ετών
Υπασπιστής Υπουργού Προστασίας του Πολίτη



Βομβιστική τρομοκρατική ενέργεια εντός του γραφείου του,
στο Υπουργείο Προστασίας του Πολίτη.

Καλό Ταξίδι Συνάδελφε !

Από τον Αρχιμανδρίτη
Νικόλαο Κ. Λαγουμτζή
Συνταγματάρχη (Θ) ε.α.
Πηγή: press-gr.blogspot.com

«Ένας συνάνθρωπος, ένας συνάδελφος θυσιά στο βωμό της τρομοκρατίας! Μια οικογένεια, πολλοί άνθρωποι, χαμένοι στον πόνο και στην θλίψη! Ο Γ. Βασιλάκης, πήγε για την εργασία του, για το μεροκάματο του και συνάντησε την άσχημη και απαίσια μορφή της τρομοκρατίας κάποιων άλλων που κτυπούν αλύπητα τον οποιοδήποτε τύχει στο αιματοβαμμένο διάβα τους! Ο Γ. Βασιλάκης, δεν θα ξαναδεί τα παιδιά του, την γυναίκα του, τους συγγενείς και φίλους του! Ούτε και αυτοί θα τον ξαναδούν! Θα συνεχιστεί η ζωή με τις... όσες δυσκολίες και αυτοί που τόσο αδίστακτα μοίρασαν θάνατο, θα σκεφθούν ότι κάτι πέτυχαν, κάτι έκαναν. Αφαίρεσαν μια ζωή! Βούτηξαν πολλές άλλες ζωές στην θλίψη, στον πόνο, στην αγωνία, στην αγανάκτηση, στον θυμό, στο γιατί, στο μεγάλο ΓΙΑΤΙ;;; Για την Δημοκρατία; Οχι βέβαια, αλλά για τον εγωισμό τους και την εγωιστική απόφαση τους, ότι παίρνουν την ζωή του οποιοδήποτε, οποτεδήποτε το αποφασίσουν. Η θλίψη και ο πόνος μας μεγάλος, και η αγάπη μας στην οικογένεια του ακόμη μεγαλύτερη! Μακάρι να είναι ο τελευταίος! Μακάρι να μην υπάρξει ΠΟΤΕ άλλος! Μακάρι....»

NEW BOOK – Would be Warriors

By: Brian Michael Jenkins (2010)

Source: www.rand.org/pubs/occasional_papers/2010/RAND_OP292.pdf

Between September 11, 2001, and the end of 2009, 46 publicly reported cases of domestic radicalization and recruitment to jihadist terrorism occurred in the United States; 13 of those



cases occurred in 2009. Most of the would-be jihadists were individuals who recruited themselves into the terrorist role. Some provided assistance to foreign terrorist organizations; some went abroad to join various jihad fronts; some plotted terrorist attacks in the United States, usually with little success because of intervention by the authorities. The threat of large-scale terrorist violence has pushed law enforcement toward prevention rather than criminal apprehension after an event — or, as one senior police official put it, “staying to the left of the boom,” which means stopping the explosions or attacks before they occur. This shift toward prevention requires both collecting domestic intelligence — always a delicate mission in a democracy — and

maintaining community trust and cooperation.

Contents

Preface	iii
Summary	vii
Acknowledgments	xi
Would-Be Warriors: Incidents of Jihadist Terrorist Radicalization	
in the United States Since September 11, 2001	1
An Average of Six Cases a Year	1
Who Are These Homegrown Terrorists?	3
What Did They Intend to Do?	6
No Terrorist-Prone Personality	7
The 1970s Saw Greater Terrorist Violence	8
Are We Doing This Right?	9
Recruitment Will Continue	12
A Chronology of the Cases	13
Bibliography	19

Europe's antiterrorism agencies favor human intelligence over technology

Source: <http://www.washingtonpost.com/>

The tip from Spain was only a vague warning. But it was enough for France's domestic intelligence agents to go to work, tapping phones, tailing suspects and squeezing informants.

Before long, they rolled up a group of Muslim men in a provincial French town who, beneath a tranquil surface, were drawing up al-Qaeda-inspired plans to set off a bomb in the Paris subway. The plot, described by a source with firsthand information, was one of 15 planned terrorist attacks by jihadist cells in France that have been thwarted in recent years, according to a count by the Central Directorate of Internal Intelligence (DCRI), France's main antiterrorism force. One was a bomb plot directed against the directorate's own headquarters. The antiterrorism policing -- it is not a "war," specialists here emphasized -- has been conducted for the most part in the dark, and in a style that sets France and other European countries apart from the United States. As U.S. officials seek to understand what may have led a Pakistani immigrant to try to blow up Times Square, and how he boarded an airplane at John F. Kennedy International Airport despite multiple computerized watch lists, Europe's specialists have pointed to their own approach as an example of how to proceed. "You have got to be proactive," said Jean-Louis Bruguière, who as an investigating magistrate handled many of France's major antiterrorism cases and now is a liaison to the U.S. Treasury Department on terrorist financing. "It is not a question of defense." From the beginning, Bruguière and other specialists said, the emphasis in Europe has been on domestic human intelligence rather than the computerized systems such as watch lists favored by U.S. security agencies. That has meant tedious hours of surveillance, patient listening-in on telephone conversations, careful review of bank records, and relentless recruitment of informants among Islamic zealots who are motivated to betray acquaintances by everything from fear of losing visas to a desire to clear the name of Islam in European minds. A DCRI field agent, interviewed recently on France 2 television under restricted conditions with his face blurred out, said all 15 of the terrorist plots stopped recently in France were uncovered because of information received from human sources, recruited among a Muslim population estimated at more than 5 million. "In the shadows, we put into place -- for months, sometimes years -- detection systems, surveillance arrangements that allow us to act at the right moment," Bernard Squarcini, until recently the DCRI director, said in an interview with *Le Point* magazine. "Our obsession is to anticipate, that is, to neutralize terrorists before they strike." Police in some U.S. cities, most notably New York and Los Angeles, have extensive and sophisticated programs to engage with communities and infiltrate potentially dangerous groups. But Lee H. Hamilton, who co-chaired the 9/11 Commission, said U.S. human intelligence efforts must be "greatly expanded and refined" to tackle the increasing threat of homegrown terrorism. "You have to have people who go into a specific community, an ethnic group, religious group, a sectarian group, get acquainted with their people, their leaders, and get to know their community," Hamilton said in an interview. "Those communities know, usually, the people within the community that are disaffected, mad, angry, maybe even threatening." In France, to pressure for more information and keep would-be terrorists off balance, the specialists said, police and domestic intelligence officers carry out frequent raids, taking young Muslim men into custody for interrogation and intimidation. That treatment extends to Islamic groups that may never imagine carrying out a terrorist attack but eventually could help with logistics, even unwittingly, or just hear about someone with violent plans. "They are constantly bothered," said Xavier Raufer, a veteran terrorism expert who heads the Criminology Institute at the University of Paris II. "The most fragile of them are singled out, contacted and eventually flipped." About three dozen people have been sentenced to prison over the last three years in connection with antiterrorism raids, many of them under a broad-gauge law that defines as a crime "criminal association with intent to commit terrorism," according to a recent Interior Ministry report. Peter Neumann, director of the London-based International Center for the Study of Radicalization and Political Violence, said British officials also seek to penetrate seedbeds for Islamic violence before it happens and, in doing so, are willing to work with what he called "slightly dubious characters." "In Britain, if a group came forward and said that, we are against al-Qaeda but we are kind of thinking that Hamas suicide bombings in Israel are okay, this would not stop funding by the British government," he said. "In America, that ambiguity would not be tolerated." François Heisbourg, a defense specialist who played a key role in drafting the white paper outlining France's antiterrorism policies, noted that French and other European police also have more

latitude in dealing with terrorism suspects than their American counterparts. The DCRI, for instance, has been exempted from oversight by France's National Committee on Computer Science and Liberties, allowing it to monitor computer messages and Islamic Web sites without outside restriction. French police can demand a show of identity for no specific reason, Heisbourg recalled, and can hold suspects for questioning over two days -- or more in terrorism cases -- without intervention by defense lawyers. Police and prosecutors in other European countries have similar latitude. "Even though we're similarly democratic, we have very different views of the practical application of those values," said Kenneth Wainstein, homeland security and counterterrorism adviser to President George W. Bush and a former assistant attorney general for national security. "I recall being surprised when our European counterparts discussed cracking down on jihadist rhetoric on the Internet. That would never fly here. For us, much of that rhetoric would be protected by the First Amendment." France and Britain both got early starts on dealing with terrorism -- France because of Palestinian nationalists and Algerian extremists who attacked in Paris, and Britain because of the Irish Republican Army. But French authorities got a particularly informative insight in 1994 from documents uncovered after an attempted terrorist attack by the Armed Islamic Group, an Algerian fundamentalist cell involved in a guerrilla war to overthrow the government in Algiers. Although the Armed Islamic Group grew out of Algeria's particular situation, Bruguière said, the documents suggested even then that something broader was happening -- the beginnings of anti-Western Islamist jihadism of the type championed by Osama bin Laden. "As a result, we saw the Islamic terrorist threat coming a lot sooner than the Americans," Bruguière said in an interview. "They were documents about the Armed Islamic Group, but they showed that the project was to be much bigger, that it was to be something like what happened on 9/11."

Maritime Security: Varied Actions Taken to Enhance Cruise Ship Security, but Some Concerns Remain

Source: www.gao.gov

Summary

Over 9 million passengers departed from U.S. ports on cruise ships in 2008, and according to

GAO
United States Government Accountability Office
 Report to the Chairman, Committee on
 Homeland Security, House of
 Representatives

April 2010

MARITIME SECURITY

Varied Actions Taken to Enhance Cruise Ship Security, but Some Concerns Remain

agency officials, cruise ships are attractive terrorist targets. GAO was asked to review cruise ship security, and this report addresses the extent to which (1) the Coast Guard, the lead federal agency on maritime security, assessed risk in accordance with the Department of Homeland Security's (DHS) guidance and identified risks; and (2) federal agencies, cruise ship and facility operators, and law enforcement entities have taken actions to protect cruise ships and their facilities. GAO reviewed relevant requirements and agency documents on maritime security, analyzed 2006 through 2008 security operations data, interviewed federal and industry officials, and made observations at seven ports. GAO selected these locations based on factors such as the number of sailings from each port. Results of the visits provided additional information on security, but were not projectable to all ports.

The Coast Guard has assessed the risks to

cruise ships in accordance with DHS guidance--which requires that the agency analyze



GAO-10-400

threats, vulnerabilities, and consequences--and, with other maritime stakeholders, identified some concerns. Specifically, agency officials reported in January 2010 that there had been no credible threats against cruise ships in the prior 12 months, but also noted the presence of terrorist groups that have the capability to attack a cruise ship. The Coast Guard, cruise ship and facility operators, and law enforcement officials generally believe waterside attacks are a concern for cruise ships. Agency officials and terrorism researchers also identified terrorists boarding a cruise ship as a concern. The Coast Guard has also identified the potential consequences of an attack, which would include potential loss of life and economic effects. Federal agencies, cruise ship and facility operators, and law enforcement entities have taken various actions to enhance the security of cruise ships and their facilities and implement related laws, regulations, and guidance, and additional actions are under way. DHS and component agencies have taken security measures such as the Coast Guard providing escorts of cruise ships during transit, and CBP's review of passenger and crew data to help target passenger inspections. Cruise ship and cruise ship facility operators' security actions have included developing and implementing security plans, among other things. The Coast Guard is also in the process of expanding a program to deter and prevent small vessel attacks, and is developing additional security measures for cruise ships. In addition, CBP's 2005-2010 Strategic Plan states that CBP should seek to improve identification and targeting of potential terrorists through automated advanced information. CBP, however, has not assessed the cost and benefit of requiring cruise lines to provide passenger reservation data, which in the aviation mode, CBP reports to be useful for the targeting of passengers for inspection. GAO's previous work identified evaluations as a way for agencies to explore the benefits of a program. If CBP conducted a study to determine whether collecting additional passenger data is cost effective and addressed privacy implications, CBP would be in a better position to determine whether additional actions should be taken to augment security.

Radical Islam and the Balkan Muslim Diaspora in the United States

Source: <http://www.homelandsecurity.org/journal/>

Steven Oluic

U.S. Military Academy

Introduction

There is an acute lack of accurate information on the Balkan Muslim communities in the United States. In fact, data on the entire Muslim minority in the United States vary widely from source to source. Total U.S. Muslim population estimates range from 4 million to 8 million, with 7 million (as of 2003) being the most widely reported figure. This number includes all Islamic sects found in the United States. According to Geneive Abdo, as of 2003 there were approximately 1,300 mosques and 300 to 400 Islamic schools nationwide. Balkan Muslims are overwhelmingly members of the Sunni sect of Islam and practice their beliefs in a very relaxed and even secular manner. Significant challenges arise in the fact that the 2000 census offers the most recent national data available, and it does not clearly reflect the new Balkan states and identities that have emerged since the 1990s. Before the census, many individuals from the region may have simply identified themselves as "Yugoslav" as opposed to Albanian, Bośniak, Macedonian, or any of the other nationalities that were part of Yugoslavia. The Balkan Muslim communities were widespread across Yugoslavia and remain, with the exception of Bosnia, similarly located in the successor states (see figure 1).



Figure 1. Regions of the former Yugoslavia and Albania with a significant Muslim presence displayed in green (Oluic, 2009).

The self-identification of “Yugoslav” in the census poses some challenges in differentiating the older established communities from the recent immigrant communities. Figure 2 displays the spatial footprint, by state, of census participants declaring themselves of Yugoslav ancestry.

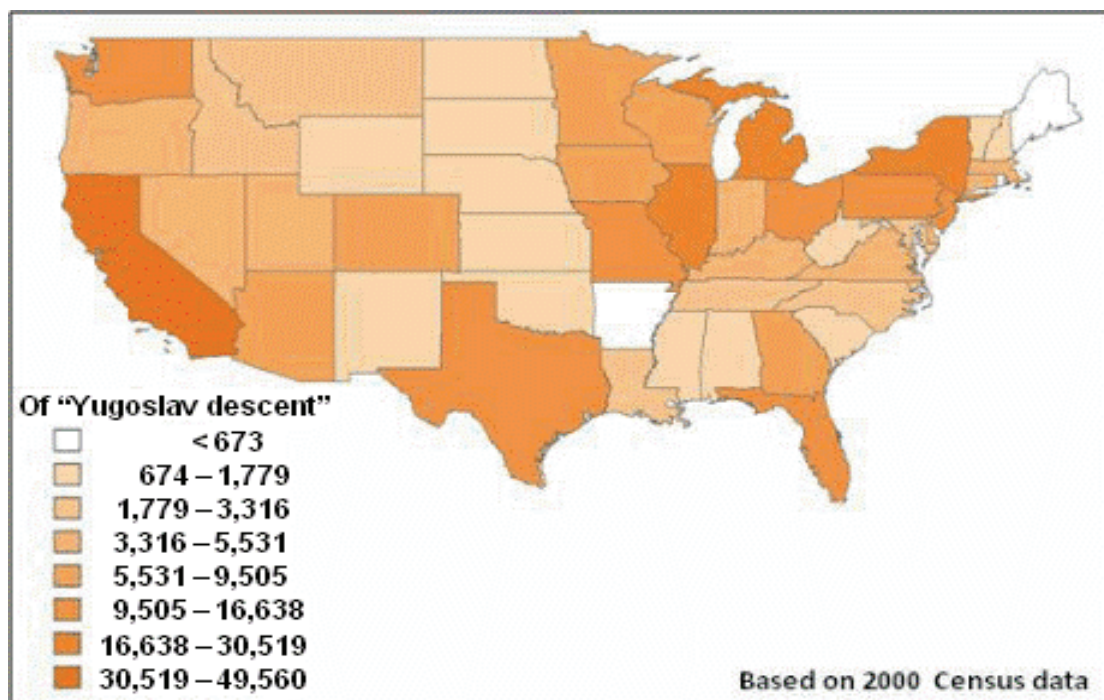


Figure 2. Spatial distribution of people declaring Yugoslav ancestry (U.S. Census 2000).

Balkan immigration to the United States is not a recent phenomenon. For over a century, Southeastern European immigrants have settled across the country; however, since the Balkan Wars, the World Wars, the 1990s Yugoslav Wars of Succession, and the opening of Albania to the outside world, a new wave of migrants has sought refuge in the United States and several European countries en masse. Whereas in the entire decade from 1980 to 1989, there were only 16,267 Yugoslav immigrants to the United States, in the 1990s the number trebled to 57,039. Figure 3 displays the number of immigrants from all the countries of former Yugoslavia since 2000, surpassing 125,000 total.

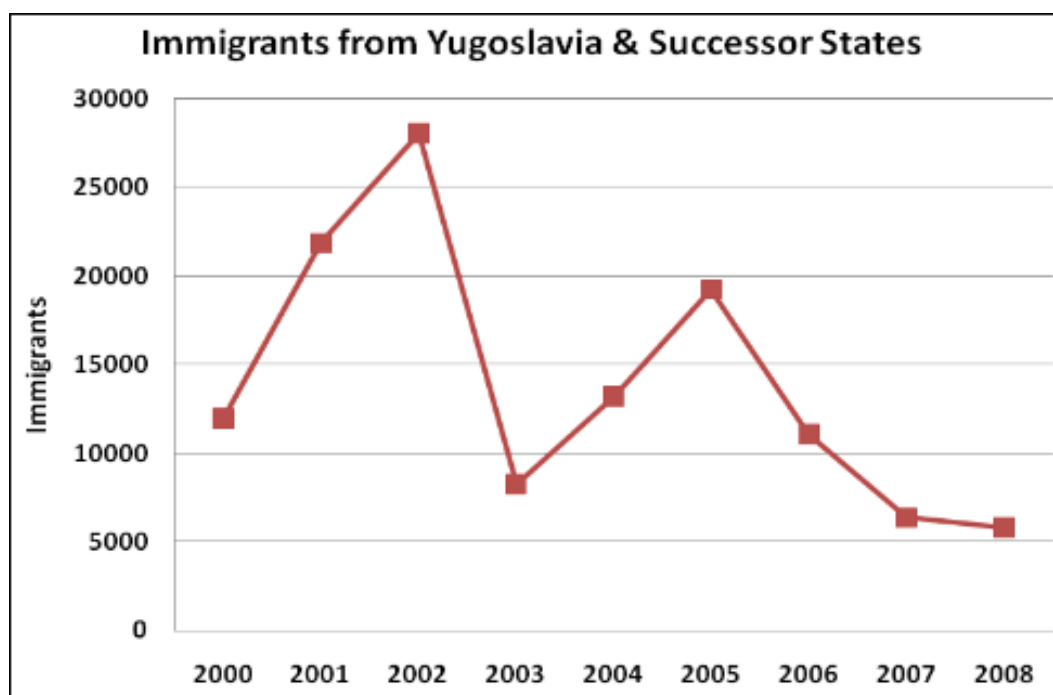


Figure 3. Immigrants from former Yugoslavia.

While this information does not reveal the specific national groups the Yugoslav immigrants stem from, it does provide a useful overview. According to the Homeland Security Department's Office of Immigration Statistics, from 2000 through 2008, over 98,000 Bosnian and 8,681 Macedonian immigrants received legal permanent resident status in the United States. According to the same source, over 45,400 Albanian immigrants also received legal permanent resident status in the United States. The term diaspora has historically been used to denote the Greek colonization of Asia Minor in 800–600 BC or the Jewish experience of displacement to Babylon in 586 BC. The meaning has changed drastically over the past 30 years, however, and for the purposes of this article “a diaspora is characterized by networks, organizations and institutions linking up people and communities settled in different countries.” Paul Hockenos noted that a diaspora comprises “those members of a common ethnic national group living outside the borders of their native home territory.” Lastly, and in the context of this article, diaspora is the self-identification and active membership in a group—the so-called hyphenated Americans. In some instances, many U.S. immigrants are so completely assimilated that they do not patronize diaspora community centers, attend diaspora places of worship, or use diaspora newspapers, journals, or radio stations, turning their backs on their ancestral ties and homelands. Modern technology via the Internet and low-cost overseas calling have impacted the trend toward full assimilation by overcoming geographical distances, enabling people to easily remain in close contact with the homeland. This destruction of distance by technology also permits nefarious activities to be conducted in the United States.

Defining the Threat

Historically, terrorism is not a unique phenomenon of the Islamic world. Modern terrorism is typically considered to have begun in the 18th century with the brutalities of the French Revolution, according to Audrey Kurth Cronin. She outlined four types of terrorist organizations operating in the world today, categorized “by their source of motivation: left-wing terrorists, right-wing terrorists, ethnonationalist / separatist terrorists, and religious or ‘sacred’ terrorists.” Terrorists from the Balkan Muslim communities have been influenced by the last two. Ethno-nationalist or separatist terrorist organizations such as the Kosovo Liberation Army are found primarily in Europe, although the Albanian diaspora provided materiel and financial support in the 1990s. The notion of religious or sacred terrorists appears to be the greatest influence on U.S. Muslim diasporas and is considered to be the greatest international security threat. While most terrorist organizations and movements have political goals and objectives, the religious terrorist operates under a different ideology and organizational framework. There are at least five reasons, according to Cronin, why these terrorists are especially dangerous: (1) “religious terrorists often feel engaged in a Manichaeian struggle of good against evil, implying” that anyone “not a member of their religion” may be “evil” and thus a legitimate target; (2) they “engage in violent behavior directly or indirectly to please the perceived commands of a deity”; (3) they “consider themselves to be unconstrained by secular values or laws”; (4) they “often display a complete sense of alienation from the existing social system”; and (5) religious terrorism has “dispersed popular support in civil society.” Religious terrorists are a growing threat and are becoming a much more geographically dispersed danger operating with little direct guidance, only the ideologies of terrorist organizations such as al-Qaeda. This diffuse threat is further emboldened by the ability to communicate and operate in an increasingly borderless, globalized world. An “important factor that must be understood is that this threat comes from radical Sunni Islam and not from Shia Islam,” according to Lee Jay Walker. In America, as well as the United Kingdom, one finds “many Shia Muslims; however, it is clear that all major global Islamic terrorism derives from radical Sunni Islam.... Islamic terrorist attacks in America, India, Indonesia, Kenya, the United Kingdom, and other nations, have all been” committed “by radical Sunni Islamists.... the inspiration behind these terrorist attacks is coming from the same avenue” and “can be traced back to” movements originating in “Saudi Arabia and Pakistan.”

The Bošniak Diaspora Community

The U.S. Balkan Muslim community has no hierarchical religious institution that can provide diaspora data as can typically be found in various U.S. Balkan Christian churches (such as the Serbian Orthodox Patriarchate or the Croatian Roman Catholic diocese). An accurate database is nonexistent and must be compiled from various sources, such as anecdotal evidence and government or academic data. According to the New York Times, from 1992 to March 2007 the State Department resettled over 131,000 Bosnian refugees in the United States, over 9,000 in the Chicago area alone. In 1998 the United States resettled approximately 30,900 refugees from Bosnia. This information, as is so often the case, doesn't differentiate among Christian, Muslim, Croat, Serb, and so on. How are Bosnians defined? Are Bošniaks, Croats, and Serbs included in the “Bosnian identity”? A major assumption used in this research on the Bošniak community is that the vast majority of Bosnian refugees are Muslim, as they suffered the greatest displacement from ethnic cleansing operations during the war and sought asylum in other countries. The Bošniak community is fairly decentralized across America, with strong local community ties back to Bosnia and Herzegovina and no national umbrella religious organization representing them yet. The Islamic Association of Bošniaks in North America was established in May 2003 in a first attempt to create an umbrella organization for Bošniak congregations in North America. Moreover, several nongovernmental and diaspora organizations, such as the Congress of North American Bošniaks, presumably represent Bošniak community political and social concerns. These organizations have been helpful in attempting to map Bošniak spatial patterns in the United States. According to Murat Muratovic, President of the Bosnian Media Group, publisher of

the Bosnjacka Dijaspora newspaper, and manager and announcer of Radio Behar, all based in St. Louis, there is a move to establish a U.S.-based Bošniak mesihat organized under the religious jurisdiction of Reis Mustafa Cerić in Sarajevo. However, there appears to be a rivalry for supremacy of this mesihat between the Chicago and St. Louis Bošniak communities. In any case, Imam Senad Agić has been picked to be the leader of this new Bošniak Islamic community. This is not unique, as the Bosnian Izlamska zajednice, or Muslim community, based in Sarajevo has mesihats in Germany, Austria, and elsewhere organized under its leadership (see figure 4). The Izlamska zajednice is considered the best-organized Muslim community in Europe.

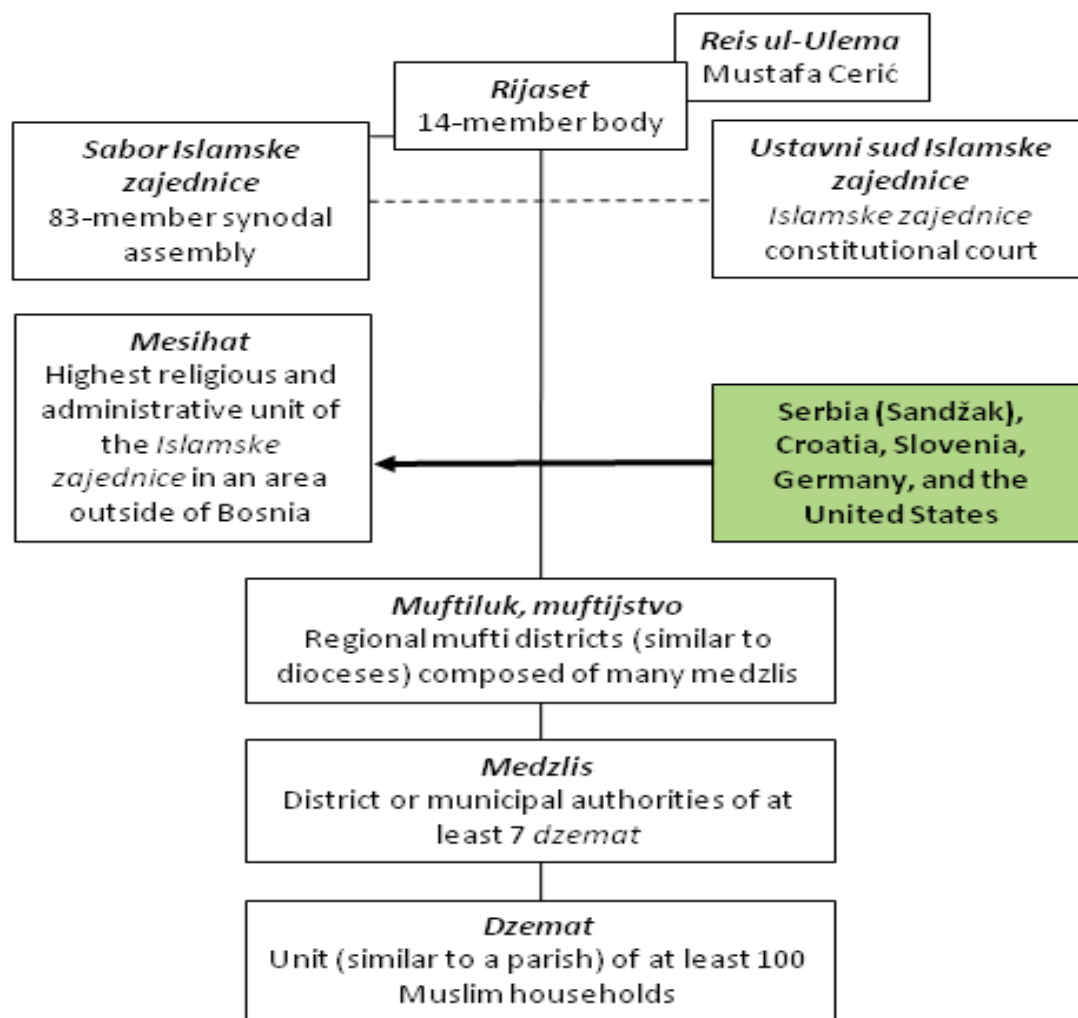


Figure 4. The Izlamska zajednice administrative hierarchy and organization (Oluic, 2009).

There are 35 dzemats, or parishes, in the United States, based in community or cultural centers. Michigan (with four) and New York, Pennsylvania, Illinois, and California (each with three) have nearly half of the dzemats in the United States (see figure 5). Their ties to the homeland are strong and can be seen in Reis Mustafa Cerić’s visits to U.S. Bošniak communities, his most recent being in October 2009, when he addressed the St. Louis Muslim community.

Figure 5. Bošniak dzemats in the U.S. as of 2009 (Oluic, 2010).



The U.S. Census Bureau’s American Community Survey provides statistical data, by decade, about immigrants from Bosnia and Herzegovina, but there are two important systematic errors. The data do not count the total number of immigrants per decade, but only those who came from Bosnia in a given decade and participated in the 2000 census. Additionally, this method fails to account for the several national groups found in Bosnia, but it is largely the Bošniak community that self-identifies as Bosnian, whereas Bosnian Serbs and Bosnian Croats self-identify as Serbs and Croats. Despite these caveats, the official and reputable data sources do indicate a clear trend of increased immigration from Southeastern Europe to the United States. According to the American Community Survey, 3,040 persons born in Bosnia and Herzegovina entered the United States prior to 1980. Any numbers reflecting Sandžak Bošniaks were incorporated within figures for immigrants from the Serbian Republic in Yugoslavia. Thereafter, during the relatively peaceful years of 1980 through 1989, only 1,870 Bosnians entered the United States. From 1990 to 2000, this number skyrocketed to 98,770 Bosnians. Most Bošniak sources note that as of 2006 there were up to 250,000 Bošniaks in the United States—perhaps more. Chicago, Detroit, and St. Louis are home to approximately a quarter of all Bošniaks in the United States. The Bošniak American Advisory Council for Bosnia and Herzegovina asserts that as of 2008 there were 350,000 Bošniaks living in the United States. The Bosnia & Herzegovina Embassy in Washington, DC, also provided immigrant population data. According to Emin Cohodarevic, the Bosnian Defense Attaché, the embassy conducted its own research into immigrant numbers, basing its findings on three sources: (1) the 2000 U.S. census, (2) numbers of immigrants and nonimmigrants admitted to the United States, and (3) Bosnian associations and communities in the United States. The attaché estimated that as of 2008, the total probably did not exceed 265,000 (see table 1). According to Agic the total number of Bosnian immigrants to the United States reached 200,000 by 2006. Bošniaks from the Sandžak region (see figure 1) began arriving in large numbers in 1967 through 1975 due to the poor economic conditions in Yugoslavia. The immigration picked up again from 1985 to the present, and according to Agic, of the 20,000-plus Sandžak Bošniaks in the United States as of 2006, the majority lived in the greater New York metropolitan area.

Table 1. Estimated U.S. population of Bosnian heritage (Bosnian Embassy, 2008)

State	Metropolitan Area(s)	Range
Missouri	St. Louis	40,000–43,000

Illinois	Chicago	35,000–39,000
California	San Jose, Santa Clara	20,000–23,000
Florida	Jacksonville, Clearwater, Orlando, St. Petersburg	20,000–23,000
Michigan	Detroit, Grand Rapids	17,000–20,000
Georgia	Atlanta	17,000–19,000
Washington	Seattle	12,000–14,000
Iowa	Des Moines, Waterloo	12,000–14,000
New York	New York City, Utica	12,000–14,000
Arizona	Phoenix	10,000–11,000
Kentucky	Louisville, Bowling Green	8,000–10,000
Oregon	Portland	4,000–5,000
Pennsylvania	Erie	4,000–5,000
Utah	Salt Lake City	4,000–5,000
Nevada	Las Vegas	4,000–5,000
Indiana	Fort Wayne	4,000–5,000
Connecticut	Hartford	3,000–4,000
Minnesota	Minneapolis	2,000–2,500

Bevo Mill, in southern St. Louis, has the largest Bošniak diaspora community in the United States. According to interviews with community leaders, a local bank manager, and the editor of the largest Bosnian-language newspaper in North America (SabaH), the population is reckoned to be anywhere from 40,000 to 70,000 Bošniaks in just this small area of St. Louis. It is the largest Bošniak community outside of Bosnia and Herzegovina. One of the most striking features of the Bošniak imprint on the local landscape is the newly constructed Islamic Community Center (figure 6). Located in a once-depressed area, the mosque has brought new life to the abandoned property. Shops, cafés, grocery stores, and other establishments have been completely revitalized as a result of the Bošniak community's entrepreneurial spirit and dynamic presence in Bevo Mill.



Figure 6. Islamic Community Center, Bevo Mill, St. Louis (Nicholas Cosmas, 2008).

Southern Commercial Bank, a Missouri regional bank, has one branch in Bevo Mill that caters almost exclusively to the local Bošniak population. It has signs in Bosnian, and it has Bosnian-speaking tellers. Even ATM transactions can be conducted in Bosnian. While the community has brought new life to the region, there have been some drawbacks. Due to the esoteric nature of the Bošniak community here, essential services can often be hard to come by. The Bošniak community is underrepresented in the local hospital staff, and translators are often not available for Bosnian-speaking patients, according to Dr. Aijlina Karamehic, a researcher at the St. Louis University School of Medicine. Moreover, based on poor experiences in their homeland, many locals do not trust the police, so crime can go unreported in the area.



Figure 7. St. Louis Metro buses. The normal color scheme is to the left; the buses with Bosnian colors, which serve Bevo Mill, are on the right (Nicholas Cosmas, 2008).

The cultural imprint of the growing Bošniak community in St. Louis is becoming quite apparent. Stores, community centers, and the local bank cater almost exclusively to the immigrants and manifest Bosnian national symbols and language. The metro buses serving the Bevo Mill area are even painted in the blue-yellow-white of Bosnia's national flag (figure

7). An interesting phenomenon noted by one of the community residents is that many Bošniak immigrants in other U.S. cities are beginning to move to St. Louis. This internal migration pattern reflects the desire of many of these residents to live among their own kind, as in other ethnic enclaves throughout the United States. A young Bošniak lady at Bosnian Specialties, a store in Hamtramck, MI, mentioned that she moved there from New York, stating, “I like it here because we are more separated than in NY—more scarves.” Table 2 lists Bošniak population data provided in an interview at the Bevo Mill offices of the Bosnian-American weekly newspaper SabaH. The newspaper has a weekly circulation of 60,000 and is purportedly the most widely read Bošniak diaspora newspaper in the United States. Based on these numbers, which are far from all-inclusive and certainly anecdotal, there are close to 300,000 Bošniaks in the United States. This figure slightly exceeds what was provided by the Bosnian Embassy. Senad Agic stated that in 2006 St. Louis had about 50,000 Bošniaks, Chicago 40,000, New York 40,000, Atlanta 10,000, Detroit 8,000, and Phoenix 6,000.

Table 2. Bošniak diaspora numbers from SabaH, St. Louis (Nicholas Cosmas, 2008).

Location	Bošniak
St. Louis	70,000
Chicago	45,000
Atlanta	35,000
New York City	30,000
Jacksonville, FL	20,000
Seattle	20,000
Detroit	15,000
Grand Rapids, Michigan	12,000
Phoenix	10,000
San Jose, CA	10,000
Salt Lake City	10,000
Houston	7,000
Las Vegas	7,000
Kentucky	7,000
Boston	“a lot”
Range	298,000+

Another data source was the annual donor listing found on the American-Bosnian Association website. The list included family names and city, state, and country location for 2005 through early 2008, listing 824 donors (see table 3). The greatest numbers of donors are located in Illinois (the Chicago area, 21.6%), New York (the Utica region, 20.9%), Missouri (the St. Louis area, 16.4%), and Iowa (10%).

Table 3. American-Bosnian Association website donor locations.

State	Metropolitan area	American-Bosnian Assn. donors
Arizona	Phoenix	13
California	Oakland	4
	Sacramento	1
Florida	Jacksonville	4

	other	2
Georgia	Lawrenceville	2
Idaho	Boise	34
Illinois	Chicago region	179
	other	4
Indiana	Fort Wayne	32
	other	1
Iowa	Waterloo	70
	Des Moines	5
	other	8
Kentucky	Lexington	5
	other	6
Massachusetts	Quincy	1
Michigan	Detroit region	29
	Warren region	11
	other	2
Missouri	St. Louis region	135
New York	Utica region	173
	other	4
Ohio	Youngstown	8
	Lakewood	5
Pennsylvania	Lancaster	1
Tennessee	Chattanooga region	10
	other	3
Texas	Houston region	6
	Ft. Worth–Dallas region	3
Vermont	Barre	2
Virginia	Greater DC region	9
	Richmond	6
	other	4
Washington	Richland region	6

The offices of SabaH provided an interesting contrast to the normally warm welcome found in the Bošniak community. Although coordination was made a day before our visit to interview the owner-editor, Sukrija Džidžovic, he failed to show up at the SabaH office. Moreover, the receptionist offered no explanation as to why the owner failed to keep the scheduled appointment and was very brusque in replies to inquiries. She questioned why we were researching the Bošniak community, who we were, and so on, but nonetheless hesitatingly provided the data listed in table 2. According to an overseas intelligence source,



Džidžovic is a former Yugoslav military officer originally from Ulcinj, Montenegro, who specialized in explosives and aircraft ordnance.

Radical Islamists Among Us?

The specter of radical Islamic activities among immigrant communities has not been lost on U.S. law enforcement and intelligence agencies. Several of the 9/11 hijackers had fought as mujahedeen in support of the Bosnian Muslim government forces during the 1990s Bosnian civil war. Their activities and links to radical Islamic groups in Bosnia and elsewhere led to several hundred being deported from Bosnia in 2005. According to Federal Bureau of Investigation officials, the now shuttered Islamic Tewhid Bošniak community center in the Bronx (figure 8) had verified links to radical Islamists in the Sandžak (Plav municipality) region of Montenegro. This community has been increasingly scrutinized over the past several years and was the U.S. branch of the Aktivna Islamska Omladina—a Bosnian Muslim fundamentalist organization that promoted an Islamic state in Bosnia. Through its outreach activities such as summer camps, Internet cafés, and youth centers, it has effectively recruited young, disenfranchised Bošniaks. SAFF, the organization's Islamic magazine, has been a font of radical Islamic preaching and has gained notoriety for publishing interviews with terrorists who have fought against U.S. forces in Iraq. In fact it can be seen as a signature clue for radical Islamic sympathies.

Figure 8. The Islamic Center Tewhid, Bronx, NY (Oluic, 2008).

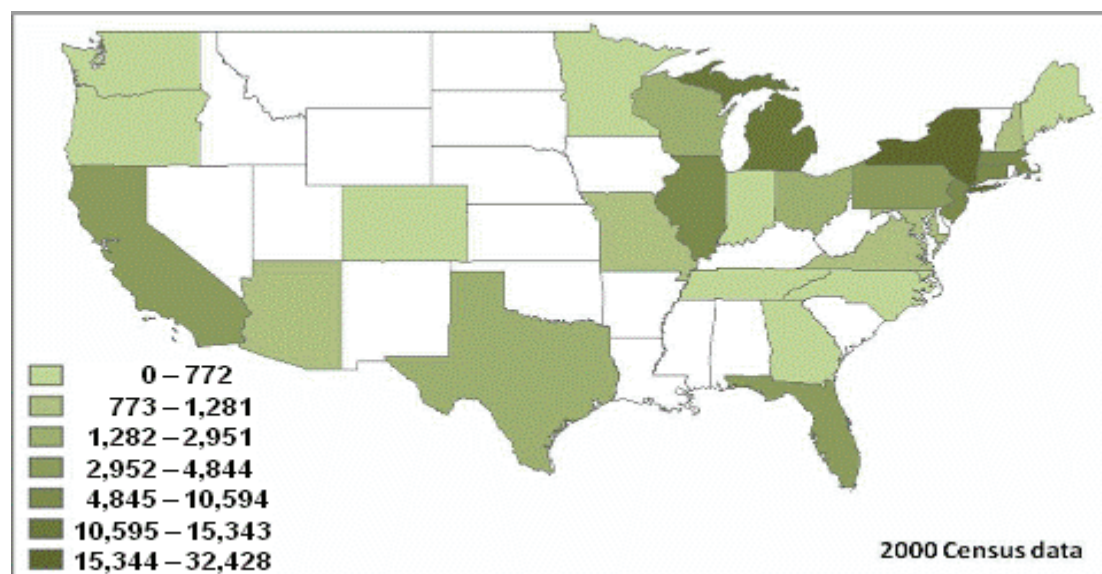
The United Muslims of North America (Udruzenje Muslimana Sjeverne Amerike), formerly at the Islamic Center Tewhid, have basically gone underground since the center's closing in early 2008. Although they still operate in North America, there is no permanent New York location even though the New York branch still leads the organization. During the 2008 Memorial Day weekend, this group sponsored a conference in New York City, hosting speakers from Macedonia, the Middle East, and other regions. In one of the conference's many meetings, it was reported that a primary goal of the United Muslims of North America should be to remain decentralized as an organization and in their activities. A possible explanation is that they wish to avoid investigation by law enforcement agencies or allow flexibility in their operations. The government's concern about the Bošniak community here and in Europe is manifested in official reporting, law enforcement activities, and information portals such as the Open Source Center, which provides thousands of timely, tailored translations, reporting, and analysis on foreign policy and national security issues from the center and its partners—publications, television and radio stations, and Internet sources

around the world. Most important, it covers Bosnia and Herzegovina's Bošniak community. Tragic incidents involving the U.S. Bošniak community have taken place, most spectacularly in the February 2007 Salt Lake City Trolley Square Mall shooting rampage. Sulejman Talovic, an 18-year-old Bosnian Muslim refugee whose family settled in the United States, killed five people and severely injured four others before being shot and killed by police. Several sources claim that he was shouting, "Allahu Akbar!" before being gunned down. Some authorities, such as the local FBI office, contend that the massacre was not related to radical Islam. Talovic's father, Suljo Talovic, noted, however, that his son had been involved with certain individuals at a mosque, and his girlfriend at the time said that Sulejman had told her, "Something is going to happen tomorrow that you'll never be able to forgive me about." Moreover, Talovic's father, who fought in Bosnia as a muhajideen (as did other Bosnian refugees in the Salt Lake City community), asserted that other people had pushed his son to murder; this should have been enough to cast doubt on the claim by authorities that the killings were not terror related. It was also established that Sulejman's father was a congregant at the Al Noor mosque, which was close to the shopping center where the massacre took place. While it is true that Sulejman Talovic was a troubled youth, having had run-ins with the local police, he was not traumatized by the war and was not even in Bosnia during the war. A somewhat more sinister and clouded story emerges when we look at another family member. Talovic's cousin Amir Omerovic, a naturalized citizen from Bosnia, on March 4, 2002, in Connecticut admitted to sending threatening letters (falsely claiming to contain anthrax) to Connecticut Governor John C. Rowland, as well as to the U.S. Coast Guard and Marines in Connecticut. Part of the letters, according to the New York Times, read: "This is only the beginning. Americans will die. Death to America and Israel." Another incident involving allegations of terrorism and the Bošniak community occurred around Halloween in late October 2007 at a Brooklyn, NY, apartment building (see figure 9). According to a resident and witness to the event, the building was raided by law enforcement officials (supposedly the NYC Police, Immigration and Customs Enforcement, and U.S. Marshals) and one suspect was taken away by authorities. The resident stated that one of the officers told him that the suspect was involved in terrorism. The apprehended suspect, Mr. Purišić, a Bošniak immigrant, lived with his wife in the building. It was his wife who reportedly contacted law enforcement officials after an incident of domestic violence.



Figure 9. Brooklyn apartment building where a Bośniak male was apprehended for alleged terror activities (Oluic, 2007).

There is an extensively documented linkage among radical Islam, al-Qaeda, and Bosnia and Herzegovina. This link extends from Bosnia to the United States and has been highlighted by the June 2009 conviction of Christopher Paul in Ohio for “providing material support to terrorists and conspiring to use a weapon of mass destruction,” according to Agence France-Presse. Paul fought with the Bosnian Muslim forces against the Serbs from 1993 through 1995. He “continued to work with al-Qaeda upon his return from Bosnia in 1997 and ‘conducted terrorist training’” replicating what “he had received in Afghanistan and Bosnia.” He was known to have links to radicals in the Balkans and travelled under several aliases, using various illegally obtained passports. Bośniak radicals have been arrested on terrorism charges in New York City and North Carolina. Anes Subasic, a naturalized Bośniak immigrant, and Hysen Sharifi, a Muslim naturalized U.S. citizen from Kosovo, were arrested in July 2009 as part of the Daniel Boyd terror conspiracy. They were charged, along with five others, with conspiring to provide material support to terrorists and conspiring to murder, kidnap, maim, and injure persons abroad. Adis Medjunin, a Bośniak immigrant, was arrested in Queens, NY, with a co-conspirator, Zarein Ahmedzayon, an Afghan immigrant, on January 7, 2010. Both have been linked to Najbullah Zazi, the Colorado airport taxi driver who was arrested in September 2009 on charges of conspiring to commit terror attacks in the United



States. All three men attended Flushing High School in Queens and were plotting to commit major terror attacks in the United States and overseas.

The Albanian Diaspora and Immigrant Community

The U.S. Albanian community is much more diverse than the Bošniak community and thus somewhat more difficult to survey and map. The diaspora community consists of Catholic, Muslim, and Orthodox religious groups. They have different immigration timelines and settlement patterns and unique U.S. experiences and histories. Many do share with the Bošniaks the bitter memories of fleeing war-torn Yugoslavia. Differentiating between these religious communities is quite difficult, as census data do not reflect religious affiliation, and therefore the data presented have to be viewed with the caveat that they cannot exclusively represent Muslim members of the Albanian diaspora. Moreover, the Albanian identity, unlike the Bošniak, rests on clan membership, language, and shared history, much less so on religion, although greater than 80% of ethnic Albanians are Muslim from Albania, Kosovo, Macedonia, and Serbia (see figure 1). For the recently transplanted Albanian community in the United States, the immigration pattern is also similar to that of immigrants from Bosnia and Herzegovina. The Albanian community in the United States is significantly larger than that of the Bošniaks. Most estimates place the total Albanian diaspora slightly over 1 million. In the past 30 years, approximately 4,780 Albanians arrived in the years prior to 1980, while 1,810 arrived from 1980 through 1989, and then the number surged to 36,780 from 1990 to 2000. These numbers represent immigrants from Albania proper and reflect the exodus fleeing the dramatic failure of communism. These numbers do not include ethnic Albanians originating from Greece, Kosovo, Macedonia, or Serbia and therefore are less than the actual number of ethnic Albanians present in the United States. Nonetheless, these data are relevant since it can be reasonably assumed that the same concentrations reflected in the map in figure 10 served as gateway communities for refugees and immigrants coming from Greece, Kosovo, Macedonia, and Serbia. Figure 10 depicts the spatial distribution of the Albanian community across the United States. As the data presented are based on the 2000 census, they do not reflect the religious background, only those simply identifying their ancestry as Albanian.

Figure 10. The U.S. Albanian diaspora community based on 2000 census data (Oluic, 2008).

FBI and other government sources note that the vast majority of Albanian immigrant and diaspora communities are found in Detroit and New York City. Moreover, there is a dangerous and powerful Albanian organized crime network centered in New York City and Detroit. This has led the FBI to establish the Balkan Organized Crime Task Force based in New York City. The Albanian population of New York City has been a concern of the task



force for some time because since the 1990s a new Albanian mafia has displaced the Russian mob in New York. With its bona fide links to Europe, the Balkans, and terrorist organizations such as the Kosovo Liberation Army, there is a significant cause for concern over the Albanian community in New York. A Brooklyn roofer with alleged ties to the city's Albanian mafia has been linked both anecdotally and in the literature with the raising of more than \$30 million in arms deals for the Kosovo Liberation Army during the 1990s. In her book, Stacy Sullivan also explored the question of why many members of the Albanian diaspora have failed to embrace American culture and instead espouse radical nationalist beliefs, remaining fairly self-isolated from mainstream society. According to Tahir Kukiqi of the Albanian Islamic Cultural Center in Staten Island, NY, there are about 100,000 or more Albanians in the greater New York City area alone. The majority of them are Muslim, while an older and more established Albanian Christian community is found in upstate New York. The center on Staten Island houses a cultural center, elementary school, mosque, and meeting place for more than 2,000 Albanian Muslims. According to Kukiqi, the vast majority of the members in the community arrived in the United States during the Communist era, in the 1980s largely, and often came via third countries such as Egypt, Turkey, or elsewhere in the Middle East. As opposed to their Orthodox and Catholic Albanian counterparts, the Albanian Muslim mosques have no hierarchical relationship to any higher authority and are much more decentralized than even the Bošniak community.

Figure 11. Staten Island Albanian Islamic Cultural Center (Oluic, 2008).

Kukiqi asserted that this affords each Muslim community greater access to members since each one can address specific local community needs, but on the other hand, such leeway can have negative consequences if questionable leaders are in charge of a mosque or community center. When asked whether it was common that the wrong people can take over an Albanian community, Kukiqi said he was only "speaking hypothetically." During the course of discussions, he never mentioned that the Albanian terrorists in custody for plotting to kill soldiers at Fort Dix, NJ, in 2007 were occasional worshippers at the mosque. Echoing Kukiqi's comments, Father Anton Kçira, a Roman Catholic priest from Kosovo and head of St. Paul's Albanian Community Church near Rochester Hills, MI, noted that in the past few years many Albanian Muslims in the greater Detroit area have grown increasingly fundamental in their interpretations of Islam. Imam Shuajb Gerguri of the nearby Albanian



Islamic Center and Mosque in Harper Woods, MI, noted that most of the area’s Albanian immigrant community came from central Albania and Kosovo. In the area neighboring the Staten Island mosque (figure 11), a number of Albanian businesses have been established, including a halal butcher shop, a pizza shop, and other family-owned businesses. None are overtly ethnic or nationalist, nor do they display Albanian symbols. In this respect, there is a stark contrast between the somewhat older Albanian community that arrived in the 1980s and the newer community that settled in the Lydig Avenue area of the Bronx. In that newer community (census tract 248), Albanian identity is much more evident and pronounced (figure 12). Whereas there is little ethno-centric Albanian advertising and there are few ethnic shops in the Staten Island community, on Lydig Avenue the presence of the Albanian community is vibrant and clearly marked on the urban landscape. According to a local shopkeeper it purportedly has the highest concentration of Albanians in New York City.

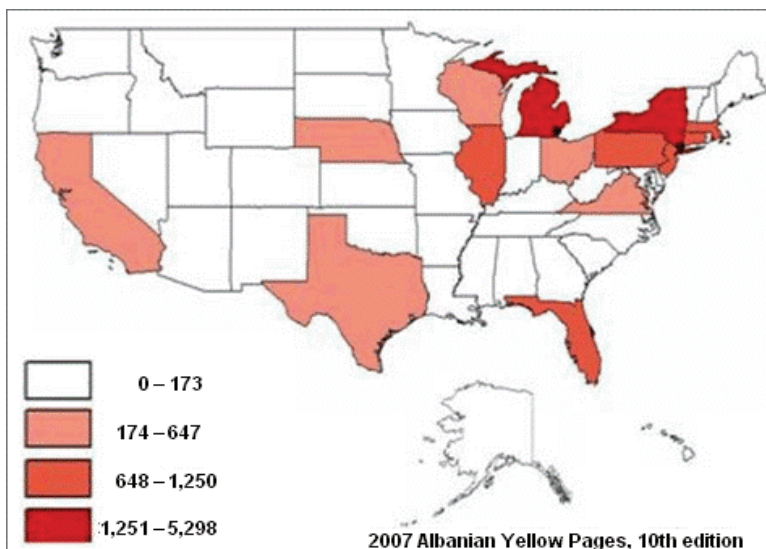


Figure 12. Albanian storefront on Lydig Avenue, the Bronx (Oluic, 2008).

Convenience store windows display advertisements for milk and qevapi (an Albanian lamb sausage) and advertisements for TV-ALB, a media company located in northern New Jersey specializing in television, radio, and telephone services for the Albanian diaspora. Service from this

company includes 20 Albanian television stations, Albanian radio, and Albanian telephone service, all received via satellite, providing connections back to the homeland. The red-and-black Albanian flag motifs are quite noticeable the length of Lydig Avenue. These colors are used in most advertisements and announcements, targeting the Albanian community.

Figure 13. The Albanian diaspora in the United States, based on the 10th Edition of the Albanian Yellow Pages (Oluic, 2008).

Ismer Mjeku, the Bronx-based publisher of the Albanian Yellow Pages and owner of Albanian.com, estimates that there are over 1 million Albanians in the United States. His 2007 Yellow Pages were the 10th edition and provided an enormous wealth of community information and anecdotal data on the U.S. Albanian diaspora. Although the directory cannot be considered accurate in the sense of a detailed census or representative survey, it does mirror fairly well the percentage of total diaspora numbers found in the 2000 U.S. Census database (table 4). According to both the census and the yellow pages, the five states with the largest Albanian diaspora communities are New York, Michigan, Massachusetts, New Jersey, and Connecticut. As with the Bośniaks, the Albanians have their community centers or parishes but to a much lesser degree. There are 11 of them, including 3 in the New York City–New Jersey metropolitan area, 3 in Connecticut, and 2 in Michigan.

Table 4. Comparison of the 2007 Albanian, 10th edition, and 2000 U.S. Census figures (Oluic, 2008) Yellow Pages

States & DC	Albanian Yellow Pages, 10th Edition		2000 U.S. Census data	
	Ethnic Albanians	Proportion of U.S. ethnic population	Ethnic Albanians	Proportion of U.S. ethnic population
New York	5,298	26.57%	32,428	29.38%
Michigan	3,244	16.27%	15,343	13.90%
Massachusetts	1,138	5.71%	10,594	9.60%
New Jersey	1,250	6.27%	7,336	6.65%
Connecticut	1,188	5.96%	7,200	6.52%
Illinois	1,030	5.17%	6,424	5.82%
Florida	1,052	5.28%	4,844	4.39%
Pennsylvania	805	4.04%	4,520	4.10%
California	647	3.24%	3,670	3.33%
Ohio	342	1.72%	2,951	2.67%
Texas	560	2.81%	2,417	2.19%
Wisconsin	434	2.18%	1,972	1.79%
Missouri	171	0.86%	1,281	1.16%
New Hampshire	61	0.31%	1,116	1.01%
Arizona	169	0.85%	995	0.90%
Virginia	261	1.31%	963	0.87%
Maryland	158	0.79%	916	0.83%
Tennessee	102	0.51%	772	0.70%
North Carolina	116	0.58%	728	0.66%

Maine	95	0.48%	649	0.59%
Georgia	173	0.87%	613	0.56%
Oregon	72	0.36%	592	0.54%
Washington	132	0.66%	508	0.46%
Minnesota	92	0.46%	444	0.40%
Colorado	79	0.40%	435	0.39%
Indiana	111	0.56%	343	0.31%
Alaska	42	0.21%	319	0.29%
District of Columbia	42	0.21%	none reported	
Idaho	53	0.27%		
Iowa	61	0.31%		
Kansas	30	0.15%		
Kentucky	92	0.46%		
Louisiana	34	0.17%		
Nebraska	369	1.85%		
Nevada	53	0.27%		
Rhode Island	37	0.19%		
South Carolina	35	0.18%		
Utah	36	0.18%		
Vermont	36	0.19%		
12 remaining states	238	1.19%		

As noted in table 4, there is a fairly large Albanian diaspora in Ohio, centered in Lakewood, which neighbors Cleveland to the east. According to Albanian community leaders, there are an estimated 5,000 Albanians in the Greater Cleveland area. Lakewood city officials verify that there is a large Albanian diaspora presence in the northern Ohio region. Lakewood, much like Detroit and New York, appears to be a gateway community for Albanian immigrants. The majority came to Ohio during Yugoslavia’s post-1994 disintegration, increasingly so after 1999. To accommodate their needs in a new homeland, the city had the “City Services Booklet” translated into Albanian. Although at times there is a language barrier, they have assimilated very well into the region and there appears to be no distinct ethnic enclave as found in Detroit or New York City. However, according to a local newspaper article, there are apartment buildings in Lakewood that cater exclusively to the Albanian community. There is an Albanian Orthodox Church located at the municipal boundary of Cleveland and Lakewood off West 117th street; it serves an older and much more established Albanian Christian community. The northeast Ohio diaspora appears to be a mix of Catholic, Muslim, and Orthodox; however, no accurate figures are yet available. Research travel to Boston, Cleveland, Detroit, and New York City revealed that the majority of pre-1990 Albanian immigrants are Christian, while the post-conflict Yugoslav immigrants are Muslim. Overall, the number of Albanian mosques and churches nationwide reflect the old and new Albanian diaspora. One source lists 16 Orthodox and 11 Catholic churches and three mosques in the United States. The majority of churches are attributable to the older, pre-1990 Albanian communities. The mosques are more recent construction, with two located in Michigan and

one in New York City. Lakewood municipal officials mentioned that there appear to be “inner” and “outer” circles among the local Albanians. The interviewed officials were not surprised to hear that this research included collaboration with the FBI. As noted by the FBI, the Albanian organized crime network lies along an axis from Detroit to New York City, traveling right through Ohio.

An Albanian Threat?

Albanian-affiliated organized crime is the gravest threat perceived by U.S. police and intelligence officials. Aspects of Albanian culture, such as the clan system, social organization, and a unique language, are especially conducive to masking criminal activities, compelling loyalty to a criminal enterprise, and operating behind a veil of secrecy and silence. These attributes make it exceptionally difficult for U.S. law enforcement officials to counter criminal networks. Can this unique culture also be utilized for radical organizations and activities? The May 8, 2007, arrest of six Islamic radicals conspiring to conduct a terrorist attack on Fort Dix, New Jersey, caught the United States off guard. After a 15-month FBI investigation, they were arrested in a sting operation during which they were attempting to purchase automatic weapons. Four of the men arrested were ethnic Albanians: three brothers from Macedonia and Agron Abdullah from Kosovo. One of the other two is Palestinian, one Turkish. The three brothers—Dritan, Shain, and Eljvir Duka—came to America by illegally crossing the U.S.-Mexican border and worked in construction and roofing. In fact the Duka family attended services at the Staten Island Albanian Islamic Cultural Center before moving to South Jersey from Brooklyn. Although defense attorneys have asserted that the men were entrapped, recorded conversations indicate that the men had a deep-seated hatred for the United States and were ready for jihad, wanting to kill as many Americans as possible at Fort Dix. The plotters also considered alternative targets, including the Lakehurst Naval Air Engineering Station and Fort Monmouth in New Jersey, Dover Air Force Base in Delaware, a U.S. Coast Guard facility, and the Army-Navy Football Game in Philadelphia. Ultimately, they chose Fort Dix because one of them had delivered pizzas there and was able to obtain a map of the installation from his father’s pizza shop. It was a tip from a Circuit City employee in January 2006 that would lead to the FBI’s investigation that monitored and recorded the group’s activities. The employee alerted police to a video that he was to convert to a DVD, showing “men firing assault weapons, calling for jihad and yelling ‘God is great’ in Arabic,” reported the Washington Post. The FBI successfully infiltrated the terrorist cell with two informants who were able to record conversations with the plotters and observe their activities. For example, one plotter said, “My intent is to hit a heavy concentration of soldiers.... This is exactly what we are looking for. You hit four, five, or six Humvees and light the whole place ... and retreat completely without any losses.” According to Greg Copley of Defense & Foreign Affairs, the arrest of these men on terrorism charges relates directly to a pattern of Islamist terrorist support operations by Bosnian and Albanian radicals in the New York, New Jersey, and Pennsylvania area. An alarming aspect of this affair is the fact that there appears to be no known direction from abroad—it was truly a homegrown cell. These men are believed to have been influenced by the Iraq war, Islamist propaganda video footage of American attacks “against Islam,” and jihadist and al-Qaeda videos. The wealth of information, propaganda, and digital imagery available on the Internet also serves to radicalize vulnerable individuals. Additionally, it has been alleged in some media reporting that the Duka brothers were influenced by their uncle who became radicalized in a New York prison before being deported back to Europe. Under his influence they gave up alcohol, grew beards, and began regular attendance at mosques. Once in custody, Eljvir Duka continued espousing radical Islamic ideology in messages to other inmates, and Dritan Duka hid an al-Qaeda DVD in a prison library book. From 1999 to 2008, 206 Albanian immigrants were deported for criminal activities. Over 250 Serbian and 42 Macedonian immigrants were also removed from the United States, but currently there is no mechanism available to determine how many were of Albanian ancestry from Kosovo and Macedonia.

Observations and Conclusions

- The Albanian Muslim and Bośniak communities have received relatively scant attention from U.S. intelligence and law enforcement organizations. Even though radical Islam and terrorism in the Balkans have been explored, the links of these very communities with their United States and global emigrant communities are only beginning to be illuminated. Most unclassified information is anecdotal at best, much of it coming from the diaspora communities themselves. Although the 2010 census will provide current information on U.S. immigrant and diaspora communities, the lack of a “religious adherence” response on the census survey hampers efforts to better understand and shed light on these communities. Moreover, the typical equating of Bosnian with Muslim, when in reality several national groups can be categorized as Bosnian, further hinders the ability of researchers to investigate the community.
- The decentralized nature of today’s terrorism, as highlighted in the Fort Dix terror attack plot, represents a profound threat to the United States. There have been numerous such plots in Europe in which homegrown terrorists, unaffiliated with any major terror organization, took it upon themselves to act. The June 4, 2006, arrest of 17 men accused of plotting bombings in Ontario has been linked to a half dozen countries and includes the arrest of two suspected terrorists in Atlanta in 2006. Monitored calls to Sarajevo, Bosnia, and elsewhere verify the globally linked terror network and jihadist ideologies. Given the porous border between the United States and Canada, greater consideration must be given to monitoring these diaspora communities. The 1990s Balkan mujahedeen fighters and their Bośniak advocates and supporters have been tied to the 9/11 attack, the Madrid bombings, and numerous other minor and attempted attacks in Europe.
- The spread of Islamic fundamentalism in the Balkans has been well documented in several recently published books and further highlights the ties between the wartime Bosnian Muslim leadership and al-Qaeda. Issuing Bosnian passports to al-Qaeda members by Bośniak officials at the Bosnian Embassies in Vienna, Austria, and Zagreb, Croatia, is just one of many examples available to analysts and policy makers. As these countries enter the European Union, the ability to use fake passports presents a real quandary for U.S. Immigration and Customs Enforcement officials.
- Just as members of the Somali refugee communities in the United States and Europe returned to Somalia to fight the Ethiopian invasion of their homeland in 2006, the Albanian and Bośniak immigrants could return to their homelands should renewed fighting arise. It is estimated that at least 20 Somali-Americans have gone to join the insurgency against the Ethiopian-backed transitional government in Somalia, presenting unique challenges to U.S. counterterrorism efforts to halt the path to radicalization and possible growth of domestic militant Islam. The self-imposed isolation and hesitance towards integration of immigrant communities such as the Somalis in Minnesota facilitates the recruitment of vulnerable individuals by radical Islamic religious leaders and terror networks. The internal migration of Bośniaks to the St. Louis urban area to be among people like them probably merits the attention of the U.S. intelligence and law enforcement community.
- Although al-Qaeda’s power and influence have been significantly diminished, its influence, outreach, and recruitment through the notion of da’wa, a recently defined Islamic mission, and the glorification of jihad and martyrdom are significant. The recruitment of easily impressionable, disaffected, or frustrated diaspora members through the extensive use of global communication technologies, the Internet specifically, and ongoing military action in Afghanistan and Iraq should elicit a greater concern at all levels of government, including domestic intelligence, law enforcement, and security agencies. At a minimum, these agencies should consider focusing efforts on the larger U.S. Balkan Muslim diaspora and immigrant communities. Currently, the FBI’s organized crime units monitor criminal networks

based in New York City and Detroit, and the FBI counterterrorism division observes the Bośniak community in the greater New York City area as part of its overall effort. Based on this research, the greater Chicago and St. Louis areas have almost entirely escaped scrutiny.

- The access and capabilities offered by modern technology such as the Internet, untraceable wireless phones, and the ever increasing transnational ties back to the homeland present an increasingly difficult challenge for U.S. law enforcement agencies. The humanitarian resettlement of Balkan Muslim groups to the United States and the concomitant strengthening of ties back to the region have inadvertently imported exposure to another source of radical Islam. The communities' natural avoidance of local law enforcement agencies, based on wartime and communist-era experiences, further hampers domestic counterterror efforts. Additionally, the tight clan system makes it almost impossible to infiltrate Albanian organized crime networks specifically and Islamic Balkan groups generally. Special attention must be given to the organized crime network, as it is a proven and effective mechanism to transfer arms, launder money, and traffic humans. Although Albanian crime syndicates are fairly secular, the encroachment of virulent ideologies among an inherently dangerous organization should not be taken lightly.
- If the Somali immigrant and refugee community in the United States is a gauge of the development and susceptibility of being recruited into international terror, more effort should be placed in exploring other recent Muslim immigrant communities. Policymakers have to reconsider using a religion marker in census data collection and in government data collection in general in spite of our hesitancy to do so. The question of divided loyalties and lack of integration have long dogged immigrants in the United States. Do American Muslims show their primary allegiance to the teachings of the Koran or to our secular government? Religious radicalization of both American residents and foreign-born immigrants is no longer constrained by location—the ideologies of terror transcend the globe, and the United States is radical Islam's primary target.

Somali Piracy Tactics Evolve; Threats Could Expand Globally

Source: <http://www.nationaldefensemagazine.org/archive/2010/April/Pages/SomaliPiracyTacticsEvolve.aspx>

Underwriters and shippers are as concerned about what the United States and other powers won't do against Somali pirates, as they are about what the pirates will do against ships they insure, own and operate. While the Gulf of Aden is a relatively safe passage for the deployment of warships through a narrow corridor in a vast gulf, some Somali pirates have



retaken the initiative in the waters of the Indian Ocean off East Africa. Continuing to treat Somali pirates as a homogenous, if not a monolithic threat, is not working. The current approach is showing diminishing returns on investments in anti-piracy. The deployment of modern warships costs easily more than a billion dollars a year, if not more, to sustain. Risks to shipping and the costs of underwriting continue to rise in the ocean where 60 percent of global commerce transits. Meanwhile,

the return on investment in piracy, which basically involves arming and supplying a handful of men and sending them out on a mother ship and two skiffs, only continues to rise. Staying on the present course guarantees that the next generation long-range Somali piracy business

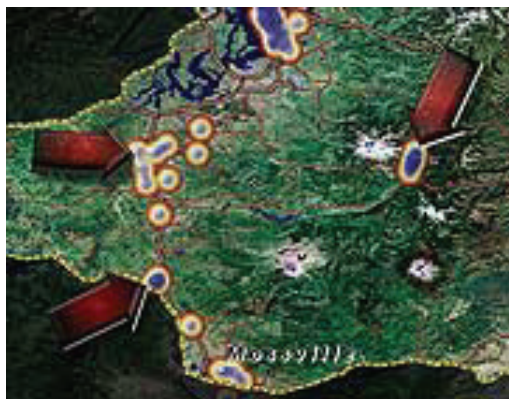
model will entrench itself. It is funded not just by record-breaking ransoms and local investors' money, but also by the flow of capital from foreign criminal gangs. Pirates now threaten sea lanes all the way to India and soon will threaten sea lanes all the way to the Strait of Malacca. This is a model capable of being exported worldwide. After the deployment of warships in the Gulf of Aden in late 2008, the underwriting and shipping communities were comforted. By the summer of 2009, it had become obvious that the navies of the world were thwarting northern Somalia's pirates. But by October, that same response inadvertently incited the more professional pirates of the eastern Somali shoreline, some led by former Somali naval officers, to pivot back into the waters of East Africa and expand long-range operations even into the high seas of the western Indian Ocean. Those pirates are now extending operations to waters rich in prizes such as the Gulf of Aden. Underwriters and shippers are therefore apprehensive again, given the new and expanding lead that pirates of southern and central Somalia gained over the world's navies by late 2009. Deployment of unmanned aircraft by the United States to the Seychelles to patrol local waters and the sending of a small contingent of French marines and Spanish private guards to protect tuna fishing boats off the islands was too little, too late. Somali pirates are operating mother ships and making attacks with impunity a thousand miles from Somali shores. The latest targets include not just tuna fishing fleets, but long-range high seas traffic. The Somali pirate gangs operating from southern and eastern ports such as Kismayo, Harardheere and Hobyo are preparing for more activity. Somalis have become adept at forward support: a technique first used in Gulf of Aden raiding, in which pirates relied on makeshift bases in Southern Yemen to resupply and refit, thanks to locals whose cooperation was likely bought with a promised share of the ransom. Evidence of forward support was discovered in the Seychelles early in 2009. Other credible intelligence indicates that at least one Somali gang has two mother ships lurking off the Maldives with orders not to come home until they hijack a large crude carrier or something similarly big by early 2010. It's obvious that these mother ships are relying more on local support than on a long "logistical tail" from their homeport. The ability to operate free from significant homeport support and instead rely primarily on forward support represents the "third generation" of Somali piracy. The first generation consists of largely opportunistic pirating within 50 miles of Somali shores, especially in the Gulf of Aden, which has occurred for centuries. The second generation consists of more premeditated and longer distance raiding into the Somali Basin and around the Seychelles and involves mother ships that juggle dependence on bulky stores on board, with continued logistical support from home ports. The third generation Somali pirates will venture beyond the limits of even traditional Somali fishermen and threaten new sea lanes, including the vital East Asian energy lanes just off India's western shores. Underwriters and shippers are justifiably worried about the world's navies playing catch-up in the central western Indian Ocean. The members of the world's leading seafarer union have already called for a boycott of the entire Indian Ocean. It is doubtful that deployment of long-range aerial surveillance in the central western Indian Ocean will make much of a difference if insufficient surface naval assets can engage the pirates and thereby deter and disrupt their operations. The East Asian sea lanes are as rich in energy and other resources as the lanes that pass through the Gulf of Aden and Suez Canal. It is not a matter of if, but when, the third generation of Somali piracy begins to inflict serious losses on those lanes off India's shores. The worst-case scenario could be set in motion by the European Union and NATO by diluting anti-piracy resources in the Gulf of Aden. As a result of the Somali pirate threat expanding unabated while the temperature rises between India and China, shipping and underwriting could become even riskier and even more expensive. The global economy, a system that relies on cheap and secure long-distance delivery of goods, energy and other resources, would take a major hit just as it is trying to get going again. While many strategic thinkers write about geopolitics, few write about what can only be called "mare-politics", or the principles of geopolitics applied to the oceans — despite the fact that the Indian Ocean boasts as many energy resources as Central Asia. Combining the dearth of ocean-based strategic thinking with the dependence of the global economy on high seas transport creates a dangerous blind spot that denies world leaders the advice and guidance they need. It also lulls them into thinking that the influence nations have on land extends

equally to the oceans. That is a dangerous miscalculation. One direct lesson from such strategic thinking is that on the high seas of the Indian Ocean, as any other sea, the brunt of the solution will have to be carried by private ships transiting by themselves, not by governments or by their navies. All nations also need to work more closely with shippers and insurers to counter pirates, if only because governments and navies can't and won't move as fast or effectively as the private players already in place. The major lanes that run on the high seas between India and Africa are in a space where no navy or navies can ever provide real protection. Private sector players should adopt a combination of measures, including better development and use of public and private intelligence, implementation of "best management practices" to deter and defend against pirate attacks, and improved underwriting solutions to help absorb the costs of attacks. These three approaches, when smartly integrated, can afford ships the most cost-effective risk management, and in a time period shorter than what any government or navy can make available realistically. If Somali pirates are allowed to demonstrate new prowess, not only will they earn even more international criminal support, but they also will become the envy of pirates in other parts of the world. This is not idle speculation: a long-range attack against an oil tanker off Benin by Nigerian pirates was attributed to envy-inspired copying. The biggest impediment to Somali-style piracy going global is having a failed state where pirates can park a stolen crude carrier within sight of shore without fear of being bothered by the local authorities. Fourth generation Somali pirates may simply kidnap premium, high-value hostages such as the ship's captain and chief officers, and while negotiating their lucrative release, use them as human shields on mother ships that constantly move all over the Indian Ocean with impunity. Rather than repatriate hijacked ships all the way back to distant Somalia, or abandon them and their cargo on the high seas at a loss, the Somali long-range raiders may spin valuable ship and cargo off to local insurgent groups or pirate gangs as payment so they are allowed to continue hunting unmolested in their waters. About the only real threat to Somali pirate expansion these days is from other pirates. Most pirates of the eastern Indian Ocean and East Asia don't have much use for crews anyway and may settle for such a division of spoils: some have networks ready not just to liquidate cargo but also ships, which are given new names, paint jobs and papers almost overnight. Those eastern pirates who don't agree to this arrangement will probably settle for a share of the ransoms Somalis collect. Fourth generation piracy is sure to appear sooner than later if we keep leaving the initiative to the best Somali gangs. Current counter-piracy approaches make it ironically even easier for them to reap most of the rewards, as their less capable competitors are eliminated, leaving the ocean and its richest prizes for them. The Somali piracy business model could soon go "viral" and export itself to not just to the rest of the Indian Ocean, but the rest of the world. And there will be nothing to stop it.

'Culture Maps' Becoming Essential Tools of War

Source: [http://www.nationaldefensemagazine.org/archive/2010/February/Pages/'Culture Maps' Becoming Essential ToolsofWar.aspx](http://www.nationaldefensemagazine.org/archive/2010/February/Pages/'Culture%20Maps'%20BecomingEssentialToolsofWar.aspx)

The U.S. military has access to the world's best topographic maps. It is now trying to build "culture maps" that include details such as a region's tribal affiliations, ethnicity, religion and language. The commander of U.S. Central Command, Army Gen. David Petraeus, in a number of speeches has repeatedly said that "human terrain" is the decisive element in counterinsurgency operations. "His remarks have had a rippling effect across the intelligence community," said Jesse Wilson, who works at the command's Afghanistan Pakistan Intelligence Center of Excellence. Officials there are pairing human terrain analysts with traditional



intelligence teams. Traditional intelligence, based upon satellite and aircraft imagery of the geophysical environment, worked well in past wars where open battle spaces far removed from civilians were the norm. Commanders needed to know the lay of the land in order to attack the opposing force. But in current conflicts, they are relying upon soldier interactions with the local people to gather information. “They’re told to walk the beat and make friends with the population,” said Navy Lt. Cmdr. Shane Halloran, who in December returned from a five-month deployment to Afghanistan. The socio-economic climate of a region and the cultural norms, values and attitudes are qualities that the nation’s intelligence agencies in the past have overlooked. The National Geospatial-Intelligence Agency “is not set up to collect this type of information,” said Joel Maloney, director of the military operations group within the agency’s analysis and production directorate. Intelligence analysts collect all the relevant geospatial information over an area, including the mapping, terrain elevation data and the latest imagery, and then analyze the terrain looking for culverts or other physical features that might lend themselves to an ambush or an improvised explosive device, or IED, attack, he said. They also include data from other intelligence disciplines such as signals or human intelligence. At Central Command, the human terrain specialists work side by side with the geospatial-intelligence analysts to produce maps of a different vein, said Wilson, team chief of regional commands south and west in the human terrain analysis branch. For example, if analysts plot on a map military reconstruction or development projects in Afghanistan with roadside bomb attacks during the same period, they may see correlations that show an increase or decrease in the number of those attacks over time. Human terrain analysts are trained to hone in on cultural facts quickly and fuse them with geospatial data to make maps that traditional analysts wouldn’t normally consider, said Swen Johnson, founder and CEO of SCIA LLC, a Reston, Va.-based company that specializes in socio-cultural intelligence analysis. Human terrain analysts seek to map out where tribes, ethnic groups and religious sects are located. They document attitudes — where a population’s beliefs and values are most prevalent — and annotate where certain behaviors tend to occur or not occur. “Human terrain” maps are assembled in layers so that analysts can correlate previously unrelated qualities of an area to each other, Johnson explained. One map might show the locations of all the tribes in a region. A second map of that same region might depict the known locations of all the suspected insurgents. By superimposing one over the other, an analyst might discover that the bad guys are in a single tribe. Social dynamics information, including local grievances and tribal rifts, can bolster troops’ knowledge of whether certain individuals or groups should be deemed friend or foe. Such maps could also be useful for search and rescue, and humanitarian assistance teams. “Zeroing in on the things that matter to the populations that we study and then turning that cultural information into a geospatial product is really at the heart of what we do,” said Johnson, an Army veteran. “We’re not just map makers. We also give assessments of what that map means,” he added. Troops lacked that insight in Iraq, which cost the nation thousands of lives and billions of dollars, he said. Johnson found himself in a tough situation as a counterintelligence special agent who was deployed to Kosovo in 2000. “I was supposed to walk the ground, meet with Muslim leaders, imams in their houses to find out where the bad guys were. But I did not have a good understanding of where the significant social groups were,” he recalled. It would have been nice if the maps that he carried had identified the neighborhoods where ethnic Albanians, Serbians, Turks and gypsies lived, he said. “You needed to efficiently reach those people, get the story and then send it up to higher headquarters to piece them together.” The deployment of unmanned surveillance aircraft has not fixed the intelligence gaps, he added. “All that equipment out there, to us, is taking away from where the focus ought to be: Using the tools of the social scientist to understand the environment on the ground,” said Johnson, who holds a doctorate in sociology and founded SCIA after completing a five-year enlistment in the Army. Troops on the ground, meanwhile, are tackling the problem with a new mentality. In a program separate from Central Command’s human terrain analysis efforts, the Army has embedded small teams of anthropologists with ground forces to collect data (see related story). Other initiatives have cropped up across regional command south in Afghanistan, Halloran said. A British task force element operating in central Helmand Province last year was ordered to

survey the populations through which they were moving. Newly arrived units to the theater are becoming aware of the data collection efforts. As Halloran was preparing to deploy back to the United States in December, he received a phone call from a Stryker battalion that had been moved out to Zabul Province as part of the realignment of forces in Afghanistan. “There was a [provincial reconstruction team] out there that didn’t have a lot of information for them in that area of Zabul, and they knew I had some [maps]. So they called me up and said, ‘Hey, we’re brand new here, what do you guys have for us?’” he recalled. Halloran and his team back at Central Command had produced wall maps depicting the region’s tribal safe houses. Previous units had used those maps as templates for policing and security operations. Troops would overlay additional data and use them as guidance for planning their missions. “It’s very much about having the information about the human geography of the area,” he said. The first thing that the International Security Assistance Force’s new regional command south commander, British Maj. Gen. Nick Carter, asked for upon taking the reins in November was an intelligence briefing on the population, said Halloran, who at the time was deployed as the human terrain lead at the Kandahar Intelligence Fusion Center. Special operations forces also are leaning on human terrain analysis products, said Wilson, who supported the Combined Joint Special Operations Task Force-Alpha commander in Afghanistan last year. Human terrain analysis was used to make assessments about the source of violence in the area. Because troops at all levels are finding utility in human terrain data, Central Command officials are pushing a plan to network U.S., coalition and allied forces into a single socio-cultural knowledge database that will provide them with pooled information. “You’re seeing an effort that actually transcends any single discipline and a link between civil operations and military operations,” said Air Force Maj. Tom Hornik, chief of the command’s human terrain analysis branch within the Afghanistan Pakistan Intelligence Center of Excellence. The so-called Afghanistan Pakistan tribal knowledge base would be accessed through a secure Internet host site, the Combined Information Data Network Exchange, or CIDNE. CIDNE is available for use by coalition forces in Afghanistan, said Air Force Maj. John Redfield, a spokesman for U.S. Central Command. It is available via three networks: combined enterprise regional information exchange system (CENTRIXS), battlefield information collection and exploitation system (BICES), and secret Internet protocol router network (SIPRNET). Access to U.S. databases is a problem for non-U.S. partners. The intelligence community has a propensity to over-classify reports, but sometimes the socio-cultural information in classified reports is not considered sensitive, said Wilson. Officials at Central Command’s human terrain analysis branch have decided to produce two versions of all products — the first one is classified and the second version is releasable to coalition forces. “It’s a burden on us, but we know that that is what’s needed in this sphere of information sharing,” Wilson said. Unlike geographical terrain that changes over the course of decades, the human terrain is constantly evolving. Maps need to be updated continuously, but with limited resources in the intelligence community, that is difficult to do, said Johnson. “We feel it takes at least 208 hours to make a good analyst into a good human terrain analyst,” he said. “It’s an art for sure, more than a science.”



Headcam Records a Cop’s-Eye View

Source: <http://www.aolnews.com/crime/article/headcam-records-a-cops-eye-view/19479828>

Each day when San Jose police officer William Pender goes to work, he straps on his badge, gun, radio and Taser. And then he attaches a small video camera to his left ear. The camera is part of a test program. Throughout Pender’s shift, it records whatever is in front of him. With the push of a button, he can save the video and audio of his interactions with citizens, suspects and fellow officers. It is the way of the future, he points out. “It’s actually really cool,” he says. “You can look from my point of view. What I see, the

camera sees.” William Pender, a San Jose, Calif., police officer, wears a small camera that records his actions throughout his shift. “What I see, the camera sees,” he says. Pender, a 15-year veteran, is one of 18 San Jose police officers participating in a pilot program to test the head cameras. Called the Taser Axon, the camera is made by Taser International, which also makes Taser electroshock guns. “I think it’s a tremendous piece of technology,” he says. “Everyone has been using cameras against us for so long. It’s nice to have our point of view instead of someone’s blurry phone picture that doesn’t tell the whole story.” The headcam, slightly larger than a Bluetooth phone, comes with a detached display screen and a microphone. The camera is mounted on a band that wraps around the back of the officer’s head. At the end of a shift, the officer downloads the day’s recordings onto a secure website but does not have access to edit them. “Overall, the product has worked exceptionally well,” says Sgt. Ronnie Lopez, a spokesman for the San Jose Police Department. “You know what they say: A picture is worth a thousand words. It has really allowed us to document what we do.” David Onek, a senior fellow at the Berkeley Center for Criminal Justice, says police agencies around the country are increasingly turning to new technology, especially cameras. Such equipment can be a valuable asset, he says, but officers must be careful not to intrude on citizens’ rights to privacy. “A number of these technologies can be additional useful tools for law enforcement, but none of them is a panacea,” says Onek, who also serves on the San Francisco Police Commission. “We need to look at how effective each is and balance that against legitimate civil liberties concerns and costs.” Taser International charges \$5,700 per officer for a three-year package that includes the camera and the secure video storage website, evidence.com. The Axon headcam proved its value to one officer last November in Fort Smith, Ark., another city where the device is being tested. Police officer Brandon Davis was wearing a headcam when he responded to a 911 domestic violence call and fatally shot an armed man. His recording of the incident helped lead to his quick exoneration. The headcam recorded Davis arriving at the house and talking with the woman who had called police. When she let him inside, he was confronted by her husband holding a handgun. Davis could be heard on the recording ordering the man nine times to drop his weapon. The man ignored the commands, and Davis ultimately shot him. After reviewing the video and audio of the event, authorities concluded that Davis had acted appropriately. Tom Smith, chairman and co-founder of Taser International, says the incident provided a “powerful validation” of the company’s two-year effort to develop the camera and a secure website for downloading recordings. “Although the outcome of this incident is tragic, we are proud the Axon video was helpful in the investigation of this event in order to protect the truth of what actually happened,” Smith said in a statement released by the company. “This video clearly demonstrates the power of the Axon on-officer camera.” Other cities testing the camera include San Diego, Cincinnati, and Aberdeen, S.D., which recently became the first to purchase the device. Pender says the head camera is a big improvement over the car cameras used by many departments. Unlike the car camera, which only shows events that take place in front of a police vehicle, the headcam can show an entire incident. “It’s a totally different type of technology,” he says. “Most of our work doesn’t happen in front of the car.” The Axon is designed so that it continuously records on a 30-second loop. The officer decides when to save an event and presses a button on his chest, automatically preserving the preceding 30 seconds of video along with the action that follows. During a recent traffic stop, Pender administered a sobriety test to a suspected drunken driver, then rewound the video to review the man’s performance and make sure he had the evidence he needed. “In court, he is going to lose because it’s all on tape,” he says. “The jury is going to see the guy stumbling around.” Pender, who decided to become a police officer after he was the victim of a bank holdup, says he believes the camera has the potential to improve the behavior of both the police and the public. The recording can provide clear-cut evidence and make it easier to establish a suspect’s guilt or innocence. It can also document police behavior, which could prove valuable in cases where an officer is accused of misconduct. Pender says he doesn’t act differently when he is wearing the camera. But an officer with a record of receiving complaints might be inspired to improve the way he or she treats people. “You feel very safe having it on because everything is being recorded,” he says. “At the same time, people act

very differently when you're wearing it. You have someone who might want to mouth off or not go along. They start looking at your head. "They ask, 'What is that?' They know they are being videotaped." Pender notes that officers who use the camera have to be aware of privacy issues. For example, officers need to turn off the camera when dealing with a juvenile or a rape victim, and, depending on the circumstances, when entering someone's home. It's also a good idea to remember to turn it off when using the restroom. "Sometime you forget," he says, "which is kind of scary." Spokesman Lopez foresees a day when the headcam is as standard as the police radio. "I predict in the future officers won't hit the street without wearing them," he says.

A New Book by Dr. Anat Berko

The Smarter Bomb – Women and Children as Suicide Bombers
(Hebrew)



- For the past several years the Intelligence and Terrorism Information Center has dealt with female suicide bombers as part of its overall coverage of suicide bombing terrorism. Dr. Anat Berko, a criminologist who received her PhD from Bar Ilan University, studied the involvement of women in anti-Israeli terrorism and revealed surprising facts. The Smarter Bomb is based in part on interviews she conducted with male and female security prisoners.
- To give our readers a sneak preview of the book and to reveal some of the findings about women who planned to become suicide bombers, the ITIC presents three page from the introduction, courtesy of Dr. Anat Berko and Yedioth Aharonot Publishers.

Introduction

"We'll be good together...One of my girlfriends will let me use her apartment so that we can be together...Bring condoms. You have some, right?" That was the message received by a 16-year old Israeli boy, tempted by promises of sexual adventures into meeting a girl he didn't know, behind which was a plot to kill him.

"Do you have a girlfriend?...Are you going to tell your friends about us?...We have to...Are you younger than I am?...Do you want to have sex??? I want to, but I don't want to get pregnant..."

Sixteen-year old Yair had a secret he didn't tell anyone. He thought he had met a girl older than himself who wanted to enter into a sexual relationship with him. Houda even made sure to ask, "what if your mother sees the condoms and finds out about us?" "Don't worry," he said, "she won't."

Houda manipulated Yair, weaving her web around him until he was trapped in a classic male adolescent fantasy. Their chats grew longer and more frequent, and his desire to meet her increased daily. Finally he went to the designated meeting place, where not only was Houda waiting for him, but her friends, and they killed him in cold blood.

The Houda I visited in jail hadn't changed. Using guile, ingenuity and cruelty she established her control over the other security prisoners until she had become their spokeswoman and unchallenged leader. Even after she was moved to a different wing because of the negative influence she had on the other prisoners, her shadow still hovered and threatened them. Any prisoner who dared to stand up to her, or who made her angry, risked having boiling margarine mixed with sugar thrown in her face and being scarred for life. There are prisoners who will remember Houda for ever.

For the most part, women in Palestinian society are pawns in men's hands, and passive during the stages of planning and carrying out terrorist attacks. They do not become terrorists as the logical outcome of a life of crime, as opposed to some of the male security prisoners. The examination of trial transcripts and discussions I held with Palestinian intellectuals made me suspect that the women sent on suicide bombing missions were often sexually exploited: "You're going to die anyway, so what difference does it make...?"

Carrying out a terrorist attack is supposed to upgrade the status of the terrorist's family, but the benefits received by the families of female suicide bombers are not equal to those received by the families of male suicide bombers. The discrimination between them is based on the circumstances under which women become terrorists, usually different from the men's. One can only wonder what makes a woman's conduct be considered exceptional, what motivates a woman to become a terrorist? What terrible thing did she do, or was done to her, that made her try to purify herself in such an awful way?

In many instances, women do not join a terrorist organization to carry out an attack. Rather the organization seeks them out and recruits them close to the prospective date in order to glorify itself and chalk up another attack to its credit. The various organizations are in serious competition over the number of attacks, and they hold a kind of head count to compare results.

Some of the chapters of my first book, *The Path to Paradise*, about suicide bombing terrorism, were devoted to women. Since its publication I have focused on women and children, and on the interaction between women terrorists and their dispatchers. My research indicates that women are simultaneously important and unimportant. This book examines the subject in depth and provides new insights, and various ways of viewing the involvement of women and adolescents in the service of terrorism. To gain a broader knowledge of the issue I interviewed Muslim clerics, terrorists, dispatchers of female terrorists, lawyers, and senior members of the Muslim community, both inside and outside prisons. The book is also based on the statements and stories of the female terrorists themselves. I spent many days observing military terrorist trials, and read transcripts and indictments. For the past fifteen years I have met with security prisoners in Israeli jails, among them those who orchestrated and carried out murderous terrorist attacks against Israeli civilians. The most notable among them was Ahmed Yassin, the late founder and leader of the Hamas movement. In recent years I have focused on women and adolescents who participated in terrorist attacks.

The names of the people and places in this book are fictitious, in part because of the high level of personal revelations of the people I interviewed. We shared a desire to deal with genuine issues without having harm come to them. What is written in these pages is based on conversations I held with people whom many consider impossible to understand. The special, close relationship I developed with them made it possible for me to document our meetings and try to understand their personalities and motives. I am certain that some of the events recounted in this book will open wounds for many Israelis who were badly hurt in terrorist attacks.

Within the words I looked for answers to the questions which prompted me to conduct this study: Can a woman be "good" according to the criteria of Palestinian society and a terrorist at the same time? What is behind what I learned from the meetings I held, that a terrorist woman in Palestinian society can simultaneously be important and unimportant? Is the involvement in terrorism a sign of the liberation of Palestinian women, or another way of oppressing them and preserving their social inferiority – which would explain their low status and the inferior rewards their families receive? Is the woman's body, naked and ideal as described as that of a virgin in paradise, a sexual incentive for the death industry set in motion

by men, in which the bodies of living women are sacrificed by explosions for the sake of replacing them with the women of paradise? Who are they, the Palestinian women who dared to leave their homes, in most cases without their fathers' permission, what made them, what made children join the terrorist machine? Can the human bombs of Islamic terrorism be stopped, and if so, how? Is a woman who carried out a suicide bombing attack a smart bomb or a stupid bomb?

Dr. Anat Berko

Rehearsing The Evacuation Of 70,000 Sports Fans In Less Than An Hour, With The Aid Of Avatars

Source: <http://www.medicalnewstoday.com/articles/185076.php>

What sports fan hasn't grumbled while waiting in a long, snaking lines to get into the stadium for the big game? It's enough to discourage even a diehard fan. But if you think it's a hassle getting into a sold-out game, imagine trying to get out after a bomb explodes - or even to get out under a bomb threat, for that matter. Let's start with the emergency lights failing. If you're thinking of feeling your way out by the light of your cell phone, join the crowd - they're right beside you, pushing fifty-across and a thousand-deep in a stampede. It's everyone for himself. Scenes like this may sound like a trailer for a Hollywood thriller (think Black Sunday), but their grim prospect is all-too-real. Last year, the Department of Homeland Security (DHS) and the FBI jointly warned of terrorist interest in attacking crowded stadiums. Small wonder: A bomb or noxious plume released over a throng of captive sports fans would cause major-league mayhem and terror. Mindful of the threat, stadium sentinels have been laying plans to manage and minimize the anarchy that would follow such an attack. Just how would authorities whisk 70,000 people out the gates and onto the roads quickly and safely? For an evacuation on this scale, there are no dress rehearsals or practice drills-just simulation software. Now, a new breed of simulation software - dubbed SportEvac - is being funded by the DHS Science and Technology Directorate (S&T) as part of the Southeast Region Research Initiative (SERRI), and developed and tested by the National Center for Spectator Sports Safety & Security (NCS4) at the University of Southern Mississippi. "SportEvac isn't simply more realistic," says program manager Mike Matthews of S&T's Infrastructure and Geophysical Division. It will become a national standard." Using blueprints from actual stadiums, the developers are creating virtual, 3D e stadiums, packed with as many as 70,000 avatars - animated human agents programmed to respond to threats as unpredictably as humans. Security planners will be able to see how 70,000 fans would behave - and misbehave - when spooked by a security threat. But a SportEvac avatar need not be a sports fan. The simulation includes make-believe stadium workers, first responders, even objects, such as a fire trucks or a fan's car. SportEvac tracks them all, accounting for scenarios both probable and improbable. Simulating thousands of people and cars can impose a crushing load on software and hardware. That's why, unlike SportEvac, most evacuation software apps are unable to simulate a crowd much larger than 5,000. For a college or NFL football game, that's bush-league. Beyond scaling problems, earlier simulators did not account for the myriad variations that make human behavior hard to predict and human structures hard to simulate. How adversely, for example, would an evacuation be impaired if an audible were called - a wet floor, a wheelchair, a stubborn aisle-seater, a fan fetching a forgotten bag, or an inebriated bleacher bum? Conventional evacuation simulators couldn't say. SportEvac can. And like an open-source Web browser, the SportEvac software will get better and better because it's built on open, modular code. If your IT intern creates a module that can more accurately predict parking lot gridlock, just plug it in. This also means it can be customized for any sports arena. By simulating how sports fans would behave in the minutes following an attack, SportEvac will help security experts across the country to plan and train and answer key questions, such as:

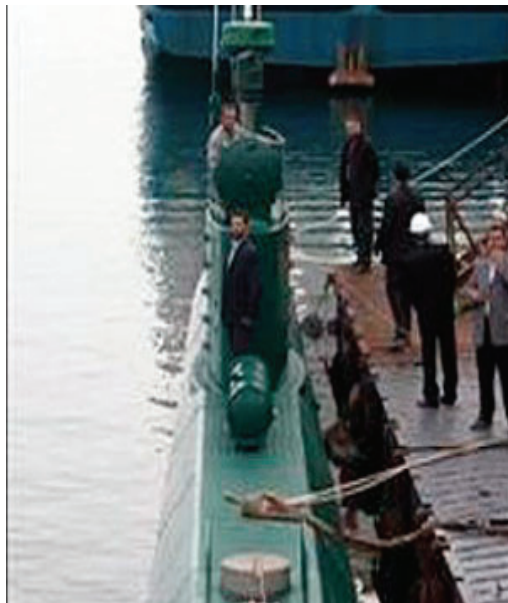
- How can my stadium be evacuated in the shortest time?
- How can civil emergency workers quickly get in as fans are dashing out?
- How can our stadium guards and ushers provide valuable information to civil responders and assist them as the evacuation unfolds?

"Interoperability is also a key goal," says Lou Marciani, NCS4 Director, who serves as the S&T project's principal investigator. Stadium security officers can use SportEvac to rehearse and refine procedures with civil responders. During a real evacuation, guards might use the same radios as the civil responders. And for every usher with a smartphone, a "SportEvac Lite" application will graphically show where fans or cars are bottlenecked. Drawing on actual architectural CAD data, the Mississippi researchers are creating 3D virtual models of seven of the state's college sports stadiums. This year, in summits and workshops, security teams from the university athletic departments will test and refine SportEvac, with help from local police, Mississippi Homeland Security agents, the Mississippi Emergency Management Agency, and security specialists from pro sports. It will then be deployed to the seven state universities. Once the schools give it the green light, S&T will make the advanced version available to other universities, pro sports venues, and amateur sports organizations. While not quite as immersive as the recent 3-D movie Avatar, SportEvac will create a safe, virtual stadium where security teams can practice guiding fans to safety, without risking life, limb, or lawsuit.

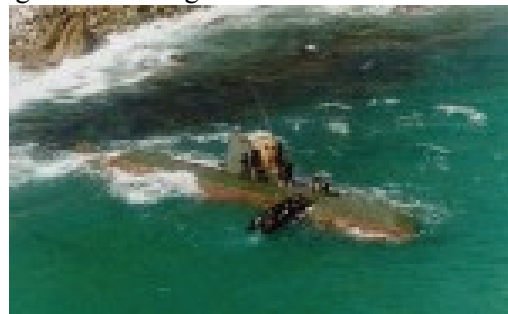
Is the U.S. Prepared to Face Midget Subs?

Source: http://www.popularmechanics.com/technology/military/news/midget-sub-attacks?click=pm_news

Don't let the funny, politically incorrect name fool you: Midget subs are a real threat. In the



hands of North Korean and Iranian navies, these small vessels make good platforms for ambushes—and the U.S. Navy is clearly ready to hone its anti-submarine skills. War tensions have been high since last week's announcement by the South Korean government that a 60-foot North Korean submarine fired a torpedo that sank a South Korean corvette and killed 46 sailors at the end of March. The South Koreans stated that a Yeono-class (alternatively spelled "Yono" – top photo) midget submarine fired the torpedo in March. (They also field a larger midget submarine, the Sang-O, that fits 15 sailors (bottom photo). At least one of these subs was also on patrol when the attack happened, according to an international team of investigators looking into the incident with



South Korea.) The attack occurred in 150 feet of water, enough room for the midget submarine to maneuver. Any sub that weighs less than 150 tons is called a midget. They can't travel too far on their own, and depend on support vessels to extend their range. In shallow water, where sonar returns are cluttered, they can prove quiet and sneaky. Often this means they can lay mines or insert commandos on beaches. According to statements by South Korea, attacks from midget subs can also include torpedoes. Iran is known to operate midget subs, and after buying a handful from North Korea, it is believed to be making its own. A civilian ship hired

to dredge the area of the attack found remains of what the government labeled a CHT-02D torpedo, made in North Korea. That torpedo would have a big enough warhead—250 kilograms—to destroy the corvette. Government reports state that the ship's sonar did not detect the submarine or the torpedo. That is what concerns the U.S. Navy. Two things heighten the risk of a similar ambush by midget submarines against U.S. ships: the complex sonar picture of shallow water where these small subs can operate, and a post-Cold War decrease in anti-submarine training. "Instead of a large number of Soviet nuclear-powered submarines on the open ocean, advanced conventional submarines operating in the littorals have emerged as the most serious threat to U.S. forwardly deployed forces, military sealift and merchant shipping," Milan Vego, professor of operations at the Joint Military Operations Department at the Naval War College, wrote in a recent piece for *Armed Forces Journal*. "The emerging threats ... are minisubmarines, swimmer-delivery vehicles, remotely operated vehicles and autonomous underwater vehicles." This week the Pentagon announced it would step up its anti-submarine training, engaging in exercises with South Korea. The decision is "a result of the findings of this recent incident," Pentagon spokesman Bryan Whitman told reporters. But crash courses in sub hunting may not help much; professionals admit it's an art as much as a science. The United States' sub-hunting abilities have atrophied since the Soviet Union dissolved. One obstacle to revamping anti-submarine training is bringing it out of simulators and into the real world. It takes a lot of effort to conduct a real sub hunt, but these skills need to be continuously honed. "The skills for successful conduct of anti-submarine warfare (ASW) must be maintained; otherwise, they will quickly atrophy," Vego warns. The Navy has done a better job spending money on technology that can locate submarines. During the Cold War, permanent networks of sensors on the sea floor helped keep tabs on Soviet submarines. Similar networks have not been established or upgraded for use in new hotspots. "Undersea surveillance systems developed during the Cold War have limited effectiveness today," Vego says. It appears the South Koreans share that lethargy, but South Korean officials now say a permanent snooping system will be installed. South Korean Lt. Gen. Park Jung-e said at a media briefing that "our plan is to reinforce submarine measures by establishing a submarine detection system in areas that are vulnerable." The United States is also fielding a deployable piece of underwater detection technology, called the Advanced Deployable System (ADS) that is built for shallow-water emergencies. The system proposes to use expendable, battery-powered passive acoustic arrays that are connected with fiberoptic cables. The system will be integrated into the Navy's much-delayed but recently commissioned Littoral Combat Ship.

StarTribune.com | MINNEAPOLIS - ST. PAUL, MINNESOTA

Editorial: Terrorism today: Threat level is high

Source: <http://www.startribune.com/opinion/editorials/95152829.html?page=2&c=y>

"I can guarantee you that we will soon be talking about Somalia as much as Yemen."


PETER NEUMANN, director of the International Centre for the Study of Radicalisation and Political Violence and a senior lecturer at King's College in London, speaking at a May 17-19 conference, "Reporting on International Security and Terrorism," in New York. The conference was organized by the Thomson Reuters Foundation, the Stanley Foundation and Gerda Henkel Stiftung.

Almost nine years after 9/11, terrorism is a fast-evolving, mostly underestimated worldwide threat, and America may be more vulnerable to attacks today than it was on that sunny September morning. That grim assessment was the consensus of experts who spoke at a recent journalism conference on terror and security issues held, fittingly, in an office tower on Times Square in New York. "Terrorists can win and have won," said Sebastian Gorka, assistant professor of irregular warfare at the College of International Security Affairs in Washington. To borrow a sports cliché, Gorka's warning can best be summarized this way:

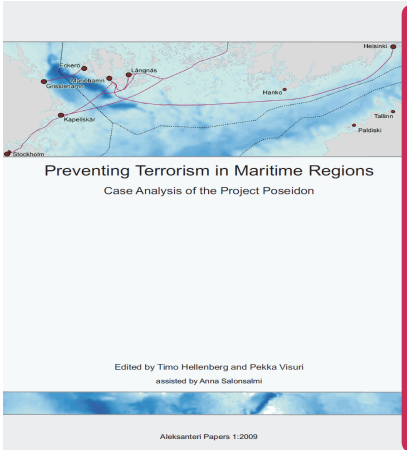
We can't stop acts of terror, we can only hope to contain them. To that end, counterterrorism today is a complex exercise in risk management. The tactics of terror have morphed since 9/11. Terrorists are using the Internet, including social media, to develop worldwide networks based on personal relationships rather than traditional chain-of-command hierarchies. In many cases, it's impossible for law enforcement officials to draw a leadership diagram or come up with a geographical frame of reference for a terrorist organization, said Peter Neumann, director of the International Centre for the Study of Radicalisation and Political Violence and a senior lecturer at King's College in London. Terrorists of today are also trying to kill more people with their attacks and create widespread fear by targeting civilians. Often their aims are less negotiable, Neumann said, in contrast with groups such as the IRA that had clear political goals. The panelists assembled in New York listed myriad types of current threats, from suicide bombing to nuclear weapons and cyberterrorism. **One security expert described how an attack using the radioactive material from an X-ray machine in a veterinary clinic could shut down Times Square for months. Another said there is growing concern that terrorists will hack into medical devices or records. One especially chilling scenario: A terror network hacks into a large hospital database and changes patient drug prescription data.** The growing number of weak and failed states around the world provides an expanding breeding ground for terror, and Somalia is at or near the top of the list. That should not be shocking to Minnesotans, who have read news reports of as many as 20 young Somali-American men from the state being recruited by the terrorist group Al-Shabaab in the past two years to return to fight in Somalia's civil war. Five of them have died, including one who killed others in a suicide attack. A sixth man, a Muslim convert from Minneapolis, also is believed to have been killed in Somalia. Neumann said the apparent radicalization of the 20 men while still in the United States has drawn the attention of a concerned Department of Homeland Security. And federal officials told the Star Tribune last year that the threat of homegrown attacks in the United States -- such as the failed May 1 Times Square plot -- is increasing. The United States and its allies appear to have weakened Al-Qaida, but other affiliated and independent networks such as Al-Shabaab are growing more active and dangerous, according to several of the expert panelists. For Minnesotans, especially those in the local Somali community and law enforcement officials throughout the state and federal government, that's a chilling reminder that the **lessons learned on 9/11 must not be forgotten as we grapple with a new set of threats today.**

Project Aether

Source: <http://www.helsinki.fi/aether/project/index.html>



The logo for Project Aether features the word "AETHER" in a large, stylized, serif font with a metallic texture, set against a background of a cloudy sky. To the left of this is the logo of the University of Helsinki, which consists of a stylized bird or leaf shape with the text "UNIVERSITY OF HELSINKI" below it.



A map of the Baltic Sea region showing major cities and shipping routes. The map is titled "Preventing Terrorism in Maritime Regions Case Analysis of the Project Poseidon". It includes a red vertical bar on the right side. Below the map, it is edited by Timo Hellenberg and Pekka Visuri, assisted by Anna Salomaa. The map shows cities like Stockholm, Helsinki, Tallinn, and others, with shipping routes indicated by red lines.

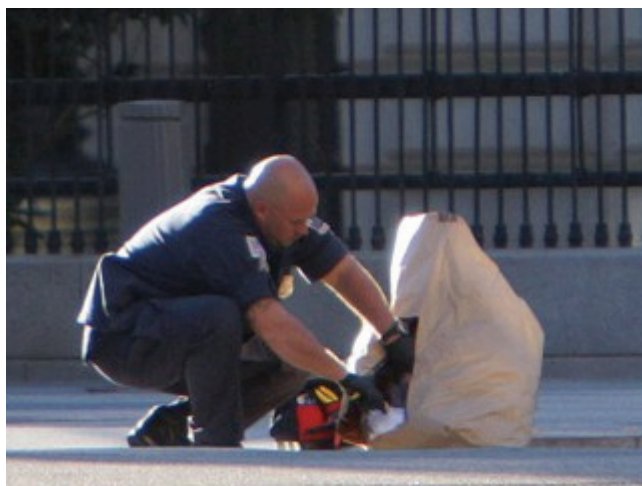
The aim of the "Project Aether – Air passenger transport security in the case of CBRN threat by terrorists" is to investigate situation awareness and decision making at the European Union level in the case of a complex CBRN (chemical, biological, radiological, nuclear) threat-related crisis situation on board an airplane. The project also seeks to identify the prevention capacity against the use of CBRN material. These aims shall be achieved through a careful analysis and simulation of an open-ended scenario with several development lines. The Project started in the beginning of April, 2009, and lasts for two years. It is funded by the European Commission Directorate-General Justice, Freedom and Security under the Programme for "Prevention of and

Fight against Crime”. The Aether project is a continuation project for the former Aleksanteri Institute led project “**Poseidon – Preventing Terrorism in the Baltic Sea Region**”. Two exercises (Table Top and Livex) will be organised within the project in Finland in October 2010. Both the state authorities and private operators will participate in the exercises. Each project partner will produce 2-3 working papers that will also support the organisation of two project exercises involving state authorities. The Aether project publication will be released at the Brussels conference in February 2011.

Jihadi Calls For 'Suspicious Bags' To Be Left Throughout DC and NYC

Source: <http://abcnews.go.com/Blotter/jihadi-calls-suspicious-bags-left-dc-nyc/story?id=10826590>

A recent internal FBI report warns federal, state and local authorities to be alert for a potential new tool in the jihadi terror arsenal the placing of suspicious, but harmless, bags in public places to inspire fear, disrupt public transportation and tie up police and bomb squads. The so



called "battle of suspicious bags" was encouraged by an unknown poster to a known jihadi website. On May 12th, the poster suggested an "invasions suspicious bags (sic)" in "the heart of Washington and New York," as the FBI's Washington Field Office Intelligence Division noted in its May 27th "Situational Information Report." The bags would contain not bombs, but innocuous items, a tactic that has been used by other political extremists in the U.S. in the recent past. "The stated goal of the campaign," said the report, "was to exploit desensitization of first

responders caused by response fatigue to suspicious, but harmless items." The FBI report did not include the full text of the jihadi forum post, but said "the poster suggested packing bags with innocuous items and placing them in public areas has the capability to occupy response assets and disrupt public infrastructure and transportation." The poster's credibility was not known, according to the FBI, but the site where the information was posted was listed as a "known jihadi web site." The information had also been shared among numerous law enforcement agencies in advance of the bulletin's circulation. The jihadi posting came within two weeks after an attempted car bombing in Times Square. The man charged in the case, Faisal Shahzad, has alleged link to Islamic fundamentalists overseas. So far, no evidence of any "suspicious bag" campaign has been found in either Washington or New York. In New York, there was a spike in calls to police about suspicious packages in the immediate aftermath of the May 1 Times Square bombing attempt, law enforcement officials said. During the week right after the failed attack there were 140 calls a day to the New York City Police Department of suspicious packages, compared with 90 per day in the week prior to the attack. The NYPD Bomb Squad was called out in force to investigate several items, including a cooler, a pizza box and a car with propane tanks in its back seat. Each incident, however, was unrelated to the others, and showed no signs of being



part of an organized campaign, officials said. Authorities told ABC that they were familiar with the tactic of sowing fear with suspicious bags, and there were telltale signs that could help them establish whether such a campaign was underway. Anarchists have used the tactic in the U.S. with some success, at venues such as the 2000 Philadelphia Republican Convention, where hoax bomb knapsacks including some with messages were left at or near the convention. The threat of another such campaign was also investigated prior to the Republican Convention in New York in 2004 and authorities trained for a variety of potential responses. The FBI's Washington Field Office included the information on the jihadi posting in what has become an annual event -- the circulation of a report reminding authorities that "Summer Tourist Season Increases the Potential for Terrorist Threats." "Washington DC and the National Capital Region (NCR) remain primary targets for Extremists, particularly during the summer tourist season, " this year's report states. The possibility of a suspicious bag campaign was at the top of a list of "indicators to assist in detecting potential terrorist activity." The FBI's Washington Field Office declined to discuss the issues raised in the "Situational Information Report. The FBI in New York, meanwhile, said it provides situational awareness training specifically geared towards helping patrol officers and others to determine when an bag or other object might be suspicious. Said Special Agent Richard Kolko, spokesman for the FBI's New York Field Office, "Our Bomb Techs recently had a training class for FBI personnel from New York and several other field offices to educate them on how to identify suspicious packages, or routine items in order to help recognize what may or may not be potentially dangerous. This helps cut down on the calls for items that just don't warrant sending out the bomb squad and provides the agents on the street additional situational awareness as they go about their daily duties." Kolko noted that this training class was not related to the Washington Field Office report or to the jihadi posting.

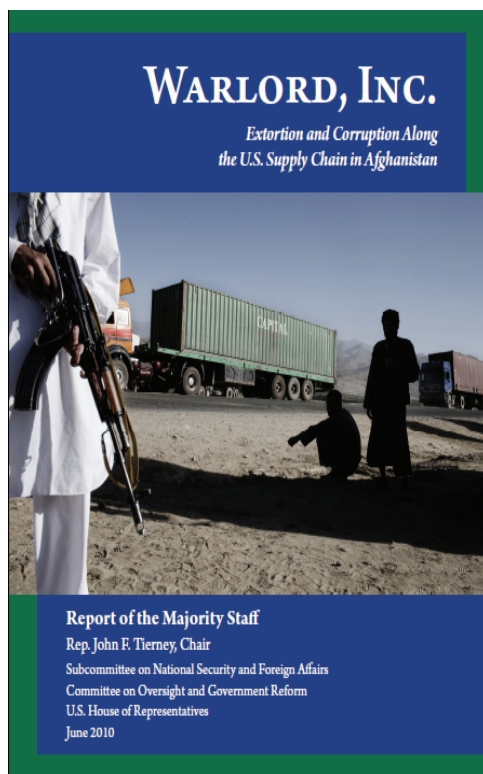
Army testing green laser kits in Afghanistan

Source: <http://www.army.mil/-news/2010/06/02/40214-army-testing-green-laser-kits-in-afghanistan/>



The Army's Green Light Escalation of Force, or GLEF system, is being tested in Afghanistan to assist Soldiers by giving them an interim step before escalating force. The Army's Program Executive Office Soldier is fielding several Green Laser Escalation of Force, or GLEF, kits to units in Afghanistan for operational assessment. The GLEF systems are mounted as an accessory to Common Remotely Operated Weapon Stations or CROWS, the turret system

that provides Soldiers the ability to employ cameras, sensors and weapons from inside the protection of an armored vehicle. The non-lethal green-light laser gives Soldiers an interim step before escalating force while conducting daily operations. "Protecting civilian populations is critical to our success in fighting insurgencies," said Col. Douglas Tamilio, project manager for Soldier Weapons. "Green lasers have proven safe and effective as a non-lethal tool that sends a strong message without the need to employ deadly force." The GLEF system emits a wide band of green light that temporarily disrupts a person's vision so that driving a vehicle or aiming a weapon becomes difficult if not impossible. One application would be to warn civilians away from checkpoints and other areas where their safety is at risk. At closer distances, the lasers provide an immediate, nonlethal capability to deter aggressive actions. "The human eye is four times more sensitive to green light than to red light during the day and far more sensitive at night," explained Maj. Michael Pottratz, program manager for Crew Served Weapons. "The effect is the same as looking at the sun for a fraction of a second. The lasers send a warning signal across language and cultural barriers to keep innocent people from entering into harm's way." While green lasers have been commercially available for a number of years, the system configuration for use as a CROWS accessory is a new development. By employing previously tested and approved technologies, engineers were able to design, assemble and field the new configuration for use in CROWS systems in less than 12 months. Select units will test the systems for 90 days and report back to PEO Soldier on system performance and its impact on operations. Soldier input will be incorporated into the final designs.



Warlord, Inc

Source:

http://www.cbsnews.com/htdocs/pdf/HNT_Report.pdf

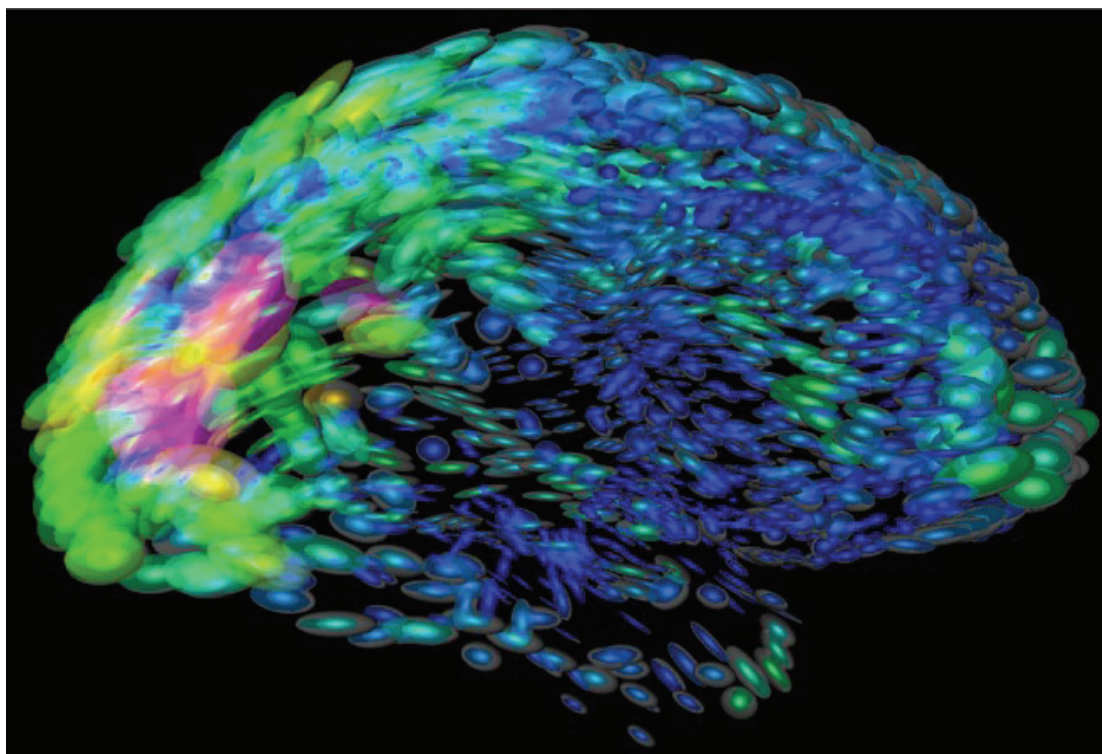
A very interesting report on what is going on in Afghanistan!

“American taxpayers have inadvertently created a network of warlords across Afghanistan who are making millions of dollars escorting NATO convoys and operating outside the control of either the Afghan government or the American and NATO militaries, according to the results of a Congressional investigation released Monday,” reports the *Times*.

Pentagon Turns to Brain Implants to Repair Damaged Minds

Source: <http://www.wired.com/dangerroom/category/darpawatch/>

An estimated 10 to 20 percent of troops coming home from Iraq and Afghanistan are



suffering from traumatic brain injuries, or TBIs, which afflict 1.7 million Americans each year. Now the Pentagon's rolling out a revolutionary initiative to treat the condition: brain implants that one researcher likens to "replacement parts" for damaged gray matter. "When something happens to the brain right now, there's so little that the medical community can do," Krishna Shenoy, associate professor of electrical engineering and bioengineering at Stanford University, told Danger Room. "Our goal is to understand — and then be able to change — how a brain responds to trauma." No surprise that military extreme science agency Darpa is behind the project, which is called [REPAIR](#), or Reorganization and Plasticity to Accelerate Injury Recovery. Yesterday, they announced an initial two-year round of \$14.9 million in funding for four institutions, led by Stanford and Brown universities, that will collaborate on the brain-chip project. All in, it'll involve 10 professors and their research teams, working in neuroscience, psychiatry, brain modeling and even semiconductors. Significant progress has already been made in understanding brain injury. Scientists can create conceptual, mathematical models of brain activity, and are also able to record the electrical pulses emitted by individual neurons in the brain, which offers insight into how those neurons communicate. That knowledge has spurred rapid progress in neural-assisted prosthetic devices, a program that Shenoy collaborated on with Geoffrey Ling, the same Darpa program manager behind REPAIR. But what experts can't yet do, Shenoy said, is alter those electrical pulses to turn brain circuits on or off. His team will use optogenetics, an emerging technique that involves emitting light pulses to precisely trigger neural activity, to develop an implanted TBI treatment device. "Before this, emitting light into the brain would be like hitting it with a hammer," Shenoy said. "What we're doing now is pin-pointing a single neuron, and that neuron will naturally change its activity depending on the cue." The implants developed by the project will likely be composed of electrodes or optical fibers, and will sit on the surface of the brain. They'll read electrical signals from neurons, and deliver appropriate light pulses to stimulate other brain regions in response. The implants would allow the brain to operate normally, by acting as substitutes for areas that were damaged or

“unavailable.” First up for Shenoy and company are optogenetic tests on mice, rats and eventually monkeys, to better understand how different regions of the brain interact. For example, how one area of the brain knows which signals to send to other parts. Once they’ve got that down, the researchers hope to develop chips that essentially mimic those interactions, so that an implant can “read a signal from region A, bypass damaged area B, and get that signal to C,” Shenoy said. And while Darpa’s interested in ailing vets, the implants could have broad civilian application, including help for those who’ve suffered a stroke or undergone surgery to remove a brain tumor. If all goes according to plan, Shenoy expects implants for lab animals within four years.

Watching for Watchers

Source: http://www.stratfor.com/weekly/20100616_watching_watchers

By *Scott Stewart*

Situational awareness inevitably leads to the question: “What in the world am I looking for?” The brief answer is: “warning signs of criminal or terrorist behavior.” Since this brief answer is very vague, it becomes necessary to describe the behavior in more detail.

Surveillance

It is important to make one fundamental point clear up front. The operational behavior that most commonly exposes a person planning a criminal or terrorist act to scrutiny by the intended target is surveillance. Other portions of the planning process can be conducted elsewhere, especially in the age of the Internet, when so much information is available online. From an operational standpoint, however, there simply is no substitute for having eyes on the potential target. In military terms, surveillance is often called reconnaissance, and in a criminal context it is often referred to as casing or scoping out. Environmental activist and animal rights groups trained by the Ruckus Society refer to it as “scouting.” No matter what terminology is being used for the activity, it is meant to accomplish the same objective: assessing a potential target for value, vulnerabilities and potential security measures. Surveillance is required so that criminals can conduct a cost-benefit analysis. The amount of time devoted to the criminal surveillance process will vary, depending on the type of crime and the type of criminal involved. A criminal who operates like an ambush predator, such as a purse-snatcher, may lie in wait for a suitable target to come within striking distance. This is akin to a crocodile lying in a watering hole waiting for an animal to come and get a drink. The criminal will have only a few seconds to size up the potential target and conduct the cost-benefit calculation before formulating his plan, getting ready and striking. On the other extreme are the criminals who behave more like stalking predators. Such a criminal is like a lion on the savannah that carefully looks over the herd and selects a vulnerable animal believed to be the easiest to take down. A criminal who operates like a stalking predator, such as a kidnapper or terrorist, may select a suitable target and then take days or even weeks to follow the target, assess its vulnerabilities and determine if the potential take is worth the risk. Normally, stalking criminals will prey only on targets they feel are vulnerable and can be successfully hit, although they will occasionally take bigger risks on high-value targets. Of course, there are many other criminals who fall somewhere in the middle, and they may take anywhere from a few minute to several hours to watch a potential target. Regardless of the time spent observing the target, all criminals will conduct this surveillance and they are vulnerable to detection during this time. Given that surveillance is so widely practiced, it is quite amazing to consider that, in general, criminals and terrorists are terrible at conducting surveillance. There are some exceptions, such as the relatively sophisticated surveillance performed by Greenpeace and some of the other groups trained by the Ruckus Society, or the low-key and highly detailed surveillance performed by some high-end art and jewelry thieves, but such surveillance is the exception rather than the rule. The term “tradecraft” is an espionage term that refers to techniques and procedures used in the field, but term also implies quite a bit of finesse in the practice of these techniques. Tradecraft, then, is really more of an art rather than a science, and surveillance tradecraft is no exception. Like playing the violin or fencing with a foil, it takes time and practice to become a skilled surveillance practitioner. Most individuals involved in criminal and terrorist activity simply do not devote

the time necessary to master this skill. Because of this, they have terrible technique, use sloppy procedures and lack finesse when they are watching people. Although everybody planning a criminal or terrorist attack conducts preoperational surveillance, that does not necessarily mean they are good at it. The simple truth is that these individuals are able to get by with such a poor level of surveillance tradecraft because most victims simply are not looking for them. And this is where we tie the discussion back into last week's Security Weekly. Most people do not practice situational awareness. For those who do, the poor surveillance tradecraft exhibited by criminals is good news. It gives them time to avoid an immediate threat and contact the authorities.

Demeanor Is the Key

The behavior a person needs to outwardly display in order to master the art of surveillance tradecraft is called good demeanor. Good demeanor is not intuitive. In fact, the things one has to do to maintain good demeanor frequently run counter to human nature. Because of this, intelligence and security professionals who work surveillance operations receive extensive training that includes many hours of heavily critiqued practical exercises, often followed by field training with a team of experienced surveillance professionals. This training teaches and reinforces good demeanor. Criminals and terrorists do not receive this type of training and, as a result, bad surveillance tradecraft has long proved to be an Achilles' heel for terrorist and criminal organizations. Surveillance is an unnatural activity, and a person doing it must deal with strong feelings of self-consciousness and of being out of place. People conducting surveillance frequently suffer from what is called "burn syndrome," the erroneous belief that the people they are watching have spotted them. Feeling "burned" will cause surveillants to do unnatural things, such as suddenly ducking back into a doorway or turning around abruptly when they unexpectedly come face to face with the target. People inexperienced in the art of surveillance find it difficult to control this natural reaction. Even experienced surveillance operatives occasionally have the feeling of being burned; the difference is they have received a lot of training and they are better able to control their reaction and work through it. They are able to maintain a normal looking demeanor while their insides are screaming that the person they are surveilling has seen them. In addition to doing something unnatural or stupid when feeling burned, another very common mistake made by amateurs when conducting surveillance is the failure to get into proper "character" for the job or, when in character, appearing in places or carrying out activities that are incongruent with the character's "costume." The terms used to describe these role-playing aspects of surveillance are "cover for status" and "cover for action." Cover for status is a person's purported identity — his costume. A person can pretend to be a student, a businessman, a repairman, etc. Cover for action explains why the person is doing what he or she is doing — why that guy has been standing on that street corner for half an hour. The purpose of using good cover for action and cover for status is to make the presence of the person conducting the surveillance look routine and normal. When done right, the surveillance operative fits in with the mental snapshot subconsciously taken by the target as the target goes about his or her business. Inexperienced people who conduct surveillance frequently do not use good cover for action or cover for status, and they can be easily detected. An example of bad cover for status would be someone dressed as "a businessman" walking in the woods or at the beach. An example of bad cover for action is someone pretending to be sitting at a bus stop who remains at that bus stop even when several buses have passed. But mostly, malefactors conducting surveillance practice little or no cover for action or cover for status. They just lurk and look totally out of place. There is no apparent reason for them to be where they are and doing what they are doing. In addition to "plain old lurking," other giveaways include a person moving when the target moves, communicating when the target moves, avoiding eye contact with the target, making sudden turns or stops, or even using hand signals to communicate with other members of a surveillance team or criminal gang. Surveillants also can tip off the person they are watching by entering or leaving a building immediately after the person they are watching or simply by running in street clothes. Sometimes, people who are experiencing the burn syndrome exhibit almost imperceptible behaviors that the target can sense more than observe. It may not be something that can be articulated, but the target just gets the gut feeling that there is something wrong or odd about the way a certain person behaves. Innocent bystanders who are not watching someone usually do not exhibit this behavior or trigger these feelings. The U.S. government often uses the acronym "TEDD" to illustrate the principles that can be used to identify surveillance conducted by counterintelligence agencies, but these same principles also can be used to identify criminal and

terrorist surveillance. TEDD stands for time, environment, distance and demeanor. In other words, if a person sees someone repeatedly over time, in different environments and over distance, or someone who displays poor surveillance demeanor, then that person can assume he or she is under surveillance. If a person is being specifically targeted for a planned attack, he or she might be exposed to the time, environment and distance elements of TEDD, but if the subway car the person is riding in or the building where the person works is the target, he or she might only have the demeanor of the attacker to key on because the attacker will not be seen by the observer over time and distance or in different environments. Time, environment and distance are also not applicable in cases involving criminals who behave like ambush predators. Therefore, when we are talking about criminal surveillance, demeanor is the most critical of the four elements. Demeanor will also often work in tandem with the other elements, and poor demeanor will often help the target spot the surveillant at different times and places. In a situation where a building or subway car is targeted for an attack rather than a specific person, there are still a number of demeanor indicators (people wearing unseasonable warm clothing, such as trench coats, people with protruding bulges under their clothing, people who are sweating, mumbling, or fidgeting, people who are trying to avoid security personnel or young people who appear to be out of place in a certain venue) that can be observed just prior to the attack. Such indicators include people wearing unseasonable clothing in warm weather (such as trench coats); people with odd bulges under their clothing or wires sticking out from their clothing; people who are sweating profusely, mumbling or fidgeting; people who appear to be attempting to avoid security personnel; and people who simply appear to be out of place. According to many reports, suicide attackers will often exhibit an intense stare as they approach the final stage of their attack plan. While not every person exhibiting such behavior is a suicide bomber or shooter, avoiding such a person rarely has much of a downside. One technique that can be helpful in looking for people conducting long-term surveillance is to identify places that provide optimal visibility of a critical place the surveillant would want to watch (for example, the front door of a potential target's residence or office). These optimal observation points are often referred to as "perches" in surveillance jargon. Perches can then be watched for signs of hostile surveillance like people who don't belong there, people making demeanor mistakes, etc. This principle can also be extended to critical points along frequently and predictably traveled routes. Potential targets can conduct simple pattern and route analyses to determine where along the route they are most predictable and vulnerable. Route analysis looks for vulnerabilities, or choke points, on a particular route of travel. Choke points have two main characteristics: They are places where the potential target must travel and where rapid forward motion is difficult (such as sharp, blind curves). When a choke point provides a place where hostiles can wait with impunity for their victims and have access to a rapid escape route, the choke point becomes a potential attack site. These characteristics are found in attack sites used by highly professional kidnap/assassination teams and by criminal "ambush predators" such as carjackers. While the ideal tactic is to vary routes and times to avoid predictable locations, this is also difficult and disruptive and is warranted only when the threat is high. A more practical alternative is for potential targets to raise their situational awareness a notch as they travel through such areas at predictable times in order to be on the alert for potential hostile surveillance or signs of an impending attack. The fact that operatives conducting surveillance over an extended period of time can change their clothing and wear hats, wigs or other light disguises — and use different vehicles or license plates — also demonstrates why watching for mistakes in demeanor is critical. Of course, the use of disguises is also an indicator that the surveillants are more advanced and therefore potentially more dangerous. Because of a surveillant's ability to make superficial changes in appearance, it is important to focus on the things that cannot be changed as easily as clothing or hair, such as a person's facial features, build, mannerisms and gait. Additionally, while a surveillant can change the license plate on a car, it is not as easy to alter other aspects of the vehicle such as body damage (scratches and dents). Paying attention to small details can produce significant results over time. As we noted last week — and it is worth repeating here — paying attention to details and practicing situational awareness does not mean being paranoid or obsessively concerned about security. When people live in a state of paranoia, looking for a criminal behind every bush, they become mentally and physically exhausted. Not only is this dangerous to one's physical and mental health, but security also suffers because it is very hard to be aware of your surroundings when you are exhausted. Therefore, while it is important to watch for the watchers, watching should not involve feelings of fear or

paranoia. Knowing what is occurring in the world around them empowers people and gives them a sense of security and well-being, allowing them to spot the good things in life as well as the potential dangers.

"This report is republished with permission of [STRATFOR](#)"

CBRNE-TERRORISM Newsletter

Δελτίο ΧΒΡΠΕ-ΤΡΟΜΟΚΡΑΤΙΑΣ

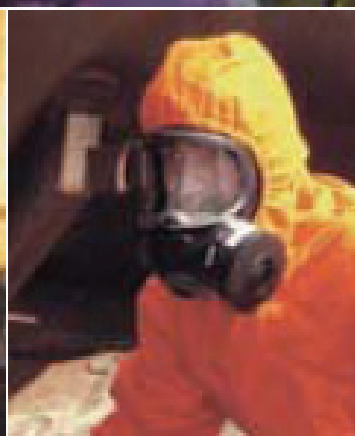
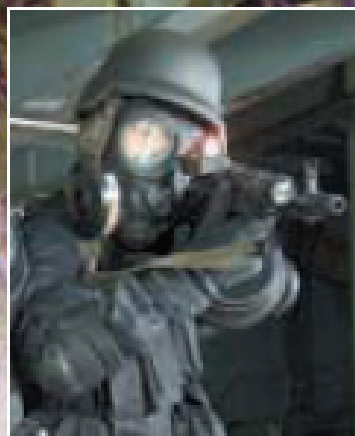
Volume 3 - 2010

A large, intense explosion is the central focus of the image, with bright orange and yellow flames and a thick plume of white smoke rising from the ground. In the background, a white truck is visible, partially obscured by the smoke and fire. The truck has a red stripe along its side and some equipment on its roof. The overall scene is chaotic and depicts a major incident.

NEW Events

SCOTT[®]

RESPIRATORY
PROTECTION



Solutions for Military Applications

Scott are specialists in the design and manufacture of respiratory protection equipment. They supply military customers with self contained breathing apparatus, escape sets, airline breathing equipment and air purifying filters and masks across the globe. A comprehensive range of powered air purifying respirators for Civil Defence applications is also part of the Scott portfolio. Scott are at the cutting edge of respiratory protection technology, developing new products, providing the highest levels of protection meeting latest operational requirements and standards. Visit www.scottsafety.com for details.

SCOTT
HEALTH & SAFETY

United Kingdom

Tel: +44 (0)1605 711711
Email: scott.sales.uk@tycotint.com

Finland

Tel: +358 (0)6 3244 543 and -544
Email: scott.sales.fi@tycotint.com

www.scotthealthsafety.com

New Upcoming Events



(July 22-23; Osage Beach, MO) The conference will bring together experts and professionals to consider and discuss effective violence prevention and other intervention strategies to reduce risk to human life when emergencies occur. This year's conference will focus on suicide prevention and emotional wellness issues for both the educational and first responder communities. [View event website](#)



HARVARD SCHOOL OF PUBLIC HEALTH
CENTER FOR CONTINUING PROFESSIONAL EDUCATION
Where theory informs practice and practice informs theory®

Radiological Emergency Planning: Terrorism, Security, and Communication (August 16-20; Boston) This conference will examine the latest requirements for responding to a radiological emergency and respond to changes under way from both government and industry, as emergency planners and emergency response team members face a host of new challenges in an era of unprecedented public scrutiny. [View event website](#)



(August 23-25; Indianapolis) This risk assessment conference is for geographic information system specialists, emergency managers, geologists, state and local planners, and the like. It will include educational sessions, hands-on training, and networking opportunities. [View event website](#)



(August 24-28; Chicago) Fire-Rescue International offers executive education and brings together chief officers from across the United States and around the world to exchange ideas, learn from experts, and see the latest equipment, products, and services for emergency responders. At this year's conference it will launch the Battalion Chief program. [View event website](#)

Centre for International Studies

Dublin City University

Terrorism and New Media: Building a Research Network (September 8-9; Dublin, Ireland) This conference will bring together academics from a broad range of disciplines with policy makers and security practitioners who have knowledge and/or expertise that can facilitate advances in the study of terrorism and new media, particularly the Internet, in novel ways. [View event website](#)



Asia-Oceania Resilience Conference (October 5-6; Singapore) This conference will bring together, for the first time in Asia, security, emergency management, crisis management, business continuity management, risk management, disaster recovery, and disaster relief professionals from 29 countries eager to learn about products and services that support all aspects of corporate and community resilience. [View event website](#)



National Sports Safety and Security Conference (August 2-4, 2010): For the first time in the United States, a National Sports Safety and Security Conference and Exhibition will be held, focusing solely on the sports safety and security industry. The gathering of top professionals in the field will provide a wholesome environment dedicated to security/safety technologies, products, services, and education for safeguarding the assets and spectators we are charged to protect. The conference theme is "Balancing Safety, Security, and Spectator Experience." Exhibitors, sponsors and attendees are guaranteed to meet a wide range of sports venue owners, operators, managers, security staff, first-responders, government agency representatives, architects, planners, educators, trainers, and league/association officials. (<http://www.usm.edu/sportheventsecurity/conference.php>)



THE UNIVERSITY OF SOUTHERN MISSISSIPPI
 NATIONAL CENTER FOR
 SPECTATOR SPORTS
 SAFETY AND SECURITY

ΔΕΝ ΣΕ ΞΕΧΑΣΑΜΕ !



~~~~~