

June 2015

# CBRNE NEWSLETTER TERRORISM

E-Journal for CBRNE & CT First Responders



10 years

*terrorism*

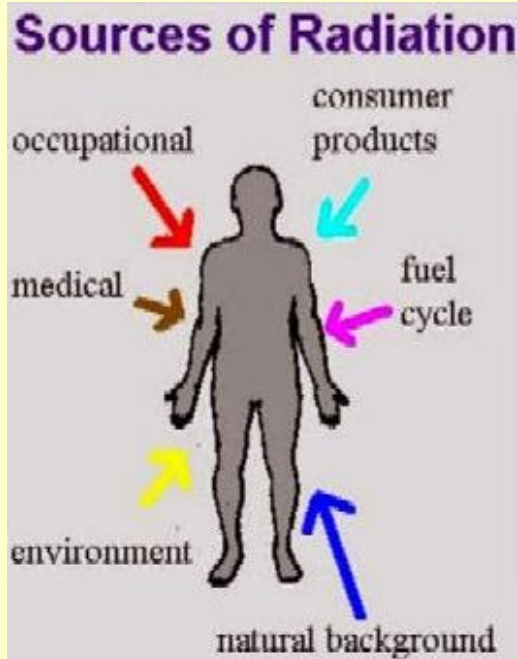


[www.cbrne-terrorism-newsletter.com](http://www.cbrne-terrorism-newsletter.com)

## First drug approved for radiation treatment

Source: <http://thedailyjournalist.com/scientia/first-drug-approved-for-radiation-treatment/>

As a result of research performed by scientists at the University of Maryland School of Medicine (UM SOM), the U.S. Food and Drug Administration has approved the use of a drug to treat the deleterious effects of radiation exposure following a nuclear incident. **The drug, Neupogen®, is the first ever approved for the treatment of acute radiation injury.**



The research was done by Thomas J. MacVittie, PhD, professor, and Ann M. Farese, MA, MS, assistant professor, both in the University of Maryland School of Medicine (UM SOM) Department of Radiation Oncology's Division of Translational Radiation Sciences. The investigators did their research in a non-human clinical model of high-dose radiation.

"Our research shows that this drug works to increase survival by protecting blood cells," said Dr. MacVittie, who is considered one of the nation's leading experts on radiation research. "That is a significant advancement, because the drug can now be used as a safe and effective treatment for the blood cell effects of severe radiation poisoning."

Radiation damages the bone marrow, and as a result decreases production of infection-fighting white blood cells. Neupogen® counteracts these effects. The drug, which is made by Amgen, Inc., was first approved in 1991 to treat cancer patients receiving chemotherapy. Although doctors may use it "off label" for other

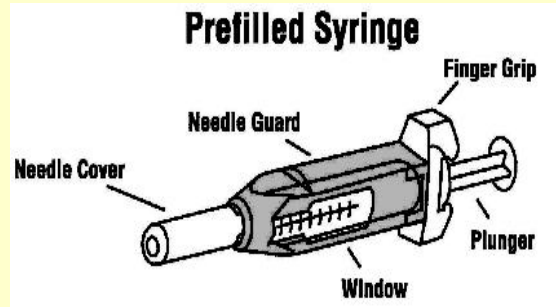
indications, the research and the resulting approval would speed up access to and use of the drug in the event of a nuclear incident.

This planning is already under way. In 2013, the Biomedical Advanced Research and Development Authority (BARDA), an arm of the Department of Health and Human Services, bought \$157 million worth of Neupogen® for stockpiles around the country in case of nuclear accident or attack.

Neupogen® is one of several "dual-use" drugs that are being examined for their potential use as countermeasures in nuclear incidents. These drugs have everyday medical uses, but also may be helpful in treating radiation-related illness in nuclear events. Dr. MacVittie and Ms. Farese are continuing their research on other dual-use countermeasures to radiation. They are now focusing on remedies for other aspects of



2



radiation injury, including problems with the gastrointestinal tract and the lungs.

The research builds on 40 years of work that Dr. MacVittie and his team have conducted in the field of radiation research, during which they have helped to define the field. The Neupogen study is also part of a broad portfolio of research being conducted by faculty in the Department of Radiation Oncology. Among these are Minesh Mehta, MD, the medical director of the Maryland Proton Treatment Center, who is focusing on research into thoracic oncology, neuro-oncology, integrating imaging advances with radiation therapy, and innovative applications of new radiation therapy technologies to test biological concepts.



Another researcher in the department is Zeljko Vujaskovic, MD, PhD, director of the Division of Translational Radiation Sciences; he is doing research on identifying potential biomarkers predicting individual patient risk for injury, and to develop novel therapeutic interventions/strategies to prevent, mitigate, or treat radiation injury.

“In terms of both research and treatment, our department is leading the way in developing the most effective discovery-based clinical applications to help protect and heal patients,” says William F. Regine, MD, professor and Isadore & Fannie Schneider Foxman Endowed Chair in Radiation Oncology at the UM SOM.

He added that research has served as the foundation for the Department of Radiation Oncology’s recent development of four clinical modalities for the treatment of cancer through radiation:

Proton Treatment, a precise approach to cancer, which targets tumors while minimizing harm to surrounding tissues. Proton treatment uses protons traveling at about two-thirds the speed of light to precisely deliver beams of radiation to the tumor. This treatment will be

available in the new 110,000 sq ft Maryland Proton Treatment Center before the end of the year;

Selective Internal Radiation Therapy, a precision modality for treating patients with particularly difficult to remove tumors involving the liver such as those from colorectal cancers; Gammapod, a new, high-precision, noninvasive method of treating early-stage breast cancer;

Thermal Therapies, the use of “heat” in treating a broad spectrum of malignancies.

“The Department of Radiation Oncology’s work is just one example of how the School of Medicine is discovering innovative ways to repurpose existing drugs that are able fight a broader array of critical diseases,” said Dean E. Albert Reece, MD, PhD, MBA, who is also the vice president for Medical Affairs, University of Maryland, and the John Z. and Akiko K. Bowers Distinguished Professor and Dean of the School of Medicine. “We are particularly proud of the Neupogen research as it is not only important scientifically; it is crucial for our country’s public health and its national security.”

## **New reactor design recycles nuclear waste**

Source: <http://www.homelandsecuritynewswire.com/dr20150529-new-reactor-design-recycles-nuclear-waste>

An advanced nuclear reactor under development by Hitachi could help solve the nuclear waste problem, and University of Michigan researchers were involved in verifying its safe performance through computer simulations.

The U-M team worked with colleagues at the Massachusetts Institute of Technology and the University of California, Berkeley. After more safety analysis, Hitachi plans to move forward with a prototype of the “resource-renewable boiling water reactor” in the next few years.

One of the major technological hurdles for nuclear energy is developing systems to dispose of the waste produced by typical reactors. It must be sealed away for hundreds of millennia while the radioactivity naturally decreases.

**A U-M release reports that Hitachi’s new design would burn off the longest-lived radioactive materials, called transuranics, shortening that isolation period to a few centuries. This would recycle the nuclear**

**waste to produce yet more energy and reduce the amount that must be stowed away.**

“Because of transuranics, we’re talking about lifetimes for storing fuel that we can’t even fathom,” said Thomas Downar, U-M professor of nuclear engineering and radiological sciences. “You get this down to a hundred years, then you’re talking about the ability to engineer a container that you have confidence will last that long.”

In the conventional boiling water reactors that currently produce about 30 percent of all the nuclear-generated electricity in the U.S., the neutrons that split uranium atoms have been slowed by the boiling water. In contrast, the Hitachi design uses fast neutrons since they are more likely to split, or fission, transuranic atoms.

Prototype fast reactors have been running since the 1970s, but they use a sodium coolant. Sodium burns when it comes into contact with air and reacts



violently with water. This is one of the reasons why U.S. utilities that operate reactors have been hesitant to consider sodium-cooled designs.

A water-cooled fast reactor, though, could offer safer and more familiar operation. The challenge was designing a water-cooled core that would stop itself if it started overheating and the water turned to steam. In conventional reactors, the water's slowing action acts as a failsafe because steam is less effective at decelerating neutrons. Since fewer neutrons are at the right speed to cause fissions, the reaction rate slows down too.

The simulation of the reactor core confirms that the dead zones allow the reactor to operate safely. This image shows where atoms split, or fission. The fuel rods run vertically, with the red, high-fission fuel regions and blue, low-fission dead zones. Credit: Seker et al, University of Michigan

For a boiling water reactor that's burning transuranics, this scenario is trickier. The faster neutrons could mean a faster fission rate, creating more heat, steam and fast neutrons.

"If something goes wrong and the power increases, you want to have the fission rate

decrease," Downar said.

To create this safety feature in their reactor, Hitachi engineers plan large dead zones in the fuel rods, made of materials with a much lower probability of fissioning with fast neutrons. Hitachi calculated that as the presence of steam reduced the density of the water, fast neutrons were likely to travel further. By keeping the active regions of the fuel assembly small, more neutrons would be lost to these "blanket" regions in an overheating scenario, slowing the fission rate.

Before beginning the expensive process of prototyping, Hitachi wanted to confirm with outside experts that the design would perform as expected.

The release notes that with funding from the Department of Energy, members of Downar's group spent the last three years developing codes that could simulate the more complex layout and physics of Hitachi's reactor core design. For example, uranium fission reactions are reasonably steady and easy to predict, but transuranic reactions are irregular and difficult to calculate accurately.

The U-M team developed a method to generate data that simulates the way transuranics burn. They then applied this data to established codes currently used for boiling water reactor analysis. By looking at what happened when the steam bubbles appeared, the team found that the fast neutrons tended to leave the reactive part of the fuel assembly, slowing the reaction rate as planned.

Now, the university teams are about to begin a careful comparison of their methods with the predictions from the Hitachi computer codes to discover any differences in the simulation of the advanced reactor's performance. Hitachi will fund the teams at U-M, MIT and Berkeley for the next phases of the project.

## France will not sign off on a nuclear deal with Iran if military sites are off limits to inspectors

Source: <http://www.homelandsecuritynewswire.com/dr20150529-france-will-not-sign-off-on-a-nuclear-deal-with-iran-if-military-sites-are-off-limits-to-inspectors>

Laurent Fabius, France's foreign minister, said France will not accept a deal on Iran's nuclear program if Tehran refuses to allow inspections of its military sites as part of the final agreement. Throughout the negotiations with Iran, France has taken a

tougher stance toward Iran than the other negotiating countries, known as the P5 + 1 (the five permanent members of the Security Council – the United States, United Kingdom, Russia, China, and France – and Germany).



"France will not accept a deal if it is not clear that inspections can be done at all Iranian installations, including military sites," Fabius told the national assembly in Paris on Wednesday, urging other negotiating partners to adopt a similar position.

The *Guardian* notes that Fabius's comments came a week after Iran's supreme leader, ayatollah Ali Khamenei, insisted he would not allow the Iranian negotiating team to accept inspections of military sites or questioning of the country's nuclear scientists.

"We have already said that we will not allow any inspections of military sites by foreigners," the ayatollah said last week. "They also say that we must allow interviews with nuclear scientists. This is interrogation. I will not allow foreigners to come and talk to scientists who have advanced the science to this level."

Fabius said: "Yes to an agreement, but not to an agreement that will enable Iran to have the atomic bomb. That is the position of France, which is independent and peaceful."

Talks resumed in the Austrian capital, Vienna, on Wednesday for addressing the remaining issues concerning the final agreement, which

was initially expected to be reached by the end of June, but diplomats have since said that the self-imposed deadline could be extended.

"We are not bound by time, but we are committed to this issue that a good agreement with details that are favorable to us is hammered out, even if it may take a long time," said Abbas Araqchi, a senior Iranian negotiator, according to the Iranian state-run Press TV.

The French ambassador to the United States, Gérard Araud, tweeted on Tuesday: "Our goal is to get an agreement by the deadline. Likely that Iran will wait for the last days for compromising, like in March."

Yukiya Amano, the head of the International Atomic Energy Agency (IAEA), said the additional protocol of the Nuclear Non-Proliferation Treaty (NPT) that Iran has agreed to implement would give the IAEA the right to request inspections of all nuclear facilities, including military sites.

Earlier this week, Araqchi was quoted by journalists to have said that his country was prepared to grant "managed access" to military sites, but denied that statement later.

## A Combination of Pre- and Post-Exposure Ascorbic Acid Rescues Mice from Radiation-Induced Lethal Gastrointestinal Damage

By Yasutoshi Ito,<sup>1</sup> Manabu Kinoshita,<sup>2,\*</sup> Tetsuo Yamamoto,<sup>1</sup> Tomohito Sato,<sup>1</sup> Takeyuki Obara,<sup>1</sup> Daizoh Saitoh,<sup>3</sup> Shuhji Seki,<sup>2</sup> and Yukihiro Takahashi<sup>1</sup>

<sup>1</sup>Military Medicine Research Unit, Test and Evaluation Command, Ground Self-Defense Force, Setagaya, Tokyo, Japan;

<sup>2</sup>Department of Immunology and Microbiology, National Defense Medical College, Tokorozawa, Saitama, Japan;

<sup>3</sup>Division of Traumatology, Research Institute, National Defense Medical College, Tokorozawa, Saitama, Japan.

*Int J Mol Sci.* 2013 Oct; 14(10): 19618–19635.

Source: <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3821576/>

### Abstract

The development of an effective therapy for radiation-induced gastrointestinal damage is important, because it is currently a major complication of treatment and there are few effective therapies available. Although we have recently demonstrated that pretreatment with ascorbic acid attenuates lethal gastrointestinal damage in irradiated mice, more than half of mice eventually died, thus indicating that better approach was needed. We then investigated a more effective therapy for radiation-induced gastrointestinal damage. Mice receiving abdominal radiation at 13 Gy were orally administered ascorbic acid (250 mg/kg/day) for three days before radiation (pretreatment), one shot of engulfment (250 mg/kg) at 8 h before radiation, or were administered the agent for seven days after radiation (post-treatment). None of the control mice survived the abdominal radiation at 13 Gy due to severe gastrointestinal damage (without bone marrow damage). Neither pretreatment with ascorbic acid (20% survival), engulfment (20%), nor post-treatment (0%) was effective in irradiated mice. However, combination therapy using ascorbic acid, including pretreatment, engulfment and post-treatment, rescued all of the mice from lethal abdominal radiation, and was accompanied by



remarkable improvements in the gastrointestinal damage (100% survival). Omitting post-treatment from the combination therapy with ascorbic acid markedly reduced the mouse survival (20% survival), suggesting the importance of post-treatment with ascorbic acid. Combination therapy with ascorbic acid may be a potent therapeutic tool for radiation-induced gastrointestinal damage.

► Read the full paper at source's URL.

## Nuclear Fuel Cost Calculator

Source: <http://thebulletin.org/nuclear-fuel-cycle-cost-calculator>

This tool allows users to calculate the economic costs of nuclear power using a wide range of variables. It is meant to assist leaders and citizens from around the world as they make policy decisions about nuclear technology and fuel cycles. It is based on an economic model developed by University of Chicago professor (and *Bulletin* Science and Security Board member) Robert Rosner, with assistance from former colleagues at Argonne National Laboratory, researchers Sam Olofin and Jeremy Klavans, and support from the MacArthur Foundation.



## Dabiq: ISIS Could Transport Nuke from Nigeria into U.S. Through Mexico

Source: <http://www.breitbart.com/national-security/2015/06/03/dabiq-isis-could-transport-nuke-from-nigeria-into-u-s-through-mexico/>

**June 03 – The Islamic State (ISIS/ISIL), in the latest edition of its propaganda magazine, indicated that it could purchase a nuclear weapon in Pakistan, take it to Nigeria, and then smuggle it into the U.S. through Mexico by using existing trafficking networks in Latin America.**

In an op-ed article published in the ninth edition of ISIS' *Dabiq* magazine released in late May, the jihadist group claims it could transport a nuclear device in the same way illicit drugs are smuggled into Europe through West Africa, adding that Boko Haram's presence in Nigeria could facilitate the transaction (pp.74-77).

The Nigeria-based Islamic terrorist group, Boko Haram, pledged allegiance to ISIS in March.

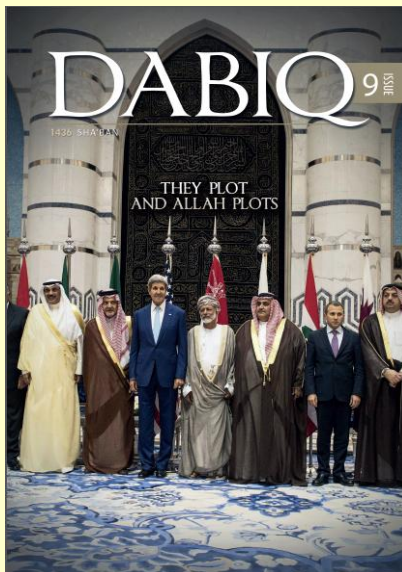
In March, Gen. John Kelly, commander of U.S. Southern Command (Southcom), warned that Islamic terrorist groups such as ISIS could exploit the

capabilities and knowledge of Latin American smuggling networks to infiltrate the U.S. through Mexico and possibly bring in weapons of mass destruction.

The general, in October 2014, acknowledged that illegal drugs from South America move "through West Africa, up the Maghreb and into Western Europe," adding that ISIS enemy al Qaeda and its affiliates take "a lot of money to allow it to flow."

According to the alleged author of the *Dabiq* op-ed article, kidnapped British photojournalist John Cantlie, ISIS could smuggle a nuke into the U.S. by using the same route and reversing the flow— moving the nuke from West Africa into South America, from where it could be transported into the United States through Mexico.

"Let me throw a hypothetical operation onto the table," Cantlie wrote in the article entitled "The Perfect Storm."



“The Islamic State has billions of dollars in the bank, so they call on their wilāyah [province] in Pakistan to purchase a nuclear device through weapons dealers with links to corrupt officials in the region.” He added:

The weapon is then transported over land until it makes it to Libya, where the mujāhidīn [fighters] move it south to Nigeria. Drug shipments from Columbia bound for Europe pass through West Africa, so moving other types of contraband from East to West is just as possible. The nuke and accompanying mujāhidīn arrive on the shorelines of South America and are transported through the porous borders of Central America before arriving in Mexico and up to the border with the United States.

“From there it’s just a quick hop through a smuggling tunnel and hey presto, they’re mingling with another 12 million ‘illegal’ aliens in America with a nuclear bomb in the trunk of their car,” he also wrote.

If not a nuke, ISIS could easily smuggle in “a few thousand tons of ammonium nitrate explosive” that is easy to manufacture, said the article.

Cantlie wrote that ISIS, which started as a movement in Iraq, has suddenly morphed into a global phenomenon that the West and the democratic world as a whole is ill-prepared to handle.

He said that Boko Haram controls most of Nigeria, home to “an exhausted and smashed national army that is now in a virtual state of collapse”.

While testifying before the Senate Armed Services Committee in March, Gen. Kelly noted, “Last year, ISIS adherents posted discussions on social media calling for the infiltration of the U.S. southern border. Thankfully, we have not yet seen evidence of this occurring, but I am deeply concerned that smuggling networks are a vulnerability that terrorists could seek to exploit.”

**“While there is not yet any indication that the criminal networks involved in human and drug trafficking are interested in supporting the efforts of terrorist groups, these networks could unwittingly, or even wittingly, facilitate the movement of terrorist operatives or weapons of mass destruction toward our borders, potentially undetected and almost completely unrestricted,”** he added.

The general, speaking at the National Defense University in Washington, D.C. in October 2014, warned that Latin American drug cartels were working with jihadist groups in West Africa, namely Sunni group Al Qaeda in the Islamic Maghreb and its affiliates.

**The Iranian terrorist threat**

Source: <http://www.terrorism-info.org.il/en/article/20787>

**Overview**

1. On February 26, 2015, US Director of National Intelligence (DNI) James R. Clapper presented the members of the Senate Armed Services Committee with the Worldwide Threat Assessment of the US Intelligence Community.
2. The Threat Assessment for 2015 was presented at a time when the United States heads an international coalition leading an attack against ISIS in Syria and Iraq. Indeed, in the Threat Assessment for 2015, emphasis is clearly placed on the American campaign against Sunni-jihadi terrorism (whose most prominent representatives are ISIS and Al-Qaeda). Conversely, the head of the DNI does not mention the threat of Shiite terrorism, including the challenges of terrorism from Iran and Hezbollah. In this context, Hezbollah is not mentioned (apart from a single reference,

- stating that it supports the Lebanese Army against the “leakage” of Sunni terrorism from Syria). Iran itself is mentioned in other contexts as a country that constitutes a substantial and diverse challenge (cyber, espionage, arms control) while engaging in its nuclear program.
3. The lack of references to the threat of Iranian and Shiite terrorism contradicts previous publications by US government agencies (the Intelligence Community and the State Department) in 2014, which stated that Iran and Hezbollah continued to directly challenge the interests of US allies and that Hezbollah had increased its global terrorist activity in recent years to a level not seen since the 1990s (see Appendix A).
4. In the ITIC’s assessment, the lack of reference to the Shiite terrorist threat, and Iran and Hezbollah as its



generators, is not accidental. The ITIC believes that this is due to a combination of political considerations (the US dialogue with Iran over the nuclear agreement) and the idea that Iran and Hezbollah may be of assistance in the campaign against ISIS in Syria and Iraq and possibly in other countries (Iran is mentioned together with the United States, the West and the Arab countries as confronting ISIS). Under these circumstances, the US prefers to downplay Iran's use of the "terrorist weapon" (including the massive support that it provides to Hezbollah and its use of the latter to advance its own strategic goals in the face of Israel and the entire region).

5. It should be noted that in contrast to the review by the head of the DNI, the Qods Force and Hezbollah do appear on the DIA's list of terrorist threats, although it seems they are mentioned in the report in rather weak terms. In the list of global threats<sup>[1]</sup> presented to Congress by DIA Director Vincent R. Stewart (February 3, 2015), Iran and Hezbollah are mentioned on the list of terrorist threats. The chapter "Terrorism" is devoted primarily to Al-Qaeda and ISIS, while Iran and Hezbollah are mentioned laconically:

"Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF) and Lebanese Hizballah are

instruments of Iran's foreign policy and its ability to project power in Iraq, Syria, and beyond. Hizballah continues to support the regime of Syrian President Assad, pro-regime militants and Iraqi Shia militants in Syria..."

6. In practice, Iran remains a country that sponsors terrorism and perceives terrorism and subversion as a main tool for promoting its policy and its interests in the Middle East. The Iranian regime, by means of the Qods Force, an elite unit of the Revolutionary Guards, allocates significant resources in the form of money, high-caliber manpower and weapons to support terrorist organizations in the Middle East, the most prominent of which is Hezbollah. Past experience has proved that acts of terrorism and subversion promoted by Iran are not limited only to the Middle East, but are carried out in many countries around the world. In the ITIC's assessment, as Iran's self-confidence grows, especially if it feels that it has made achievements with the United States in the negotiations over its nuclear program, it is liable to increase the scope of its support to terrorism and its daring use of terrorism and subversion in the Middle East and around the world.

<sup>[1]</sup>Worldwide Threat Assessment, February 3, 2015, DIA website.

## Israel conducted tests to assess the impact of dirty bombs

Source: <http://www.homelandsecuritynewswire.com/dr20150609-israel-conducted-tests-to-assess-the-impact-of-dirty-bombs>

June 09 – **Between 2010 and 2014, Israeli scientists at the Dimona nuclear reactor conducted a series of experiments, under the code name "Green Field," to examine the consequences of a dirty-bomb explosion in Israel.** The purpose of the experiments was defensive – to measure the likely effect of a dirty bomb and evaluate countermeasures. The experiments did not evaluate to offensive potential of a dirty bomb. In the experiments, scientists **detonated twenty explosive charges weighing between a quarter of kilogram and twenty-five kilograms, mixed with the radioactive material technetium-99m, which is widely used in medical imaging.** The experiments

employed Dimona's most advanced technologies, including micro-UAVs to measure radiation and sensors to measure the explosive yield.

*Haaretz* reports that most of the test explosions were done in the Negev desert, and that one of the explosions was conducted in an enclosure.

**Scientists found that intense radiation could be detected at the core of the explosion, and that wind-carried radioactive particles would carry low-level radiation to the surrounding area. The scientists concluded that the most serious impact of a dirty bomb is the**





psychological impact on the population. If the dirty bomb exploded in an enclosed area, that area would have to be closed for a long time to be decontaminated.

As part of the project, an experiment called "Red House" was meant to examine a scenario of radiological material being placed in a crowded location, but without exploding it. Radioactive material, diluted in water, was placed in the ventilation system of a two-story building. The experiment

showed that this is not an effective way of spreading the material inside the building, as most of it was stopped by the air-conditioning filters.

The newspaper notes that after the 9/11 terrorist attacks in the United States, Israel began preparations for dealing with a possible dirty-bomb explosion. In 2006 the Israel Ministry of Health issued instructions on the steps which had to be taken in the event of a radiological attack.

**EDITOR'S COMMENT:** It would be great to have the details published one day!

## Multi-Mode Passive Detection System (MMPDS)

Source: <http://www.decisionsciencescorp.com/about-us/mmpds/>

Decision Sciences' *Multi-Mode Passive Detection System (MMPDS)* combines technology invented by top government scientists at Los Alamos National Laboratory with considerable private sector investment and expertise, to deliver totally safe, effective and reliable automated scanning to speedily detect both shielded and unshielded nuclear and radiological threats.

Additional modality enables explosive and contraband detection. Harnessing the natural occurrence of muons in the atmosphere, Decision Sciences' MMPDS tracks muons through even heavily shielded materials and computes a 3-D image of what is being scanned. In combination with a gamma radiation detector, MMPDS



can scan a typical 40-foot shipping container in 45 seconds, on average, providing accurate and safe scanning while facilitating the flow of commerce. The MMPDS technology produces no ionizing radiation, meaning it is completely safe for people, animals, plants and food. MMPDS modular construction enables the system to be scaled up or down to scan any type of vehicle, rail cars and cargo containers.



MMPDS satisfies the 100% scanning requirement recommended by the US 9/11 Commission and later adopted by the U.S. Congress.

With near-zero false alarms, the MMPDS promises to improve the safety, effectiveness and efficiency of cargo scanning operations around the globe while providing the global transportation industry with a cargo scanning solution that is accurate, efficient, safe, modular and cost-effective.



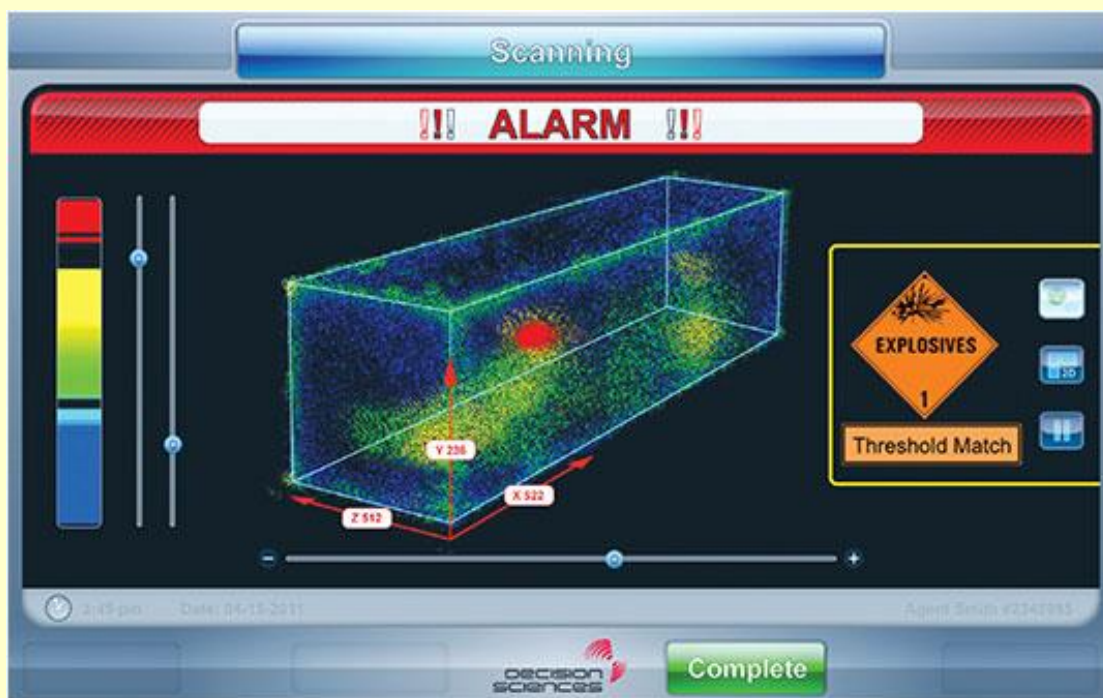
**Technology Advancements**

Decision Sciences continues to expand the capabilities of its original scanner. Through the addition of latent gamma-ray technology, the company has already increased the efficiency and effectiveness of the detector.

**Applications**

Decision Sciences' MMPDS is ideally suited for seamless integration into critical infrastructure, ports, borders, and air and rail operations around the globe where there is an ever-growing need for efficient, accurate detection and deterrence of nuclear terrorist threats. Designed to be embedded within existing infrastructure or as a stand-alone application, Decision Sciences' MMPDS can easily be scaled to fit a wide variety of applications.

It is easy to operate and makes scanning and locating threats very simple. An operator only need look at MMPDS display screen to see where, in 3-D, a threat has been located.



**Key Technology**

A key driver behind the success of Decision Sciences' MMPDS is a technology called muon tomography. Muons are naturally occurring cosmic ray-induced particles that continuously rain down from the Earth's upper atmosphere, harmlessly penetrating everything they touch. Decision Sciences' MMPDS tracks these muons, detecting and recording their deflection signatures with advanced proprietary software and algorithms as they pass through an object within the MMPDS

**Israel Experiments With A Weapon Of Mass Disruption**

Source: <http://www.forbes.com/sites/jamesconca/2015/06/12/israel-experiments-with-dirty-bombs-and-radiation/>

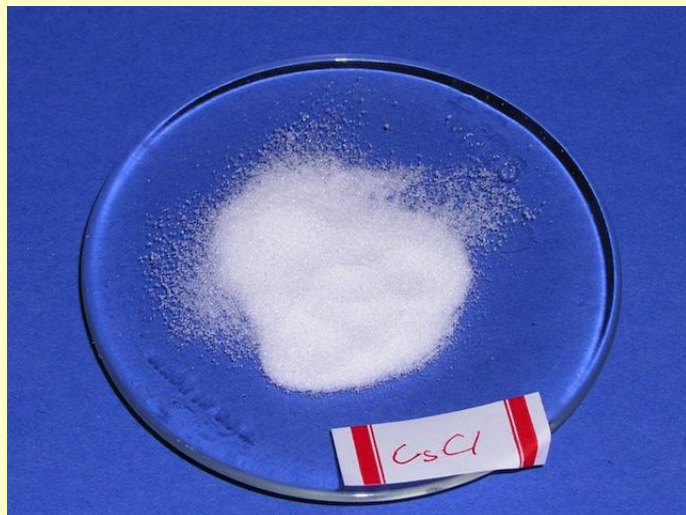
June 12 – The Haaretz just reported that Israel performed a four-year dirty bomb project with radioactive material to determine the effectiveness of a dirty bomb attack and how to defend against one. The conclusion was such an attack would be ineffective and that they don't pose a substantial danger beyond the conventional blast and the psychological effect.

The United States did detailed studies of dirty bombs years ago, and came to the same conclusion. Sandia National Laboratory did a majority of this work (Musolino and Harper, 2006), in conjunction with New Mexico Tech's Energetic Materials Research and Testing Center, and Los Alamos National Laboratory (Conca and



Reynolds, 2006), but an extensive amount of work has been done by DHS, universities, DOE and all of our national laboratories.

A dirty bomb, or radiation dispersal device (RDD), uses a conventional bomb, such as a car bomb, to disperse radioactive materials in a populated or financial district to cause great economic and social disruption disproportionate to their actual radiological



with the medical isotope <sup>99m</sup>Tc. Tiny drones and special sensors were used to measure radiation and the force of the blast.

After the blasts, high-level radiation was measured at the center of the explosions, with only low levels of wind-dispersed radiation measured beyond ground zero, showing that the radiation aspect of such an attack would be ineffective.

<sup>137</sup>CsCl powder, presently used in the irradiation industry, is the terrorist's dirty bomb material of choice. <sup>137</sup>Cs is inexpensive (<\$3/Ci) and emits a hard gamma ray at 0.66 MeV requiring about 18 cm of lead or three feet of concrete to fully shield. It has a high specific activity (87 Ci/g) so the amount filling a coffee can (~ 5.5 lbs or 2.5 kg) will make a super RDD of over 200,000 Ci. The powdered form makes dispersal easy and its 30-year half-life means it will be a problem for over 200 years if not cleaned up quickly. In the environment, CsCl dissolves easily into Cs+ and Cl-, and behaves like KCl (salt substitute). Photo by J. Wischnewsky

effects and well beyond the physical destruction from their conventional bomb components.

Termed Weapons of Mass Disruption by Sig Hecker, a dirty bomb is a psychological weapon, not a nuclear weapon.

Research has shown that only those close enough to be hurt or killed by the car bomb itself, or other explosive device, would get a significant radiation dose. Few people, if any, would die from the radiation from a dirty bomb, even a big one, although tens to hundreds could die from the conventional blast.

But it would scare everyone. The panic and bureaucratic confusion would most likely prevent the correct and timely response, driving clean-up costs upwards of several hundred billion dollars if detonated in an area like Manhattan.

**The only scientifically-correct depiction of a dirty bomb attack was BBC/HBO's 2004 film Dirty War, a required viewing in our dirty bomb response classes for police, fire and military personnel.**

The Israeli tests involved conventional explosives laced with radioactive material that were detonated mostly in the desert, although one was performed at a closed facility. Twenty detonations were carried out involving between 0.250 and 25 kilograms of explosives together

Radioactive materials are used in many fields in almost all countries around the world, particularly for research, medical, and industrial applications. Dozens of radiological source producers and suppliers are found on six continents, and about a billion sources exist worldwide. Most, like household smoke detectors, have such low activities that they pose no threat.

The rise in the number of terrorist acts since 2001 has raised concerns about these radiological sources being used in RDDs. Because the general public is so frightened about anything radioactive, panic must be anticipated even if there is no real health threat from the radioactive component. The Department of Homeland Security is particularly concerned about the degenerate case of a phantom RDD, where no radioactive material is used but an implication or anonymous tip indicates there is. This could still cause considerable panic with large economic consequences.

There have only been two attempted dirty bomb attacks in history, both by Chechens against Russia about ten years ago. One failed and the other was foiled.

Although many variables determine the effectiveness of an RDD attack, the key factors are the quantity, type and



amount of radiation emitted, and its chemical form (whether it is a powder, a non-metal solid or metal). Gamma radiation can penetrate great distances and, depending upon the energies, requires shielding of about 18 cm of lead or 3-feet of reinforced concrete. Beta radiation can only penetrate a short distance and the personal protective gear of a firefighter can block much of the dose. Alpha radiation is the least penetrating of all and can be stopped by a piece of paper or ordinary clothing.

#### For RDD discussions, isotopes of

- Pu, Am and U are primarily alpha emitters
- <sup>60</sup>Co and <sup>137</sup>Cs are gamma emitters
- <sup>90</sup>Sr is a beta emitter
- <sup>60</sup>Co usually occurs as a metal (either pellets or small rods)
- <sup>137</sup>Cs comes as a powder
- <sup>90</sup>Sr is as a ceramic
- Pu, Am and U are various oxides and non-metal solids.

Although the public generally thinks of Pu and enriched-U when hearing the word radioactive, these are not effective RDD materials because they are primarily alpha emitters, are costly, cannot be obtained in large amounts, are well-tracked and secured, and are more useful to terrorists in the production of an actual nuclear weapon than being wasted in an RDD. Spent nuclear fuel is also a useless material for dirty bombs since it is impossible to disperse.

In this sense, <sup>137</sup>CsCl powder is by far the most effective RDD material and the only terrorist's material of choice. It is easy to get, cheap (less than a few dollars a Ci), is an easily dispersible powder, and emits a hard gamma.

Fortunately, dirty bombs have an inherently self-regulating feature. The greater the dispersal, the more people affected, but the lesser the dose.

As an example, a 25-gram <sup>137</sup>CsCl source (about 2,200 Ci) is lethal after about 1 hour of exposure at 1 meter (dose ~ 1,000 rem/hr or 10 Sv/hr). However, it is not lethal if spread over the one-billion square feet of surface area in 10 by 10 city blocks (dose < 1 rem/yr or 10 mSv/yr). This is the area of a large downtown metropolis covered by a good-sized car bomb. Once an attack has happened, the only effective option that is readily available is simply to wash-down the entire area with fire-hydrant water. Not just a little water – a real deluge. <sup>137</sup>CsCl is so soluble that it can be completely washed off of surfaces with water.

However, the wash down must be done quickly and completely, within days, or even hours, of the event, to preclude further effects such as diffusion into building materials, secondary migration, and cumulative dose effects.

Diffusion rates into materials like concrete are primarily a function of moisture content and will depend strongly upon weather conditions and porosity of the materials. If the weather remains dry and sunny, little diffusion will occur, but the material can be re-aerosolized and move elsewhere. But if the surfaces become wet (not enough to wash off the Cs), or if surfaces are wet during deposition, then significant diffusion into the concrete can occur quickly.

On a wet surface, Cs can diffuse into many concretes more than a quarter of an inch per week. If that were allowed to happen, the clean-up costs would be quite large. Cs would hardly diffuse at all into granite, glass or metal even after several years, no matter what the conditions.

There is considerable debate over the wash down approach, but it is unlikely any other strategy can be implemented rapidly enough to be effective. One hundred fire hydrants operating for 24 hours delivers about one hundred million gallons of water, sufficient to wash off even a billion square feet. And would wash most of the Cs into the stormwater drainage system where it will be sufficiently diluted to almost background levels. Remember, a large source is only a few pounds of radioactive material.

As to the people in the affected area, all persons should be evacuated and non-essential personnel excluded thereafter. Expect self-evacuation for large affected populations of uninjured persons (thousands to tens of thousands) and provide them with safe designated routes out of the affected area. **NO ONE SHOULD ATTEMPT mass decontamination of large populations, like you've seen in movies. It's unnecessary and would result in riots.**

Instead, advise people who are not injured from the blast to go home, remove and bag external clothing before entering their residences, shower with warm water and soap, and do not use hair conditioner, hair color, or other fixative hygiene products. After emergency response is over, attempt to survey bagged clothing of those

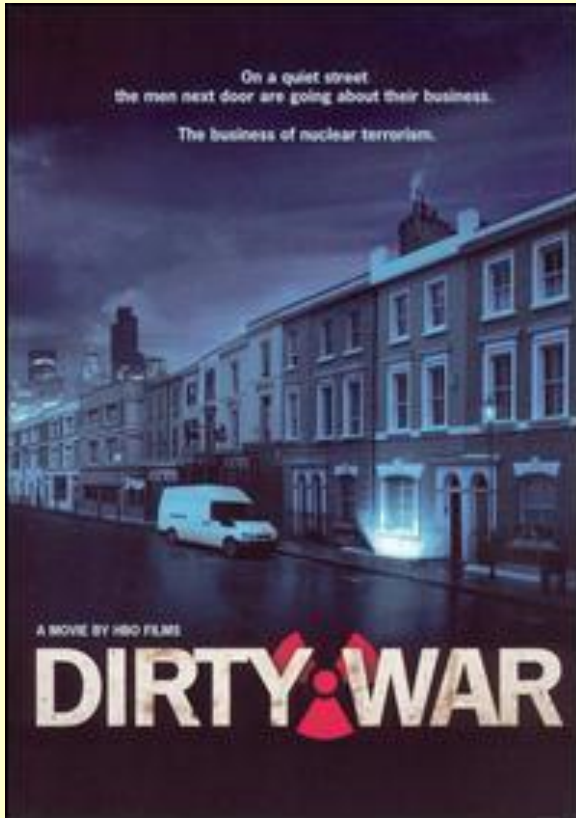


persons who think they were contaminated. Although people who are not hurt by the initial blast are unlikely to be significantly contaminated, our irrational fear of low levels of

radiation makes panic the real weapon in a dirty bomb attack.

**I encourage you to watch the film Dirty War, and let me know what you think they did wrong!**

*Dirty War* is a 2004 BBC, in association with HBO Films, made-for-TV movie thriller/drama about a terrorist attack on Central London, written by Lizzie Mickery and Daniel Percival. It was originally broadcast on BBC One on September 24, 2004, on HBO on January 24, 2005, and the first time on American broadcast television on PBS on February 23, 2005. It won a BAFTA Award for Best New Director (Fiction), Daniel Percival.



**Plot**

The film opens with a June 2003 quote from Eliza Manningham-Buller, the director general (DG) of MI5: "It will only be a matter of time before a crude chemical, biological, or radiological (CBRN) attack is launched on a major western city" and provides the basic premise for the film.

The film follows the journey of radioactive material, hidden in vegetable oil containers, from Habiller, Turkey, which is approximately 210 kilometres (130 mi) west of Istanbul, through Sofia, Bulgaria, onwards to Deptford, then to an East End Indian food takeaway restaurant, and finally to a rented house in Willesden, where the radioactive material and other components are assembled into a dirty bomb.

When the bomb goes off in the heart of London, next to the entrance to Liverpool Street Underground station, the city's

inadequate emergency services plans are put to an immediate test - with disturbing results for a population ill-prepared to understand or obey anti-contamination and quarantine orders.

In addition to touching upon the motivations of the Islamic extremist terrorists to conduct what they saw as a martyrdom operation, the events are shown through the eyes of three principal groups: the government, the emergency medical services, and the police.

Nicola Painswick, Minister for London, and Deputy Assistant Commissioner (DAC) John Ives (Ewan Stewart), of the Metropolitan Police Anti-Terrorist Branch, present a governmental point of view.

Watch Commander Murray Corrigan of the London Fire Brigade, and his wife Liz Corrigan, who works for the National Health Service, present two viewpoints.

Detective Sergeant (DS) Mike Drummer and Detective Constable (DC) Sameena Habibullah lead the Police investigation to catch the terrorists before the bomb is detonated. DC Habibullah, an English Muslim policewoman from Luton, who speaks Urdu, Punjabi, and Arabic, presents a unique point of view throughout the film.

**Legacy**

The film is considered an accurate portrayal of a potential radiological terrorist attack with subsequent emergency response. As such, the film has been used to train American first-responders who may be called upon to respond to similar incidents.



**EDITOR'S COMMENT:** I watched the movie again mainly because you need a movie to understand the magnitude of the consequences of release of CBRNE agents in urban environment. One important key point is at the very beginning of the movie when the Minister of London is asking one of the head officials: "How many are taking part in the drill?" "Around 60" he replied. "And how many are living/working in this building/area?" "Around a thousand" he replied... This is a movie need to be shown and analysed in all CBRNE schools and specialized units. Perhaps it is time to revise and reconsider our response plans based on what people will actually do instead on what we would like them to do! And this can be done only when planners can answer this very simple question: "What would be my reaction if I was involved in a real CBRNE incident myself". This **anthropocentric** approach might one day help save lives.

▶ The movie can be seen at: <https://www.youtube.com/watch?v=poZXRUxlaqk> (90 min).



**Isolated Zone: 3.5 square miles for 30 years...**

## RETHINKING THE UNTHINKABLE

*The Cold War began in 1945 with the use of nuclear weapons to end World War II and officially ended in December 1989 with a joint declaration in Malta by Presidents George H. W. Bush and Mikhail Gorbachev. In retrospect, excepting the regional wars in places like Korea and Vietnam, this 44-year period was remarkably stable. While many factors contributed to this stability, the contribution of nuclear weapons is undeniable.*

Nowhere is this stability more obvious than in Europe. During the 3.5 centuries before 1945, a major war had erupted in Europe every 11.9 years, and each lasted an average of 6.6 years. As the weapons for conventional war improved, each new war was more vicious and cost more in human lives than the previous one.

Source: [http://acdemocracy.org/wp-content/uploads/2014/12/NSS-december2014-rethinking\\_the\\_unthinkable.pdf](http://acdemocracy.org/wp-content/uploads/2014/12/NSS-december2014-rethinking_the_unthinkable.pdf)



## Bacteria may help clean groundwater contaminated by uranium ore processing

Source: <http://www.homelandsecuritynewswire.com/dr20150616-bacteria-may-help-clean-groundwater-contaminated-by-uranium-ore-processing>

June 16 – A strain of bacteria that “breathes” uranium may hold the key to cleaning up polluted groundwater at sites where uranium ore was processed to make nuclear weapons. A team of Rutgers University scientists and collaborators discovered the bacteria in soil at an old uranium ore mill in Rifle, Colorado, almost 200 miles west of Denver. The site is one of nine such mills in Colorado used during the heyday of nuclear weapons production. The research is part of a U.S. Department of Energy program to see if microorganisms can lock up uranium that leached into the soil years ago and now makes well water in the area unsafe to drink.

A Rutgers University release reports that the team’s discovery, published in the 13 April 2015 issue of *Public Library of Science One (PLoS One)*, **is the first known instance where scientists have found a bacterium from a common class known as betaproteobacteria that breathes uranium. This bacterium can breathe either oxygen or uranium to drive the chemical reactions that provide life-giving energy.**

“After the newly discovered bacteria interact with uranium compounds in water, the uranium becomes immobile,” said Lee Kerkhof, a professor of marine and coastal science in the School of Environmental and Biological Sciences. “It is no longer dissolved in the groundwater and therefore can’t contaminate drinking water brought to the surface.”

Kerkhof leads the Rutgers team that works with U.S. Department of Energy researchers. Breathing uranium is rather rare in the microbial world. Most examples of bacteria which can respire uranium cannot breathe oxygen but often breathe compounds based on metals — typically forms of solid iron. Scientists had previously witnessed decreasing concentrations of uranium in groundwater when iron-breathing bacteria were active, but they have yet to show that those iron-breathing bacteria were directly respiring the uranium.

While the chemical reaction that the bacteria perform on uranium is a common process known as “reduction,” or the act of accepting electrons, Kerkhof said it is still a mystery how

the reduced uranium produced by this microorganism ultimately behaves in the subsurface environment.

“It appears that they form uranium nanoparticles,” he said, but the mineralogy is still not well known and will be the subject of ongoing research.

The Rutgers team was able to isolate the uranium-breathing bacterium in the lab by recognizing that uranium in samples from the Rifle site could be toxic to microorganisms as well as humans. The researchers looked for signs of bacterial activity when they gradually added small amounts of dissolved uranium at the right concentration back to the samples



where uranium had become immobilized. Once they found the optimal uranium concentrations, they were able to isolate the novel strain.

Exactly how the strain evolved, Kerkhof said, “we are not sure.” But, he explained, bacteria have the ability to pass genes to each other. So just like bacteria pick up resistance to things like antibiotics and heavy metal toxicity, this bacterium “picked up a genetic element that’s now allowing it to detoxify uranium, to actually grow on uranium.” His research team has completed sequencing its genome to support future research into the genetic elements that allow the bacterium to grow on uranium.

What Kerkhof is optimistic about is the potential for these bacteria to mitigate the specific groundwater pollution problem in Rifle. Scientists at first expected the groundwater to flush into the Colorado River and carry the dissolved uranium with it, where it would get diluted to safer levels. But



that hasn't happened. Other potential methods of remediation, such as digging up the contaminated soil or treating it with harsh chemicals, are thought to be too expensive or hazardous.

"Biology is a way to solve this contamination problem, especially in situations like this where the radionuclides are highly diluted but still present at levels deemed hazardous," said Kerkhof. If the approach is successful, it could be considered for other sites where uranium

was processed for nuclear arsenals or power plant fuel. While the problem isn't widespread, he said there's potentially a lot of water to be concerned about. And the problem could spread beyond traditional places such as ore processing sites.

"There is depleted uranium in a lot of armor-piercing munitions," he said, "so places like the Middle East that are experiencing war could be exposed to high levels of uranium in the groundwater."

— Read more in *Nicole M. Koribanics et al., "Spatial Distribution of an Uranium-Respiring Betaproteobacterium at the Rifle, CO Field Research Site," PLOS One (13 April 2015).*

## **Dirty bomb: Just how worried should we be as ISIS seeks ultimate threat?**

**By Matthew Moran and Christopher Hobbs**

Source: <http://edition.cnn.com/2015/06/16/opinions/isis-dirty-bomb/>

June 16 – Last week, the news emerged that ISIS terrorists have reportedly obtained radioactive materials from hospitals and



research facilities captured in Iraq with a view to developing a radioactive "dirty bomb."

Unsurprisingly, the prospect of ISIS dabbling with unconventional weapons has been greeted with considerable concern. The Iraqi government has appealed to the United Nations for international help to "stave off the threat" in this regard and Australian Foreign Minister Julie Bishop recently acknowledged that NATO countries are deeply concerned by the situation.

**But what can ISIS actually do with these newly acquired radioactive materials? What is the nature of the threat?**

First off, it is important to emphasize that radioactive sources of the type acquired by ISIS cannot be used to create a nuclear bomb.

These sources are mostly used for medical research and treatments such as radiotherapy, and are completely unsuited to the development of nuclear weapons.

This said, the harmful effects of these sources, stemming from their chemical toxicity and radioactive properties, can be exploited in other ways. If inhaled or ingested, for example, these materials can be lethal. This was evidenced by the poisoning of Alexander Litvinenko in 2006, when

just a fraction of a gram of radioactive polonium proved enough to kill the former KGB officer.

Fortunately, achieving this type of internal exposure on a large scale would prove enormously challenging for a terrorist group. Consequently, attention has focused on the use of these materials by ISIS in a dirty bomb.

Combining radioactive materials with conventional explosives, this is a bomb with an edge. A dirty bomb would spread radioactive materials, contaminating the local area and any individuals in the nearby vicinity. Crucially, however, this contamination would be mostly external in nature and, if the attack was promptly identified as being radioactive, decontamination of individuals would be a relatively





straightforward process. The exposure time of anyone affected would be limited and the negative health effects mitigated.

Indeed, with a dirty bomb, members of the public are more likely to be harmed by the impact of the conventional explosives than that of the radioactive materials.

This point was borne out by a series of tests conducted over a four-year period by the Israeli Defence Forces (IDF) in the Negev Desert. As part of this project - details of which were recently published by Haaretz -- some 20 devices laced with radioactive materials were detonated and their effects observed. The IDF concluded that a dirty bomb attack poses little physical danger beyond the conventional blast. The real threat from dirty bombs lies in their psychological and economic effects -- a fact that often sees these devices described as weapons of mass disruption rather than weapons of mass destruction.

From a psychological perspective, for example, nuclear weapons are associated with death and destruction on an enormous scale, and dirty bombs benefit from association with these more sophisticated weapons simply because they incorporate radioactive materials.

There is an important distinction to be made between nuclear and radiological materials but this is often lost in media reports and commentary on these issues. In any case, a dirty bomb detonated in a major urban center would be sure to cause widespread fear and panic.

The economic costs associated with a dirty bomb would also be considerable. A 2011 Congressional Research Service report, for example, suggested that the clean-up after such an attack could figure in the billions of dollars, if detonated in a high-value area such as city center or port. Little wonder, then, that the security of radiological sources has emerged as a politically salient issue in recent years.

**Ultimately, while the thought of ISIS using dirty bombs to further its terrorist agenda is unsettling, the threat should not be exaggerated, particularly when it comes to its impact on public health. These are not the nuclear weapons that ISIS supposedly desires, and will do nothing to further the group's ambitions in this regard.**

*Matthew Moran is deputy director, and Christopher Hobbs is co-director of the the Centre for Science and Security Studies at King's College London, specializing on issues related to nuclear proliferation and security. The views expressed in this commentary are solely those of the writers.*

**EDITOR'S COMMENT:** Are the writers sure about the optimism of their conclusion in the last paragraph?

Can they simply answer this question: **"What would be my personal reaction in case I was involved in a real dirty bomb incident in my home city?"** by saying ►



## **ENEC installs second reactor vessel at Barakah**

Source: <http://www.thenational.ae/uae/enec-installs-second-reactor-vessel-at-barakah>

June 17 – The UAE completed another milestone on Wednesday in its groundbreaking nuclear power programme.

**ENEC, the Emirates Nuclear Energy Corporation, has installed the plant's second reactor vessel, which is where energy production takes place, in Barakah in the Western Region.**

The installation ceremony was attended by Sheikh Hamdan bin Zayed, the Ruler's

Representative in the Western Region, who said the UAE attached great importance to transparency in the development and operation of its nuclear programme.

"That principle is one of the main elements of national policy and I am proud to be here in Barakah today to witness the delivery of yet another safe and on-time milestone in the UAE's peaceful nuclear energy programme," Sheikh Hamdan said.



“Safe, clean and reliable nuclear energy has an important role to play in the future of our nation

“The vessel is the main component in the nuclear reactor,” he said. “It is designed to



and in the Western Region in particular. “The role of the peaceful nuclear energy programme in the Western Region is

contain the fuel assembly and coolant where the nuclear reaction takes place to produce energy. Installation of the pressure vessel



indicates the advanced stage of construction.” Experts say it the most important part of a reactor.

“The installation is very significant,” said Lady Barbara Judge, former head of the UK Atomic Energy Agency. “The reactor vessel houses all the technological parts of the reactor. “This shows that the

instrumental and will bring many benefits, from the creation of high-value job opportunities to the emergence of a sophisticated new industrial sector to support operations in Barakah.” Hamad Alkaabi, UAE Ambassador to the International Atomic Energy Agency, said the event demonstrated that the project was on track.



lessons that have been learnt around the world, especially at Barakah 1, have been well-integrated into the construction of Barakah 2, which is why the Abu Dhabi nuclear power project can be considered one of the best in the world.

"The technology, construction and the safety culture are of the highest standards."

Mohammed Al Hammadi, chief executive of Enec, said: "It is the culmination of many

During the event, Sheikh Hamdan was updated on the developments since his visit last July. This included reports on Enec's progress in construction and industrial development that supports local companies.

Sheikh Hamdan signed the base of the reactor vessel before it was lifted inside the Unit 2 reactor containment building. He also met Emirati nuclear engineers. "The UAE puts its hopes and aspirations in generations like



months of hard work and dedication from our team.

"In 2017, these reactors will begin producing



the vital electricity needed to meet the country's rapidly growing energy demands and support our continued social and economic growth."

yours, who are equipped with modern scientific knowledge," he said.

"Imparting this knowledge to the people of the UAE is the first and chief pillar of these plans, and therefore developing a workforce of scientifically and culturally qualified Emiratis is the primary concern of the UAE leadership."

**Unit 1 is now more than 73 per cent complete and expected to enter commercial operations in 2017. Unit 2 is 50 per cent complete and expected to follow in 2018, pending regulatory approval from the Federal Authority on Nuclear Regulation.**

The event was also attended by Sheikha Lubna Al Qasimi, Minister of International Cooperation and Development, and Khaldoon Al Mubarak, Chairman of the Executive Affairs Authority.



## Chinese nuclear forces, 2015

Source: <http://bos.sagepub.com/content/early/2015/06/17/0096340215591247.full>

China is the only one of the five original nuclear weapon states that is quantitatively increasing the size of its nuclear arsenal and it now is estimated to have approximately 260 warheads. The arsenal's capabilities are also increasing as older missiles are replaced with newer ones. As China assigns a growing portion of its warheads to long-range missiles, the US intelligence community predicts that by the mid-2020s the number of warheads on missiles capable of threatening the United

TYPE	NATO DESIGNATION	NUMBER OF LAUNCHERS	YEAR DEPLOYED	RANGE (KILOMETERS)	WARHEAD X YIELD (KILOTONS)	NUMBER OF WARHEADS
<b>Land-based ballistic missiles</b>						
DF-3A	CSS-2	?	1971	3,000	1 x 3,300	?
DF-4	CSS-3	~10	1980	5,500+	1 x 3,300	~10
DF-5A	CSS-4 Mod 2	~10	1981	13,000+	1 x 4,000-5,000	~10
DF-5B	CSS-4 Mod 3	~10	2015	<13,000+	3 x 200-300?	~30
DF-15	CSS-6	~100 <sup>1</sup>	1990	600	1 x ?	?
DF-21	CSS-5 Mods 1, 2	~80 <sup>2</sup>	1991	2,150	1 x 200-300	~80
DF-31	CSS-10 Mod 1	~8	2006	7,000+	1 x 200-300?	~8
DF-31A	CSS-10 Mod 2	~25	2007	11,000+	1 x 200-300?	~25
DF-41	CSS-X-20	N.A.	?	?	?	N.A.
<b>SUBTOTAL</b>		<b>~243</b>				<b>~163<sup>3</sup></b>
<b>Submarine-launched ballistic missiles<sup>4</sup></b>						
JL-1	CSS-NX-3	N.A.	1986	1,000+	1 x 200-300	N.A.
JL-2	CSS-NX-14	(48)	(2015)	7,000+	1 x 200-300?	(48)
<b>SUBTOTAL</b>		<b>(48)</b>				<b>(48)</b>
<b>Aircraft<sup>5</sup></b>						
H-6	B-6	~20	1965	3,100+	1 x bomb	~20
Fighters?	?	?	?	N.A.	1 x bomb	?
<b>Cruise missiles<sup>6</sup></b>						
DH-10	CJ-10	~250	2006?	1,500?	1 x ?	?
DH-20?	CJ-20?	?	?	?	1 x ?	?
<b>TOTAL</b>						<b>~183 (230)<sup>7</sup></b>

20

States could increase to well over 100. The nuclear warheads in the Chinese stockpile are intended for delivery mainly by land-based ballistic missile but also by aircraft and submarines. The current force has nearly 150 nuclear-capable land-based missiles, half of which are short-range and medium-range.



China has also built two types of submarine-launched ballistic missiles, one developed for a submarine no longer considered operational and the other in the final stages of development.



We estimate that China has approximately 260 nuclear warheads in its stockpile for delivery by approximately 160 land-based ballistic missiles as well as aircraft<sup>1</sup> and an emerging ballistic submarine fleet. This estimate is 10 warheads higher than last year, primarily due to additional sea-launched ballistic missiles. Each missile in the Chinese arsenal is equipped to carry a single warhead, except a small number of silo-based missiles that have been equipped to carry multiple warheads. The warheads are not mated with missiles under normal circumstances and are instead kept separate in central storage facilities.<sup>2</sup>

China is the only one of the five original nuclear weapon states that is quantitatively increasing the size of its nuclear arsenal, although the pace is slow. The arsenal's capabilities are also increasing as older missiles are replaced with newer and more capable ones. China is assigning a growing portion of its warheads to long-range missiles, and the US intelligence community predicts that by the mid-2020s China could "more than double" its number of warheads on missiles that are capable of threatening the United States to "well over 100" (Burgess, 2012: 19; US Air Force, National Air and Space Intelligence Center, 2013: 3). We estimate that China's current arsenal includes as many as 60 long-range missiles that can reach the United States, although only 45 of those can strike the continental United States.<sup>3</sup> Some Chinese missiles also have strike missions against Russia and India.

► Read the full article at source's URL.

## Of weapons programs in Iran and Israel, and the need for journalists to report on both

By Dan Drollette Jr

Source: <http://thebulletin.org/weapons-programs-iran-and-israel-and-need-journalists-report-both8410>

A country in the Middle East has a clandestine nuclear development program, involving facilities hidden in the desert. After several years, the country is on the verge of acquiring nuclear weapons, even though the United States has been using all its resources to prevent that from happening. Frantic communications fly behind the scenes, between Washington and Tel Aviv.

And where is the nuclear program located? Israel.

Although Iran's nuclear program dominates the headlines now (and did apparently have a military dimension at one time), that program has yet to produce a nuclear weapon, judging from the available public evidence. Meanwhile, the country pushing most aggressively for complete elimination of any prospect of an Iranian bomb—Israel—has an unacknowledged nuclear arsenal of its own. Although others project higher numbers, nuclear arsenal experts Hans M. Kristensen and Robert S. Norris estimate that Israel has roughly 80 warheads, built in secret.

It is noteworthy that while negotiations over limiting Iran's enrichment program have taken center stage in news coverage—and will likely dominate the headlines as a final agreement is or is not reached at the end of this month—the history of Israel's covert nuclear program draws

relatively little media attention. Israel has long maintained a policy of nuclear ambiguity, neither confirming nor directly denying that it has a nuclear deterrent, and the United States government has officially taken the same stance, prohibiting its officials from stating that Israel is a nuclear weapons country.

But as shown in the *Bulletin's* coverage over the years, the Israeli government does indeed have a robust nuclear program that began decades ago; it continues to operate outside the international nuclear nonproliferation regime to this day. This program has a convoluted history.

In a July 2013 article, nuclear proliferation scholar Leonard Weiss outlined the **Lavon Affair**, a failed 1954 Israeli covert operation against Egypt, undertaken in hopes it would destabilize the regime of Egypt's leader, Gamel Abdel Nasser. In a complicated way, the bungled effort eventually deepened the Franco-Israeli military cooperation that helped Israel create its nuclear arsenal.

The details of the Lavon Affair are complex, but essentially Israeli Military Intelligence (often known by its Hebrew abbreviation AMAN) activated a sleeper cell tasked with setting off a series of bombs in Egypt, targeted against Western and Egyptian institutions, in hopes that the attacks



could be blamed on Egyptian members of the Muslim Brotherhood or the Communist Party. AMAN apparently figured that the ensuing chaos would persuade Western governments that Nasser's relatively new regime was unstable and, therefore, unworthy of financial aid and other support.

But the best-laid schemes often go astray, and the entire Israeli operation was exposed; its members were eventually tried and convicted by an Egyptian court. This caused Israel to conduct a retaliatory military raid into Gaza that killed 39 Egyptians, upsetting Egypt still further. The Egyptians, in turn, moved closer to the sphere of the old Soviet Union, concluding an arms deal that angered American and British leaders. This led to the West's withdrawal from previously pledged support for the building of Egypt's Aswan Dam; Nasser retaliated by nationalizing the Suez Canal; and Israel, France, and Britain subsequently tried (and failed) to invade Egypt and topple Nasser. In the wake of the failed invasion, France expanded and accelerated its ongoing nuclear cooperation with Israel, which eventually helped enable the Jewish state to build nuclear weapons.

It is easy to see why the average news editor might blanch at diving into these complicated waters to give a full, warts-and-all explication of the Israeli nuclear weapons program from its earliest days. But that is no reason to fail to report about the weapons program as a fait accompli; Israel's program is as much a legitimate subject for media debate as the Iranian program—especially when Israel criticizes the proposed Iranian nuclear agreement.

Also given relatively short shrift in mainstream news coverage of Middle Eastern nuclear matters is the **NUMEC affair**, in which Israel apparently stole 100 kilograms of US bomb-grade uranium in the 1960s from a Pennsylvania nuclear fuel-processing plant. The theft was not discovered until years later, and President-elect Jimmy Carter was apparently not briefed about it until December 1976. The unexplained loss of large amounts of bomb-grade fissile material is a matter of concern, no matter what the context, but in this case it also involved a close ally—and Israel's bomb-making program could have derailed the Carter administration's Middle East peace efforts.

Similarly, there has been little coverage of documents from 1969 that were declassified a year ago; these documents show that the United States—at that moment in time—was quietly working to prevent Israel from acquiring nuclear weapons and to steer that country towards joining the Nuclear Non-Proliferation Treaty (NPT). Instead, Israel offered the United States only an ambiguous description of its plans, saying that Israel would not be the first country to introduce weapons to the Middle East, but pursued nuclear weapons in secret and declined to become a member state of the NPT. Israel still is not a member of the NPT, and its unacknowledged nuclear program angers many countries that are members. In fact, the NPT Review Conference recently collapsed without an agreement on a final document, at least partly because a group of countries wanted to begin a long-promised conference on a weapons of mass destruction-free zone in the Middle East within a set time frame, and the United States and United Kingdom—supporters of Israel, which opposed such a conference—refused to go along.

And it is surprising how little mainstream media coverage there has been about a 1987 Pentagon report, released this spring in response to a Freedom of Information Act request, that confirms that the Pentagon knew many details of Israel's nuclear program in 1987 and promptly covered them up. (A notable and praiseworthy exception to this lack of interest has been *The Nation*).

Perhaps the most concise and accessible description of the current Israeli nuclear program comes via Kristensen and Norris, who write the Nuclear Notebook column published by the *Bulletin*. “[I]t is a long-held conclusion among governments and experts,” they wrote in November 2014, “that Israel has produced a sizable stockpile of nuclear warheads (probably unassembled) designed for delivery by ballistic missiles and aircraft.” In that article, Kristensen and Norris provide a capsule description of how the Israelis were able to develop nuclear weapons while maintaining they were not “introducing” them into the Middle East—a diplomatic fiction that continues to the present day.

Kristensen and Norris estimate that Israel has a stockpile of approximately 80 nuclear warheads for delivery by two dozen missiles, a couple of squadrons of aircraft, and perhaps a small number



of sea-launched cruise missiles. “Common sense dictates that a country that has developed and produced nuclear warheads for delivery by designated delivery vehicles has, regardless of their operational status,

introduced the weapons to the region,” they wrote. “But Israeli governments have attached so many interpretations to ‘introduce’ that common sense doesn’t appear to apply.”

*Dan Drollette, Jr. is a science writer/editor and foreign correspondent who has filed stories from every continent except Antarctica. His stories have appeared in Scientific American, International Wildlife, MIT’s Technology Review, Natural History, Cosmos, Science, New Scientist, and the BBC Online, among others. He was a TEDx speaker to Frankfurt am Main, Germany, and held a Fulbright Postgraduate Traveling Fellowship to Australia—where he lived for a total of four years. For three years, he edited CERN’s on-line weekly magazine, in Geneva, Switzerland, where his office was 100 yards from the injection point of the Large Hadron Collider. Drollette is the author of “Gold Rush in the Jungle: The Race to Discover and Defend the Rarest Animals of Vietnam’s “Lost World,” published in April 2013, by Crown. He holds a BJ (Bachelor of Journalism) from the University of Missouri, and a master’s in science writing from New York University’s Science, Health and Environmental Reporting Program.*

## Radiological Weapons as Means of Attack

Anthony H. Cordesman

Source: <http://csis.org/files/media/isis/pubs/radiological%5B1%5D.pdf>

**Radiological weapons** are generally felt to be suitable largely for terror, political, and area denial purposes, rather than mass killings. Unlike nuclear weapons, they spread radioactive material contaminating personnel, equipment, facilities, and terrain. The radioactive material acts as a toxic chemical to which exposure eventually proves harmful or fatal.

**Radiation** is energy that comes from a source and travels through some material or through space. Light, heat, and sound are types of radiation. Atom-derived radiation is called ionizing radiation because it can produce charged particles (ions) in matter. Ionizing radiation is produced by unstable atoms. Unstable atoms differ from stable atoms because they have an excess of energy or mass or both. Unstable atoms are said to be radioactive. To reach stability, these atoms give off, or emit, the excess energy or mass. These emissions are called radiation. The kinds of radiation are electromagnetic (like light) and particulate (i.e., mass given off with the energy of motion). Gamma radiation and X-rays are examples of electromagnetic radiation. Beta and alpha radiation are examples of particulate radiation. Ionizing radiation can also be produced by devices such as X-ray machines.

**Three types of radiation-induced injury can occur:** external irradiation, contamination with radioactive materials, and incorporation of radioactive material into body cells, tissues, or organs. External irradiation occurs when all or part of the body is exposed to penetrating radiation from an external source. During exposure, this radiation can be absorbed by the body or it can pass completely through. A similar thing occurs during an ordinary chest x-ray. Following external exposure, an individual is not radioactive and can be treated like any other patient. External radiation does not make a person radioactive. The second type of radiation injury involves contamination with radioactive materials. Contamination means that radioactive materials in the form of gases, liquids, or solids are released into the environment and contaminate people externally, internally, or both. An external surface of the body, such as the skin, can become contaminated, and, if radioactive materials get inside the body through the lungs, gut, or wounds, the contaminant can become deposited internally. A person is externally contaminated if radioactive material is breathed in, swallowed, or absorbed through wounds. The environment is contaminated if radioactive material is spread about or uncontained. The third type of radiation injury that can occur is incorporation



of radioactive material. Incorporation refers to the uptake of radioactive materials by body cells, tissues, and target organs such as bone, liver, thyroid, or kidney. In general, radioactive materials are distributed throughout the body based upon their chemical properties. Incorporation cannot occur unless contamination has occurred.

**The three types of exposure can happen in combination and can be complicated by physical injury or illness.** In such a case, serious medical problems always have priority over concerns about radiation (such as radiation monitoring, contamination control, and decontamination). Gamma radiation is able to travel many meters in air and many centimeters in human tissue. It readily permeates most materials and is sometimes called  $\gamma$ -penetrating radiation.  $\gamma$ -Gamma rays represent the major external hazard. Radioactive materials that emit gamma radiation and X-rays constitute both an external and internal hazards to humans. Dense materials are needed for shielding from gamma radiation. Clothing and turnout gear provide little shielding from penetrating radiation. Gamma radiation is detected with survey instruments, including civil defense instruments. Low levels can be measured with a standard Geiger counter (such as the CD V-700). High levels can be measured with an ionization chamber (such as a CD V-715). Gamma radiation frequently accompanies the emission of alpha and beta radiation. Instruments designed solely for alpha detection (such as an alpha scintillation counter) will not detect gamma radiation. Pocket chamber (pencils) dosimeters, film badges, thermoluminescent, and other types of dosimeters can be used to measure accumulated exposure to gamma radiation. Beta radiation may travel meters in air and is moderately penetrating. It can penetrate human skin to the – germinal layer – where new skin cells are produced. If beta-emitting contaminants are allowed to remain on the skin for a prolonged period of time, they may cause skin injury. Beta-emitting contaminants may be harmful if deposited internally. Most beta emitters can be detected with a survey instrument (such as a CD V-700, provided the metal probe cover is open). Some, however, produce very low energy, poorly penetrating radiation that may be difficult or impossible to detect. Examples of this are carbon-14, tritium,

and sulfur-35. Beta radiation cannot be detected with an ionization chamber (such as the CD V-715). Clothing and turnout gear provide some protection against most beta radiation. Turnout gear and dry clothing can keep beta emitters off of the skin. Alpha radiation travels a very short distance through the air and is not able to penetrate the skin. Alpha-emitting materials can be harmful to humans if the materials are inhaled, swallowed, or absorbed through open wounds. A variety of instruments have been designed to measure alpha radiation. Special training in the use of these instruments, however, is essential for making accurate measurements. An ionization chamber (such as a CD V-700) cannot detect the presence of radioactive materials that produce alpha radiation unless the radioactive materials also produce beta and/or gamma radiation. Instruments cannot detect alpha radiation through even a thin layer of water, blood, dust, paper, or other material, because alpha radiation is not penetrating. Alpha radiation cannot penetrate turnout gear, clothing, or a cover on a probe. Turnout gear and clothing can keep alpha emitters off of the skin.

**There are two types of radiological weapons.** A radiological dispersal device (RDD) includes any explosive device utilized to spread radioactive material upon detonation. Any improvised explosive device could be used by placing it in close proximity to radioactive material. A Simple RDD spreads radiological material without the use of an explosive. Any nuclear material (including medical isotopes or waste) can be used in this manner. The main potential sources of such weapons "barring covert transfer from outside the US" are hospital radiation therapy (Iodine-125, Cobalt-60, Cesium-137), radiopharmaceuticals (Iodine-131, Iodine-123, Technetium-99, Thallium-201, Xenon-133), nuclear power plant fuel rods (Uranium-235), universities and laboratories and radiography and gauging (Cobalt-60, Cesium-137, Iridium-192, and Radium-226). Such materials can be delivered by a wide variety of means, including human agents, the destruction of a facility or vessel containing radioactive material, shipments or remote control devices that explode and disseminate the agent, placement in facilities or water supplies, or using aircraft, missiles, and rockets. Radiological dispersal weapons (RDWs) can also





be used to contaminate livestock, fish, and food crops.

**The effectiveness of such weapons is controversial**, and the impact can vary sharply because of the time required to accumulate a disabling or significant doses of radiation through ingestion, inhalation, or exposure. According to US military reporting on their effects, notes that, "there are no official casualty predictions for radiological dispersal weapons (RDWs). Because of the nature of the weapon, verification of the use of the weapon may prove difficult." Other findings of the Department of Defense provide important insights into the potential effectiveness of RDWs: Such a weapon would not produce a nuclear yield; but would spread contamination. While such weapons would produce far less immediate damage than devices that result in nuclear detonations, radiological weapons have enormous potential for intimidation. Targeting a nuclear reactor in an antagonist's territory to produce an accident releasing nuclear material would be another option.

There are hundreds of nuclear reactors and many more nuclear sources throughout the world, such as radiological materials used in hospitals. Both international and national measures control these items and associated materials and thereby contribute to proliferation prevention. However, post-war investigations in occupied Iraq showed that at least some of these control regimes could be circumvented, even by a state that was a nominal adherent to the Nuclear Non-Proliferation Treaty. Near-term concerns include the accumulation of large quantities of plutonium from reactors that is intended for reprocessing and/or storage, and the status of nuclear materials in the New Independent States that previously comprised the Soviet Union. The Practical Chances of Using Radiological Weapons A December 1999 report by the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction drew the following conclusions about the ability of terrorist groups to use radiological weapons: In the view of some authorities, theft of a nuclear device or building a weapon "in house" are the least-probable courses of action for a prospective nuclear terrorist.

**Far more likely-for all the reasons cited above-is the dispersal of radiological material in an effort to contaminate a target population or distinct geographical area.**

The material could be spread by radiological dispersal devices (or RDDs)-i.e. "dirty bombs" designed to spread radioactive material through passive (aerosol) or active (explosive) means. Alternatively, the material could be used to contaminate food or water. This latter option is, however, considerably less likely given the huge quantities of radioactive material that would be required. The fact that most radioactive material is not soluble in water means that its use by a terrorist would be unlikely and impractical, if the purpose is to contaminate reservoirs or other municipal water supplies, because the radioactive material will settle out or be trapped in filters. Those factors, coupled with the fact that any radioactive material will present safety risks to the terrorists themselves, collectively indicate the serious difficulties for any adversary attempting to store, handle, and disseminate it effectively. Radiological weapons kill or injure by exposing people to radioactive materials, such as cesium-137, iridium-192, or cobalt-60. Victims are irradiated when they get close to or touch the material, inhale it, or ingest it. With high enough levels of exposure, the radiation can sicken and kill. Radiation (particularly gamma rays) damages cells in living tissue through ionization, destroying or altering some of the cell constituents essential to normal cell functions.

**The effects of a given device will depend on whether the exposure is "acute" (i.e., brief, one time) or "chronic" (i.e., extended).** There are a number of possible sources of material that could be used to fashion such a device, including nuclear waste stored at a power plant (even though such waste is not highly radioactive), or radiological medical isotopes found in many hospitals or research laboratories. Although spent fuel rods are sometimes mentioned as potential sources of radiological material, they are very hot, heavy, and difficult to handle, thus making them a poor choice for terrorists. Other sources, such as medical devices, might be much easier to steal and handle. These materials, however have a lower specific activity than the materials in reactor fuel rods (although large unshielded sources are quite dangerous). Presumably, terrorists could steal a device (either in transit or at the service facility or user location) and remove the radioactive materials. Radioactive materials are often sintered in ceramic or metallic pellets.



Terrorists could then crush the pellets into a powder and put the powder into an RDD. The RDD could then be placed in or near a target facility and detonated, spreading the radiological material through the force of the explosion and in the smoke of any resulting fires. Of course, the larger the radioactive material dispersal area, the smaller the resulting dose rate. Although incapable of causing tens of thousands of casualties, a radiological device, in addition to possibly killing or injuring any people who came into contact -with it "could be used to render symbolic targets or significant areas and infrastructure uninhabitable and unusable without protective clothing." A combination fertilizer truck bomb, if used together with radioactive material, for example, could not only have destroyed one of the New York World Trade Center's towers but might have rendered a considerable chunk of prime real estate in one of the world's financial nerve centers indefinitely unusable because of radioactive contamination. The disruption to commerce that could be caused, the attendant publicity, and the enhanced coercive power of terrorists armed with such "dirty" bombs (which, for the reasons cited above, are arguably more likely threats than terrorist use of an actual fissile nuclear device), is disquieting. At the same time, a Department of Defense study notes that, "Iraqi and Russian separatists Cechnya have already demonstrated practical knowledge of RDWs. The availability of material to make RDWs will inevitably increase in the future as more countries pursue nuclear power (and weapons) programs and radioactive material becomes more available."

**The Practical Risks and Effects of Using Radiological Weapons**

**There is no question that small amounts of radioactive materials can be used to attack, threaten, and contaminate, and that the risk of radiation poses a serious psychological problem.** Covert attacks might produce slow radiation poisoning, and agents might be deliberately designed to make cost-effective decontamination difficult, time-consuming, or impossible. The limited use of small amounts of radiological weapons present the problem that there are no reliable criteria for determining which dose is dangerous or lethal, particularly if effects like long-term increases in the cancer rate are included. Responders also differ

sharply in terms of their use of sophisticated radiation detectors, and most responders are far more concerned with evacuation than the difficult problems of dealing with medical and decontamination aftermaths. In broad terms, however, these effects are somewhat similar to those of using a chemical weapon. They are not catastrophic, and even the contamination of most critical facilities could be dealt with GÇô at the cost of interruptions in service and efficiency. The large-scale weaponization of radiological materials presents a different issue. The above comments made some relatively casual assumptions about how easy or difficult it is to obtain and convert radioactive materials into a form that could be broadly disseminated over a wide area. These comments may be valid, but they also may not. There are significant disputes over how easy it is to grind up radioactive materials and spread them over an area larger than a single facility, and the unclassified literature seems to be based on generalizations rather than detailed technical analysis. This does not mean that such attacks are not possible, but it does mean that considerably more evidence is needed as to what can and cannot be done.

**One possible option is a systematic attack on a nuclear power plant.** This would require considerable expertise, access to the basic design of the plant and ideally to a full set of plans, and either an exceptionally efficient saboteur or a trained team. In most cases, it would require considerable time and effort to bypass safeguards and controls. The possible venting or overload of a reactor could then act as a radiological weapon, however, and cover hundreds of square kilometers as well as have a major potential affect on regional power supplies and some aspects of the US military nuclear program.

**Alternatively, an attacker might seize significant amounts of radioactive material from spent fuel storage, or during the nuclear fuel cycle,** which involves milling, conversion, enrichment, fuel fabrication, and disposal of waste as well as reactor operations. A seizure of spent fuel would be particularly dangerous during the first 150 days after the downloading of the reactor because Iodine-131 and Iodine-123 are present, is extremely volatile, and affects the thyroid.

**Work by the Department of Defense indicates that the following problems exist in trying to detect**



**and estimate the impact of radiological weapons:**

++ The impact of prompt radiation is extremely difficult to estimate, and lethal and serious doses can vary sharply according to exposure even in the same areas. Even personnel equipped with dosimeters present major problems in triage because dosimeter readings cannot be used to judge whole body radiation, and a mix of physical symptoms have to be used to judge the seriousness of exposure. The impact of radiation poisoning also changes sharply if the body has experienced burns or physical trauma. In the case of treatable patients, significant medical treatment may be required for more than two months after exposure.

++ Prompt detection and decontamination can have a major effect, and about 95% of external agents can be removed by simply removing outer clothing and shoes.

++ The spread of airborne radioactive particulates can vary sharply according to the size and nature of a weapon and its placement, and in the size and lethality of particles and water vapor. While most will settle within 24 hours, this will vary according to wind pattern and movement through the affected area. The drop in actual radiation of the affected material is generally much slower, but logarithmic. Radiation at the first hour after the explosion is down about 90%, and radiation is only about one percent of the original level after two days. Radiation only drops to trace levels, however, after 300 hours.

++ The test data on the longer-term (after 24 hours) effects of radiation are highly uncertain and the longer term impacts of radiation are so speculative as to be impossible to estimate. As a result, virtually all estimates of the impact of RDWs ignore the long-term casualties (96 hours to 70+ years) caused by radiation, such as cancer, and the impact of a weapon on the environment in terms of the poisoning of water and food supplies. The data on treatment of exposures from zero to 530 cGy of exposure do not even seem to call for recording the probable level of exposure.

++ The problem is further complicated by trying to estimate the specific mix of radioisotopes and radionuclides that will be produced and then become induced in the soil. The hazard prediction models used by the Department of Defense are under review, and it is not clear when new models will be available.

++ There is often a gap between generic data on radiation and the assumed level of treatment required. Much of the federal, state, and local response literature effectively dodges around the issue of triage, and the problem of choosing who will receive limited medical treatment and how these victims will be selected in the case of large scale exposures. It does not describe what is done with the assumed dying and untreatable, and some literature seems to assume that doses from zero to 70 cGy can be largely ignored, while other literature is more concerned with long-term effects. The broader issue of what indicators will be used for triage and deciding treatment and what treatment should actually be employed is generally not addressed because so many different RDWs and types of attack are possible.

++ The characterization of RDWs presents a significantly greater problem than does detection, and estimating the type and effects of a specific RDW is difficult. This is particularly true of contamination with RDWs or if detection only occurs after significant exposure. Because of the limitations of dosimeters and other detection equipment, bioassay is generally needed to determine the level and type of effects. This is critical with inhalation and ingestion.

++ Post attack radiological surveys can be very difficult for the same reasons.

++ Corpse disposal may be a major problem as may disposal of dead animals and birds. This aspect of response seems to be largely ignored.

++ Even military medical handbooks fail to address the psychological impacts of prompt and longer-term effects.

++ Food and water contamination can be a problem, and add to the response burden in any major attack.

Furthermore, considerably more study is needed of the different kinds of agents that might be used, of their different effects and risks, of the problem of characterizing the weapon versus detecting radiation, and of how triage, monitoring, and treatment need to be applied. The same is true of decontamination. As is the case with chemical and biological weapons, there is also a need for far more analysis of what kind of detection grids or systems are needed, of what level of shielding or masking would be effective,



and of how to predict dissemination and effects. More broadly, responders correctly assume that destruction and lethality are key criteria, but the main purpose of such an attack might be political or psychological. As is the case with chemical and biological weapons, public and world perceptions of the impact of such attacks would initially be based on the fact they occurred at all. It is also far from clear

how the public would react to even the most successful decontamination effort, and how well the US could guarantee the effectiveness of such a decontamination effort.

Past incidents of nuclear smuggling and black market sales have also demonstrated that it is far easier to obtain some form of radioactive than fissile material.

## Researchers show radioactive elements not acting in nature as previously modeled

Source: <http://www.homelandsecuritynewswire.com/dr20150622-researchers-show-radioactive-elements-not-acting-in-nature-as-previously-modeled>

June 22 – **Knowing how a chemical in soil reacts and transforms over time in response to neighboring elements, weather, and heat is essential in determining whether that chemical is hazardous. This is especially important when that chemical is radioactive.**

In a collaborative, international effort led by Los Alamos National Laboratory, researchers determined the speciation of uranium and plutonium pulled from soil, concrete and water reservoir sediment from six locations in the U.S., Ukraine, and Russia. Speciation is the chemical form or compound in which an element can appear, for example as nitrogen can form species of nitrate, nitrite or ammonia, among others.

“These results demonstrate the complexities of actinides in the environment and suggest that our models will not always accurately predict their long term fate and transport,” said Robert Roback, a Los Alamos Earth and Environmental Sciences Division deputy group leader and coauthor on the paper.

### Novel results, environmental implications

An LANL release reports that results clearly identified novel aspects of uranium and plutonium environmental chemistry beyond those previously reported and expected based on thermodynamics. In some samples, actinide-bearing materials that were within millimeters of each other for decades still exhibit significantly different speciation.

These results, the authors note, demonstrate complexities of actinides in the environment that are likely linked to the initial depositional form as well as to their subsequent mobilization and deposition. “These results do not

necessarily imply increased environmental risk, however, because some forms are quite stable and have low solubility,” Roback said. The results imply that to understand predict uranium and plutonium behavior in the environment, the analysis must consider site conditions, he said.

The researchers published their findings in a cover article “Multiscale Speciation of U and Pu at Chernobyl, Hanford, Los Alamos, McGuire AFB, Mayak, and Rocky Flats,” recently published by the American Chemical Society’s journal *Environmental Science and Technology*.

The researchers identified four types of both equilibrium species (mostly stabilized) and unpredicted novel types of these actinides unassociated with the source, which helped elucidate if and how the various forms of the elements may have been transformed by chemical reactions in the environment.

### Hazardous materials transformation

The chemical speciation of potentially hazardous subsurface contaminants is crucial to assessing environmental risk and remediation, because it determines the contaminants’ transport and toxicology. Understanding the behavior of uranium and plutonium contamination is imperative since not knowing the behavior is a significant impediment to environmental restoration at legacy nuclear weapons’ production and testing sites plus reactor accident locations.

Information obtained in the study will help researchers validate models that calculate safe residual levels, reducing the amount of hazardous material requiring removal and disposition. The scientists



retrieved samples from Chernobyl (nuclear power plant) and Hanford Site (plutonium reactors), Los Alamos (Manhattan Project-era waste), McGuire Air Force Base (nuclear warhead fire), Mayak (irradiated fuel processing waste) and Rocky Flats Environmental Technology Site (weapons' fissile material fabrication).

Materials from some of these sites involved high temperatures, melting, fires and explosions. In some cases, uranium and plutonium were known or suspected to have been released in acidic solutions that reacted with soil or concrete components. The goal was to determine the range of behavior in contamination and releases caused by chemical reactions.

Using synchrotron microprobes, researchers scanned soil to locate actinide hotspots and associated elements before performing more detailed analysis. Measurements were performed on beamlines at the Stanford Synchrotron Radiation Lightsource.

Quantitative electron probe microanalysis of Chernobyl samples was carried out at the V.G. Khlopin Radium Institute.

Higher temperatures (such as in the Chernobyl explosion and fire) promoted reactions and materials mixing. Samples revealed that in some cases particles melded without significant mixing, whereas other actinide particles intermingled with other metals, air and water to give a more homogenous mixture.

In a soil sample collected from Hanford, two distinct plutonium populations occur. One population, consisting of 20-micron cubes with uniformly low plutonium concentrations, was thought to have formed during initial deposition of the plutonium carried in tributyl phosphate.

The release notes that interestingly, a second population contains large plutonium concentrations as surface precipitates. The researchers suggest that this second population is evidence for plutonium mobilization and deposition onto the previously existing cubes found at Hanford.

— Read more in Olga N. Batuk et al., "Multiscale Speciation of U and Pu at Chernobyl, Hanford, Los Alamos, McGuire AFB, Mayak, and Rocky Flats," *Environmental Science & Technology* 49, no. 11 (27 March 2015): 6474–84



Greece – Vai Palm Beach (Island of Crete)



## Researchers use seismic signals to track above-ground explosions

Source: <http://www.homelandsecuritynewswire.com/dr20150526-researchers-use-seismic-signals-to-track-aboveground-explosions>

Lawrence Livermore researchers have determined that a tunnel bomb explosion by Syrian rebels was less than sixty tons as claimed by sources.

Using seismic stations in Turkey, Livermore scientists Michael Pasyanos and Sean Ford created a method to determine source characteristics of near-earth surface explosions. They found the above-ground tunnel bomb blast under the Wadi al-Deif Army Base near Aleppo last spring was likely not as large as originally estimated and was closer to forty tons.

**Seismology has long been used to determine the source characteristics of underground explosions, such as yield and depth, and plays a prominent role in nuclear explosion monitoring.** An LLNL release reports that now, however, some of the same techniques have been modified to determine the strength and source of near and above-ground blasts.

**The new method to track above-ground explosions serves as a forensic tool for investigators and governmental agencies seeking to understand the precise cause of an explosion.**

"The technique accounts for the reduction in amplitudes as the explosion depth approaches the free surface and less energy is coupled into the ground," said Pasyanos, an LLNL geophysicist and lead author of a paper appearing in an upcoming issue of *Geophysical Research Letters*.

The LLNL team used the method on a series of shallow explosions in New Mexico where the yields and depths were known.

Pasyanos and Ford's examination of source characteristics of near-surface explosions is an extension of the regional amplitude envelope method. This technique was developed and applied to North Korean nuclear explosions, then applied to chemical explosions and nuclear tests in Nevada.

"The technique takes an earthquake or explosion source model and corrects for the wave propagation to generate predicted waveform envelopes at any particular frequency band," Pasyanos said.

Methods for determining the yields of contained events range from teleseismic amplitudes and P-wave spectra to regional P-wave amplitudes and magnitudes. Pasyanos developed a method to characterize underground explosions based on regional amplitude envelopes across a broad range of frequencies. One advantage of the method is that examining the signal over a wide frequency band can reduce some of the strong tradeoffs between yield and depth, Pasyanos said

"By allowing the methodology to consider shallow, uncontained events just below, at, or even above the Earth's surface, we make the method relevant to new classes of events including mining events, military explosions, industrial accidents, plane crashes or potential terrorist attacks," Pasyanos said. "A yield estimate is often very important to investigators and governmental agencies seeking to understand the precise cause of an explosion." For the Syrian explosion, the team did not have local seismic data from Syria, but it was well recorded by regional stations from the Continental Dynamics: Central Anatolian Tectonics (CD-CAT) deployment in Turkey. If the explosion occurred well above the surface, a yield of 100 tons TNT equivalent would be required to produce the observed seismic signal.

"Given the video footage of the explosion, however, we know that it was neither at nor above the free surface, nor fully coupled," Ford said. "We estimate a chemical yield ranging from six and fifty tons depending on the depth, with the best estimate between 20-40 tons. Including independent information on the depth,



we could narrow this considerably. If, for instance, we definitively knew that the explosion occurred at two meters below the surface, then we would estimate the yield at forty tons.”

The team found that though there are expected tradeoffs between yield and depth/height, when

constrained by other information, the yields are consistent with ground truth yields in tests in New Mexico and reasonable values from what Pasyanos and Ford know about in Syria.

The research was funded by the Defense Threat Reduction Agency.

— Read more in Michael E. Pasyanos, Sean R. Ford, “Determining the source characteristics of explosions near the Earth’s surface,” [Geophysical Research Letters](#) (21 May 2015)

## Bomb-proof WALLPAPER could save lives

Source: <http://www.dailymail.co.uk/sciencetech/article-3092805/Bomb-proof-WALLPAPER-save-lives-Sticky-covering-reinforced-super-strong-Kevlar-fibres-stop-flying-debris.html>

Bomb blasts can send lethal debris flying and cause building to collapse from the shockwave. But the US Army has come up with a super strong wallpaper that could shelter soldiers from blasts.

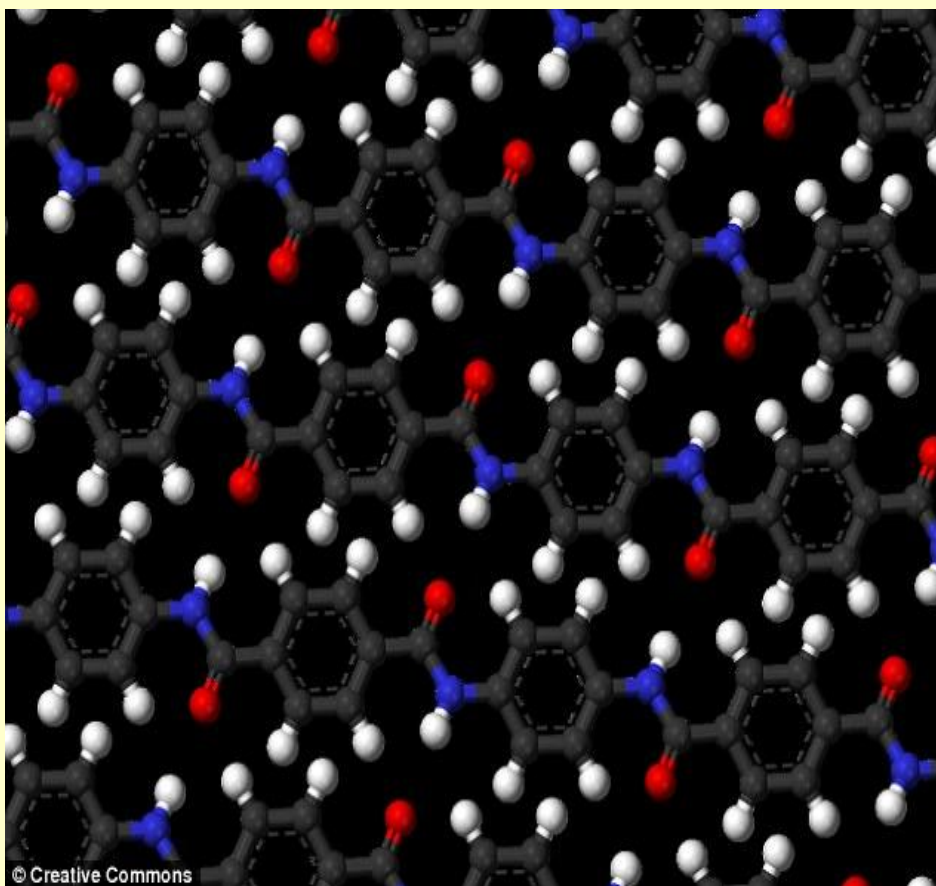
It is made from sticky fabric that is fortified with Kevlar fibres and could be swiftly applied to walls in war zones to make hideouts for

strength-to-weight ratio - making it five times stronger than steel.

When stuck to a wall, the wallpaper acts as a safety net to catch flying bricks and mortar.

A video of tests conducting on the material has shown how it can prevent walls made from bricks and breeze blocks from collapsing.

In a test recorded by Popular Science and engineer Theodore Gray, bomb-proof wallpaper was applied to walls built from different materials.



© Creative Commons

soldiers safer. Kevlar is used in everything from racing sails to body armour because of its high tensile

The wallpaper is made from a sticky fabric that is fortified with Kevlar fibres. A molecular model of the material is shown above. Its structure gives it a high tensile strength-to-weight ratio - five times stronger than steel

A wrecking ball was swung at the structures to imitate a blast and test what difference the wallpaper makes.

When the wrecking ball was pushed towards a breeze block wall without any wallpaper, the structure crumbled with one hit.

But the wall was much more resilient when strengthened with the wallpaper.





'It took a 'took a bunch of really hard hits but [the wrecking ball] still didn't really make it through the wall,' Mr Gray said. After a heavy hit, the wall bows but is held together by the wallpaper.

**LIGHTWEIGHT FLEXI ARMOUR**

Lightweight and flexible buoyant body armour also on show at the exhibition and could be in use as soon as next year.

Developed at the Naval Research Laboratory, it's designed to protect a wearer's spine and torso from bullets, fragmentation - and possibly IEDs too.

'It's a great solution for [spinal injury],' research physicist Raymond M Gamache said, 'and while the insert can't stop blunt-force trauma, you'll still be alive.'

Unlike current armour which some troops find heavy and restrictive, this new variety is 'like wearing a fabric [and] it's loose,' Mr Gamache said.

It looks like dimpled foam rubber and is highly flexible.

'You can twist and turn, but you're always going to maintain the same protection against bullets,' he said.

The test applied to a red brick wall showed similar results.

With a relatively gentle knock, the reinforced wall seems to easily absorb the impact, but with a heavier knock, bows and stays bent.

Mr Gray said: 'On the last impact we really gave it a good wallop and I pulled the ball back as far as I could and gave it a hard shove. 'You can see it has literally broken the wall in half and yet the wallpaper held.'

Nick Boone, a research mechanical engineer with the US Army, told The Huffington Post: 'Ballistic wallpaper is still in the research and development stage and does not yet have an official name, but it could one day be produced and fielded and hopefully save lives.'

Commenting on the invention, Justin Bronk, research analyst at the Royal United Services Institute, told the BBC that while the idea of coating buildings to reduce the danger of flying debris isn't new.

'What appears relatively new about this ballistic wallpaper is that it can be quickly and easily applied by non-specialised units at short notice,' he said.

'This provides significant potential tactical advantages.

Engineers will build reinforced structures and bomb them to test the wallpaper's abilities.

The prototype went on display at the Pentagon's first Department of Defense Lab Day where over 100 innovations were shown off by US Army engineers.

Lightweight and flexible buoyant body armour also on show at the exhibition, could be in used as soon as next year.

Developed at the Naval Research Laboratory, its designed to protect wearer's spines and torsos from





bullets and fragmentation - and possible IEDs too.

'It's a great solution for [spinal injury],' research physicist Raymond M Gamache said. 'And while the insert can't stop blunt-force trauma, you'll still be alive.'

Unlike current armour which some troops find heavy and restrictive, this new variety is 'like wearing a fabric [and] it's loose,' said Mr Gamache.

It looks like dimpled foam rubber and is highly flexible.

'You can twist and turn, but you're always going to maintain the same protection against bullets,' he said.

Robots, medical devices, safer helmets and high tech weapons were on show, developed by thousands of scientists working at US Department of Defence labs in 22 states.

Aerospace technology and advances in autonomy such as the Navy's unmanned Jet Ski and the Airforce's 'Vigilant Spirit' drone were also on display.

'All these things and many more allow our warfighters to have the cutting-edge capabilities they really need and laboratory innovation is at the forefront of that,' Undersecretary of Defence for Acquisition, Technology and Logistics, Frank Kendall said.

### Islamic State builds an 'air force' out of truck bombs

Source: <http://www.japantimes.co.jp/news/2015/05/30/world/islamic-states-weapon-mass-destruction-truck-bombs/#.VWsr7ZOTLz5>



May 30 – **The Islamic State group's monstrous truck bombs — easy to make, hard to stop and capable of destroying a city block — are reshaping the battlefield.**

The jihadis used about 30 explosives-rigged vehicles in the Iraqi city of Ramadi this month, blasting their way through positions that government and allied fighters had managed to hold for more than a year.

**Islamic State fighters have used looted armored personnel carriers, pick-up trucks, tankers and dump trucks.** They pack them with tons of explosives and weld steel cages around them.

When a position is too well defended for a more conventional advance, a suicide driver steers a truck bomb, protected by the makeshift armor, through enemy fire and straight to his target.

"They are protected from 12.7-mm (heavy machine-gun) fire and even some RPGs (rocket-propelled grenades). There's so much explosives (inside) that it's still effective at 50 meters," an Iraq-based Western military expert said.

Videos of attacks with truck bombs, which the jihadis have also used in the battle of Kobane



in northern Syria and on other fronts, show huge explosions that are visible from far away.

"The damage is bigger than that of a half-ton bomb dropped by a fighter jet," the Western expert said. "Truck bombs are their air force."

Responding to U.S. accusations that his troops dodged battle in Ramadi, Prime Minister Haider al-Abadi defended them by saying the impact of a truck bomb blast is akin to that of "a small nuclear bomb."

The Islamic State group did not invent what is now known as a suicide vehicle-borne improvised explosive device (SVBIED). It is unclear who holds that dubious distinction. Rigged horse carts were used more than two centuries ago, such as in a failed 1800 assassination attempt against Napoleon in Paris.

Vehicle-borne bombs' formidable potential as a weapon was put on display with the 1920 Wall Street bombing carried out by Italian anarchist Mario Buda, said Mike Davis, author of "Buda's Wagon: A Short History of the Car Bomb."

The Islamic State organization has used suicide car bombs in Baghdad for similar purposes: to sow terror in the population and paint the authorities as powerless to control and govern.

The group's previous incarnations in Iraq had already detonated 18-wheelers stuffed with explosives during the U.S. military presence, but its commanders are taking the use of truck bombs to a new level.

"The offensives in Iraq may be the first time that VBIEDs have been used as part of the order of battle of a large attacking force in Middle Eastern warfare," said Andrew Terrill, a professor at the U.S. Army's Strategic Studies Institute.

The Tamil Tigers formerly integrated suicide car and truck bombs with an infantry assault, but Davis points out they were mostly "solo attacks" to initiate battles.

"The Ramadi attack was shock and awe on a wholly different scale," he said.

A U.S. State Department official said nearly a dozen truck bombs used in Ramadi had carried explosives sufficient to cause a blast the size of the 1995 Oklahoma City bombing.

Davis said a van bomb such as that used in Oklahoma City is "the explosive equivalent of the bomb load carried by a B-24 in World War II — a poor man's air force, so to speak."

"But the truck bombs in Ramadi ... were obviously far more powerful, and probably the equivalent to an air attack with 1,000-pound (450-kg) bombs," he said.

After the fall of Ramadi, Washington sent 2,000 AT4 anti-tank weapons to equip Iraqi forces with firepower able to take out the truck bombs.

"It's good in the open but it's unguided, so if (the truck) is coming at you, you have to stand in front of it," the military expert said of the Swedish-developed weapon. "When the truck is within 100 meters, it's almost too late already. And in a city — in Ramadi, for example — it's almost impossible to avoid the truck bombs."

Thousands of security force members and allied militiamen are trying to seal Ramadi off as part of an operation to retake it, but al-Abadi admitted that entering the city is risky.

"We have decided not to fight into the cities ... because of those truck bombs, which you cannot see inside the city because there are small roads," he told the BBC this past week.

By fully integrating suicide truck bombs carrying huge payloads in ground attacks, Islamic State has already forced a tactical rethink from Baghdad and its allies.

"The greatest military myth of the previous century, of course, was that air power alone could defeat insurgents," Davis said, adding that truck bombs had helped make a "new paradigm."

## Cambodia's new bomb divers aim to make its rivers safe

Source: <http://www.theguardian.com/world/2015/may/26/cambodias-new-bomb-divers-aim-to-make-its-rivers-safe>

May 26 – It was on an unrelentingly hot day last week when Sok Chenda dived into the Mekong river and helped change how Cambodia deals with a deadly chapter from its history.

He slipped into the warm water, adjusted his mask and scuba gear, steadied his breathing and slowly began his descent several meters below, where the river water gradually





clearance and have simply lacked the technical skills to handle such salvage.

Advertisement

However, Chenda and his colleagues from the Cambodian mine action centre (CMAC), endured two years of

gruelling army-style training to get to this

turns from pale to thick, acidic yellow. Down there, in a lonely world of swirling sediment and the sound of one's own breathing, Chenda was feeling for something in the cloudiness.

And then he saw it: a live, 500lb (225kg) Mark 82 aircraft bomb that had wedged itself in the riverbed, still in the same position 40 years after it had fallen.

Working meticulously and methodically Chenda carefully fixed a cable to the metal carcass connecting the bomb to an inflatable lift bag. The bomb was pulled free and towed to land where it was then driven to a desolate field and sawed into three parts by a remote-controlled machine. The explosive matter was then set alight.

The Mark 82 was a relic from the 1960s and 70s, when Cambodia was pounded by an estimated 2.7m tonnes of ordnance dropped mostly from American planes as the war in Vietnam spilled over the border.

Had it met its target all those years ago it would have probably blown a vast hole in Cambodian soil where at least 2000sq km of land remain contaminated and possibly several thousand tonnes of munitions are still under water.



turning point in the country's efforts in UXO clearance, becoming part of the first team to safely salvage a deadly remnant from one of the country's main waterways.

The feat was nothing short of remarkable, not least because it came just two years after they learned how to swim, then scuba dive, then hone the composure to clear bombs in such an unusual environment using only their sense of touch.

"We looked at people who were learning fast," said Allen Tan, country director of the Golden West Humanitarian Foundation, which works on mine and UXO clearance and provided training for the team with funds from the US State Department.

"Forty candidates had to learn how to swim and scuba dive safely in 30 days," said

Tan. "That is quite a learning curve and it was intense ... But the number one thing was: did they have heart?"

"To make it in this you have to have very good resolve. You have to want it so bad to be able to



Even today unexploded mines and bombs kill hundreds across the country – indeed before now, this bomb's extraction would have been near impossible: Cambodia's de-mining operations are focused primarily on land



make it through and be willing to really push yourself.”

Some failed, some simply dropped out. Two candidates were failed just two days before graduation, “because it’s that serious”, Tan said.

“You can’t be their friend, because they could die. You have to take people on merit solely. We assign them numbers; we didn’t know their names and we didn’t want to know.”

In the end, he said the 10 graduates – one has since left the team – spent the next two years in further training and developed the skills and modesty needed to work in such a “mentally tough environment”.

Chenda, who spent 16 years clearing explosive ordnance on land, said he was happy to have changed direction, despite the intensity of the training.

“It was difficult to see – we could not see,” he told the Guardian of his dive. “But I was not scared. I was focused.”

Mike Nisi, Golden West’s chief of underwater operations, said the procedure was “textbook” in its execution.

As well as the vast number of bombs dropped aerially, it is estimated that up to 300 weapons supply boats from South Vietnam were sunk by Khmer Rouge forces to stop them from reaching the US-backed Lon Nol army in Phnom Penh.

Like so many other remnants of conflict, the bomb that Chenda brought to the surface may well have stayed unnoticed in the thick river mud, its fins protruding at a sideways angle,

had it not caught on the net of a 42-year-old fisherman, Yor Dieb, last month.

Dieb, who has fished these waters in a tranquil part of Kandal province for the past 20 years, knew the significance of his snagged net only when he dived in to liberate it by hand.

“I was scared,” he said, not least because it is the second bomb he has caught his net on in 10 years in this stretch of water, across which boats also ferry people.

According to the most recent report issued by the Cambodian Mine Action and Victim Assistance Authority, 64,496 casualties have been recorded since 1979 and February 2015. Of these, 19,708 people were killed, 35,822 people injured and 8,965 people had to undergo amputations.

CMAC is now able to turn its attention to remnants found underwater, as well as to the approximately 20,000 calls it receives every year from the public who come across suspicious-looking devices.

“We have found a number of cases where people have been wounded or killed by munitions under the water, even mines, when people use the traditional bamboo tools to catch catfish ... and when they come to pick up those tools, they blow up,” CMAC’s director-general, Heng Ratana, said.

For Dieb, the fisherman, the need for more focus on making riverbank communities safe from ordnance is important.

“Fishermen are so scared about finding more bombs,” he said.

## Northrop Grumman Unveils Next-Gen Unmanned Ground Vehicle

Source: [http://i-hls.com/2015/06/62976/?utm\\_source=Israel+Homeland+Security+%28iHLS%29&utm\\_campaign=ce5a6e58f9-Newsletter\\_English\\_10\\_6\\_2015&utm\\_medium=email&utm\\_term=0\\_8ee2e16ed1-ce5a6e58f9-87373033&mc\\_cid=ce5a6e58f9&mc\\_eid=521c0e089a](http://i-hls.com/2015/06/62976/?utm_source=Israel+Homeland+Security+%28iHLS%29&utm_campaign=ce5a6e58f9-Newsletter_English_10_6_2015&utm_medium=email&utm_term=0_8ee2e16ed1-ce5a6e58f9-87373033&mc_cid=ce5a6e58f9&mc_eid=521c0e089a)



Northrop Grumman announced that its subsidiary REMOTEC has unveiled the Andros FX (TM), a more capable and dexterous unmanned ground vehicle. The vehicle is designed to defeat a wide range of threats, including vehicle-borne improvised explosive devices (VBIED).

According to World Defense Net, the features of the **Andros FX** (TM) are the four track pods that replace the traditional Andros articulators and a new arm design with more lift capacity and greater dexterity by adding roll joints that provide nine degrees of freedom.

The unmanned ground vehicle also



features updated system electronics, mobility improvements for increased speed and maneuverability, and a new touchscreen operator control unit with 3-D system graphics, advanced manipulator controls and improved user interface.

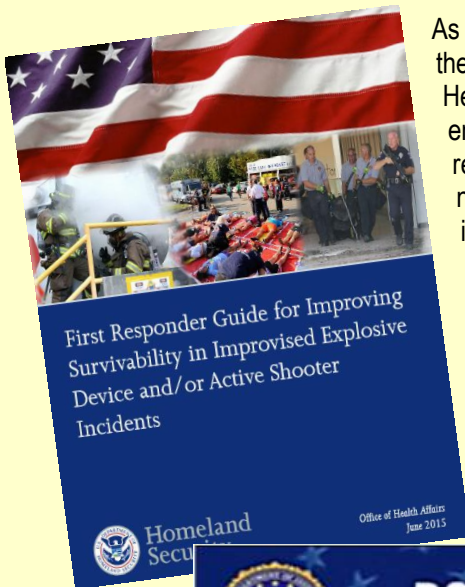
Walt Werner, director of Northrop Grumman’s REMOTEC said, “Bomb squads have told us what they need most are more capabilities to counter vehicle-borne IEDs.” In accordance to that, the Andros FX(TM)’s operating system provides much greater information to the operator while easing user workload through more interactivity with intelligent payloads such as chemical and radiation sensors. Preset arm positions and the ability to “fly the gripper” make manipulation of objects much easier, faster and more accurate.

Increased cross-functional involvement early in the design phase results in a much lower lifecycle cost as well as a product that can be quickly adapted for a variety of missions, easily upgraded and expanded, and more efficiently maintained, Werner added.

## DHS OHA Announces Release of IED and Active Shooter Guidance for First Responders










Kathryn Brinsfield, Assistant Secretary for Health Affairs

Source: <http://www.dhs.gov/blog/2015/06/09/dhs-oha-announces-release-ied-and-active-shooter-guidance-first-responders>



As part of our mission, the DHS Office of Health Affairs works to ensure that first responders around the nation have the tools, information and resources they need to respond to incidents in their communities. In recent years, improvised explosive device (IED) and active

shooter incidents reveal that some traditional practices of first responders need to be realigned and enhanced to improve the survivability of victims and the safety of first responders caring for them. To this end, OHA has drafted and released the “First Responder Guidance for Improving Survivability in Improvised Explosive Device and/or Active Shooter Incidents” to help address this issue. OHA was supported in this effort by the White House, and partnered with several federal agencies, including the Departments of Defense, Health and Human Services, Justice and Transportation, to develop these recommendations. Based on best practices

BOMB THREAT STAND-OFF CARD					
Threat Description		Explosives Capacity	Mandatory Evacuation Distance	Shelter-in-Place Zone	Preferred Evacuation Distance
 Pipe Bomb		5 lbs	70 ft	71-1199 ft	+1200 ft
 Suicide Bomber		20 lbs	110 ft	111-1699 ft	+1700 ft
 Briefcase/Suitcase		50 lbs	150 ft	151-1849 ft	+1850 ft
 Car		500 lbs	320 ft	321-1899 ft	+1900 ft
 SUV/Van		1,000 lbs	400 ft	401-2399 ft	+2400 ft
 Small Delivery Truck		4,000 lbs	640 ft	641-3799 ft	+3800 ft
 Container/Water Truck		10,000 lbs	860 ft	861-5099 ft	+5100 ft
 Semi-Trailer		60,000 lbs	1570 ft	1571-9299 ft	+9300 ft



and lessons learned from civilian and military incidents, this guidance focuses on the medical response to IEDs and/or active shooter incidents with recommendations for hemorrhage control, personal protective equipment, and response and incident management. The recommendations presented will help to save lives by mitigating first responder risk, and improving the emergent and immediate medical management of casualties encountered during IED and/or active shooter incidents.

In February 2014, DHS brought a variety of first responder groups together so that unique

solutions and perspectives that work for each community could be discussed and considered for adoption. Representatives from state and local fire service, law enforcement, emergency medical services, emergency management, and a number of federal organizations participated in subject matter expert presentations, as well as panel and group discussions, on response to IED and active shooter incidents.

I hope that all first responders will find the guidance beneficial and apply pieces of it to their communities.

► You can read the full document at:

<http://www.dhs.gov/sites/default/files/publications/First%20Responder%20Guidance%20June%202015%20FINAL%202.pdf>



### Small Drones Are A Big Danger; Think Flying IEDs: CNAS

Source: <http://breakingdefense.com/2015/06/small-drones-are-a-big-danger-think-flying-ieds-cnas/>



An Army soldier launches a Raven hand-held drone in Iraq.

Sometimes small is beautiful. Sometimes small is lethal. While China and Russia are researching stealthy and armed drones, the drunk intelligence analyst who landed a Chinese-made mini-drone on the White House lawn in last month may be the more worrying sign of things to come.

Afghan and Iraqi guerrillas kludged together murderous roadside bombs with scavenged or homebrewed explosives triggered by cellphones or garage door openers, killing more Americans than any of Saddam's Scud missiles or main battle tanks. What might similarly ingenious



insurgents do with off-the-shelf drones? “We’re seeing capabilities that were previously the monopoly of major military powers are now accessible...to non-state actors, even individuals,” said Kelley Saylor. She’s an associate fellow at Center for a New American Security and author of a report out this morning, “A World of Proliferated Drones.” (CNAS provided us a copy in advance).

“There’s been a lot of discussion around town, particularly as relates to drones in the national security space about high-end drones,” Saylor told me. “We didn’t really see there being discussion on the range of systems that are available...particularly given the availability of low-end systems, hobbyist drones, even commercial drones.”

**The biggest danger in the medium term: swarming technology.** As drones get not only smarter but cheaper, an enterprising adversary could buy a bunch and release them all at once, with the drones using insect-like artificial intelligence to converge on their target. Lots of little threats carrying lots of little bombs can add up quickly.

“Particularly if you’re looking at systems that can truly navigate autonomously, using those systems en masse is going to enable you to neutralize a much larger target,” Saylor said, “[and] it’s going to be more difficult to defend against because some of the lower end solutions like shooting the thing out with a shotgun might not necessarily be feasible.”

“Drones will enable airborne IEDs [improvised explosive devices] that can actively seek out US forces, rather than passively lying in wait,” Saylor wrote in the report. “Indeed, low-cost drones may lead to a paradigm shift in ground warfare for the United States, ending more than a half-century...in which US ground forces have not had to fear attacks from the air.”

Sophisticated drones are definitely part of that future threat, she said. But they require the resources of an advanced nation-state to develop and operate, and nation-states tend to be less murderously inventive than low-rent irregulars.

“When we are looking at the higher end systems we are seeing something that would be akin to

missiles or manned fighters,” Saylor said. “When you’re looking at traditional state use, you are probably going to find more traditional and restrained uses.”

**Guerrillas and terrorists, by contrast, generally have much less capability than nation-states, but they are more likely to use what they have in unexpected ways.**

Hezbollah has fired a drone with almost 60 pounds of explosives at Israel, although it was detected and shot down. Smaller drones are harder to detect, and states less vigilant than Israel — which has anti-missile systems constantly stopping rockets — might not be set up to detect them.

“We’re more looking at a threat that is rising from unanticipated use where US troops or allied troops are not particularly expecting a threat... and therefore your countermeasures are not really in place,” said Saylor.

**The simplest use of off-the-shelf drones would be to spy on US forces.**

That kind of low-rent reconnaissance could provide a significant tactical advantage without requiring any modifications. With a little jury-rigging, many widely available drones could carry five to 10 pounds of explosive. That’s hardly the same as a vehicle-flipping 500-lb roadside bomb, but it’s enough to kill.

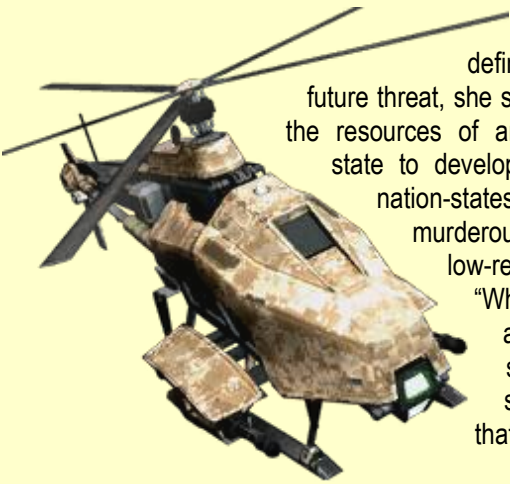
**The good news is that if you are aware of the threat, there are plenty of ways to stop it.**

“If you know these systems are coming ... you can shoot them down with a shotgun,” Saylor said. Or, if you’d like to fight robotic fire with fire, there are specialized “drone-hunting drones” that catch unauthorized flying objects in a net.

**The easiest way to defend large areas for a long time is jamming.**

At the very least you prevent the enemy drone from transmitting back intelligence to its operators. For the majority of drones flying today that navigate using either continuous GPS signals or constant remote control by a human, jamming can stop them in their tracks.

The immediate problem is what else you’ll jam. In a wilderness or free-fire war zone, the electronic collateral damage might not matter. In urban counterinsurgency, peacekeeping, or policing, however, you’ll turn the local population against you quickly if you’re constantly scrambling their cellphones. Set the jammers to avoid civilian signals like phones and police radios, and you can



bet the bad guys will convert their drone controls to use the same frequencies. The longer-term problem is that drones are getting smarter and more autonomous. "In the next few years we're going to see technologies like sense-and-avoid systems being

incorporated that allow the drone to autonomously navigate around objects," said Saylor, reducing the need for a GPS signal or constant human supervision. That makes the coming swarm much harder to stop.

## Israeli Company Trains Mice to Sniff Out Bombs at Airport Security Check

Source: <http://jpuupdates.com/2015/06/16/israeli-company-trains-mice-to-sniff-out-bombs-at-airport-security-check/>

The next time you go through security at Ben Gurion Airport, don't be surprised if you get checked out by a tiny mouse. The Israeli security company, X-Test, has trained mice to respond when they detect explosives, alerting security officers at airport and mall security checkpoints. X-Test vice-president Yuval Amsterdam, a former bomb-disposal expert for the Israel Defense Forces, addressed the Body Search 2015 conference in London last week. And said: "They're as good as dogs as far as their ability to sense, but they're smaller and easier to train. They're cheap, and you don't have to take them for a walk. Once they are trained, they become bio-sensors."



According to the Amsterdam, the mice are expected to produce much more reliable results as they can be trained in large numbers by a machine.

The developers working on the project are hoping that the mice will not only be able to detect bombs implanted inside a body but also drugs, thereby combating smuggling.

"We can teach them anything that has a scent – whether it's explosives, whether it's drugs, whether it's ivory in Africa. Anything that has a smell." Amsterdam added.

The present system for an explosive trace test involves swabbing a surface such as a laptop keyboard or cabin-bag zip and testing the swab in an explosives trace detector. The mouse system does not involve allowing the mice to scamper over passengers and





luggage. Instead, they will be contained in cages and discreetly positioned where they can sniff people and their possessions.



Philip Baum, editor of *Aviation Security International*, had high hopes for the new system: "We do not currently have explosive detection capability in our portals, or an accepted way of detecting 'internal carries'. The mice just might plug that security hole."

## SWEDEN: Four Killed In Car Blast In Gothenburg

Source: <http://news.sky.com/story/1501490/four-killed-in-car-blast-in-gothenburg>

June 13 – **Four people, including a young girl, have been killed after a car exploded in the Swedish city of Gothenburg.**

The suspected car bomb ripped apart the vehicle as it drove up to a roundabout in the city centre on Friday night.

Police are investigating the cause of the explosion, and have not released details of the victims.

Eyewitness Janne Wolltin told public broadcaster SVT

that pieces of the car shot into the air in front of him.

"When I came up to the car I saw that it must have been a bomb," he said.

"It was completely torn apart, the front part of the engine and everything was gone."

One of the victims was a well-known criminal gang leader in the city, according to local news reports.

Gangs in Gothenburg have been involved in tit-for-tat revenge killings in recent years.

**In March, gunmen sprayed a pub in the city with bullets, killing two people and injuring 10 others.**

Robert Karlsson, head of the region's criminal investigation unit, said it was too early to say if the explosion was linked to gangland violence.

"We have no leads, either in one direction or another. We are just at the beginning of this," he said.

Gothenburg police said three people in the car died at the scene, and the young girl died later in hospital.



## A growing threat: Car hacking

Source: <http://www.homelandsecuritynewswire.com/dr20150526-a-growing-threat-car-hacking>



A string of high-profile hacks — the most recent on President Obama's personal email account — have made cybercrime an ever-growing concern in the United States. Despite the publicity, most people still think of hacking as something which is done only to information systems like computers and mobile devices.

In reality, hacking is no longer confined to the information world. The level of automation in modern physical systems means that even everyday automobiles are now vulnerable to hacking.

On Friday, Virginia governor Terry McAuliffe announced a public-private working group to address the threat of automotive hacking. A U.Va. release reports that the University of Virginia, the Virginia State Police, and the Charlottesville security firm Mission Secure Inc. will play key roles in conducting this joint research project between various government agencies and private firms.

McAuliffe appointed Barry Horowitz, professor and chair of U.Va.'s Department of Systems and Information Engineering, as a member of the Virginia Cyber Security Commission in 2014, and Horowitz will help oversee the new research project.

"The motivation has been that more and more in your everyday life you see that we're

automating physical systems," Horowitz said. "And unlike an information system, a physical system could kill you by accident."

In 2012, Horowitz was part of a Department of Defense-funded research team that began identifying ways to protect unmanned aerial vehicles from cyberattacks on their controls. During that project, he and his fellow researchers realized that there were broader applications for their work. Together with U.Va.'s Licensing and Venture Group, they founded Mission Secure as a way to address threats to a variety of automated physical systems.

Mission Secure's goal is to create a monitoring system that allows critical physical systems — like the vehicles used by the defense, energy, and transportation industries — to keep working during a cyberattack.

The new working group involving U.Va., the State Police, and Mission Secure will help the government gain an advantage over future cyber criminals by learning to anticipate and respond to possible threats before they occur.

"Our goal is to help with this vulnerability assessment and testing and see what is potentially possible for forensics," Mission Secure CEO David Drescher said. "At some



point when the police show up at an accident, they will need to determine whether that accident was caused by human error or whether some kind of a cyber incident occurred.”

To date, there are no known cases of cyberattacks on government or civilian vehicles in the United States, but law enforcement agencies are certainly aware of the possibility. Before working with State Police, Mission Secure and U.Va. ran tests on an automated Toyota Scion owned by Charlottesville’s Perrone Robotics Inc. Using just a wireless key fob, researchers were able to take control of the Scion’s braking and acceleration.

A recent episode of CBS’s “60 Minutes” also showed how a hacker was able to cause problems to an ordinary sedan being driven by reporter Lesley Stahl. In that demonstration, the hacker used a laptop to take control of the acceleration, braking, windshield wipers and car horn.

Alarming as these possibilities are, Horowitz said that cybersecurity for physical systems already has a huge advantage that is lacking in the security for information systems. Physical systems are capable of far fewer functions, so it is much easier to recognize when they are exhibiting “illogical behavior.”

Examples of this illogical behavior would be continued acceleration while slamming on the brakes or automatic windshield wipers that turn on when there is no rain. It is immediately apparent that there is a problem, so the next steps are to correct the malfunction and identify its source.

This is where Mission Secure’s patent-pending Secure Sentinel device comes in. It acts as a monitor that drivers can trust and is extraordinarily secure compared to the system it is guarding.

Horowitz said that the purpose of the device is twofold. “First, save the driver in the car,” he

said, “and second, let’s figure out who did it and how we can find them.”

The platform will do this by simultaneously monitoring potential areas for attack and alerting the driver of any incoming issues. Further tests will determine the most efficient way to alert the driver, but Horowitz said it may start out as something as simple as a horn blast. Once any consequences of an attack are stopped, the system will then begin forensic work to track where it came from.

The Virginia State Police will use their own experience to help researchers identify the most likely points of attack.

“We’re trying to figure out what we call the ‘most likely and consequential’ cyberattacks that could occur,” Drescher said.

The release notes that the State Police have provided two police cruisers to be used as test subjects for the research, one each of the standard Ford and General Motors models they use. Researchers will test them for vulnerabilities on an escalating scale starting with the most basic and working their way up to more sophisticated attacks.

“We’re starting with common tools,” said Ed Suhler, Mission Secure’s co-founder and vice president of implementation. “We want to see what your average IT person could accomplish and then work our way up from there.”

Right now, there is an information gap between the fields of mechanical engineering and computer science. By looking for ways to bridge that divide, the research team hopes to better prepare Virginia for the future of automated vehicles. This commitment from the governor’s office means more law enforcement personnel could be trained and educated on the overlap between physical systems and cybersecurity.

“As a population, we’re not prepared yet,” Horowitz said. “Luckily, nor are the attackers quite yet.”

## Cyber Warriors Need Plenty of Rest

Source: <http://fas.org/blogs/secretcy/2015/05/usaf-cyber/>

**New guidance from the U.S. Air Force on the use of cyberspace weapons directs Air Force personnel to get a good night’s sleep prior to performing military cyberspace operations and to refrain from alcohol while on duty.**

“Crew rest is compulsory for any crew member prior to performing any crew duty on any cyber weapon system,” the May 5 guidance says. “Each crew member is individually responsible to ensure he or she obtains sufficient rest during crew rest periods.”



Furthermore, "Crew members will not perform cyberspace mission duties within 12 hours of consuming alcohol or other intoxicating substances, or while impaired by its after effects," the new Air Force guidance stated.

"This instruction prescribes operations procedures for cyberspace weapons systems under most circumstances, but it is not a substitute for sound judgment or common sense," the Air Force said.

The document discusses the general conduct of Air Force cyber operations, including so-called "Real-Time Operations & Innovation" (RTOI) projects that enable the USAF "to generate tools and tactics in response to critical cyber needs at the fastest possible pace."

See [Cyberspace Operations and Procedures](#), Air Force Instruction 10-1703, volume 3, 5 May 2015.

With the growing normalization of defensive and (especially) offensive military operations in cyberspace, more and more U.S. military doctrine governing such activity is gradually being published on an unclassified basis. Some of the principal components of this emerging open literature include the following:

[Cyberspace Operations](#), Joint Publication 3-12, 5 February 2013

[Cyberspace Operations](#), Air Force Policy Directive 10-17, 31 July 2012

[Command and Control for Cyberspace Operations](#), Air Force Instruction 10-1701, 5 March 2014

[Legal Reviews of Weapons and Cyber Capabilities](#), Air Force Instruction 51-402, 27 July 2011

[Information Assurance \(IA\) and Support to Computer Network Defense \(CND\)](#), Chairman of the Joint Chiefs of Staff Instruction 6510.01F, 9 February 2011

[Department of Defense Strategy for Operating in Cyberspace](#), July 2011

## Brazil Put Its Military In Charge of Cyber Security

Source: <http://i-hls.com/2015/05/brazil-put-its-military-in-charge-of-cyber-security/>



44

Brazil is currently one of the most technologically developed country in South America and it is also concerns its military. Social media, online banking and a software industry development are the state's locomotives.

However, along with the developed internet environment, the digital world dark side cannot

be ignored. Online scams, hacking, espionage and digital surveillance are at place. The problem is with the proper response to those threats from the government side. It may have seriously misinterpreted the nature and significance of those threats and, as a consequence, the best way to tackle them.



For political reasons Brazil has outsourced most responsibility for the country's cyber security to the military. While the armed forces has enthusiastically embraced this new role, placing them in charge of overall cyber security for both civilian and military networks is a mismatch that could have damaging consequences the country's security.

Not all the cyber threats are equal therefore not all of them are to be treated by the military alone. Brazil's popular protests of June-August 2013, for example, coincided with a sharp rise in hacktivist activity, but if the military to take care and deal with it, it might pose danger on a social scale

Since Edward Snowden's revelations which involved listening on Brazilian President Dilma Rousseff's phone by US surveillance, it ratcheted-up Brazil's concern with cyber security. The U.S. National Security Agency was routinely spying on wide spread of state and commercial networks, but Brazil was friendly to the United States most of the time in Latin America. The recent developments are rising skepticism towards US intentions and Washington should not underestimate the reputational damage that its global surveillance strategy has inflicted.

**There is virtually no public debate or research in Brazil into those responsible for launching cyber attacks, what their interests and motivations might be, how they operate, or if and how they might be connected to criminal and political organizations.**

While operating to a large extent in the dark, the Brazilian government has nevertheless rapidly constructed a sprawling cyber security and defense infrastructure.

Its response is narrowly focused on just one or two dimensions of these threats—especially foreign ones. At the center of the state's response is the Brazilian Army's Center for Cyber Defense (CDCiber), one of the only such entities in South America. Yet the emphasis on a military response may be incommensurate with the real (as opposed to existential) threats facing the country. Despite allegations of Hezbollah smuggling weapons to Brazilian gangs (these rumors have been circulating for decades), the country has comparatively few external cyber threats from foreign governments or terrorist groups.

This represents a mismatch with the real and emerging threats in cyberspace. Instead of

focusing on international and domestic cyber-criminality, which constitutes by far the gravest risk, the state is doubling down on strengthening cyber war-fighting and anti-terrorism capabilities.

Government is overemphasizing broader issues of national security rather than addressing the core of the cyber crime, as most pressing challenges confronting citizens.

The military approach to cyber insecurity in Brazil is consistent with a broader effort to find a role for the Brazilian armed forces in the twenty-first century. On the one hand, they are strengthening border control and anti-drug activities in the Amazon and the so-called tri-border area of Argentina, Brazil and Paraguay. On the other, the military is seeking to expand its reach and influence in cyberspace.

For instance, CDCiber and Brazil's central intelligence agency (ABIN) created social media monitoring platforms in the aftermath of the 2013 protests.

Meanwhile, other public institutions such as the Federal Police are less generously resourced and supported. These developments are partly inspired by Brazil's desire to enhance its geopolitical reach and relevance. As a rising power, the Brazilian government is mobilizing the country's nascent cyber security architecture to project soft power in bilateral relations and multilateral arenas. For example, in 2013 the President requested that the UN develop a new global legal system to govern the Internet.

Brazil's own Internet architecture is still in progress. While there have been some important developments, there are conflicting lines of accountability among institutions, distorted funding priorities, confused public debate, contradictory legislative measures and the importation of outside solutions for local challenges. In the meantime, the military has "captured" resources for cyber defense, with potentially dangerous implications for civil liberties more generally.

What is more, the comparatively limited engagement of civil society in cyber security debates in Brazil means that the armed forces have free reign to advance their interests.

Military, law enforcement and civilian entities may exaggerate risks in order to increase their likely access to resources. If Brazil is to build a cyber security system fit for



purpose, an informed debate is imperative. At a minimum, Brazilians need to better understand the dynamics of cyber crime groups, and the ways in which traditional crime is migrating online. It also needs to monitor how security forces are adapting new

surveillance technologies. Above all, the government should encourage a broader debate with a clear communications strategy about the need for cyber security and what forms this might take.

**EDITOR'S COMMENT:** Interesting! Cyber defense goes to military. CBRNE defense goes to military. What is next towards Rio 2016?



## Rumor-detection software detects, corrects erroneous claims on Twitter

Source: <http://www.homelandsecuritynewswire.com/dr20150601-rumordetection-software-detects-corrects-erroneous-claims-on-twitter>

June 01 – A week after the Boston marathon bombing, hackers sent a bogus tweet from the official Twitter handle of the Associated Press. It read: “Breaking: Two Explosions in the White House and Barack Obama is injured.”

Before the AP and White House could correct the record, the stock market responded, dropping more than 140 points in a matter of minutes. Losses mounted into the billions.

The market recovered just as quickly, but analysts said the timeframe could well have been long enough for in-the-know perpetrators to profit through trading.

Rumors and their negative effects can spread rapidly in these hyperconnected times, says Qiaozhu Mei, an associate professor in the **University of Michigan School of Information and Department of Electrical Engineering and Computer Science.**

A U-M release reports that this is why he and a team of researchers have developed software to help society identify and correct erroneous claims on Twitter. They introduced the software recently at the International World Wide Web Conference in Florence, Italy. Later this summer, they hope to put it in practice at a website they're developing called **Rumor Lens.**

“One post of a rumor in social media can sometimes spread beyond anyone’s control,” said Mei, an expert on text mining and natural language processing. “Our goal is to detect emerging rumors as quickly as possible.”

The team demonstrated what its software is capable of by analyzing two sets of tweets: thirty million sent relating to the Boston Marathon bombing in April 2013 and a random sample of 1.2 billion tweets sent during November of the same year.

They gathered the second set from Twitter’s Gardenhose — 10 percent of its real-time stream. The datasets represent both an unpredictable, high-profile event that would likely spawn rumors and a relatively uneventful span of time.

The software successfully detected 110 rumors from the stream of tweets about the Boston Marathon bombing, with an average accuracy of more than 50 percent. Its average accuracy was 33 percent for Twitter Gardenhose data.

Both percentages are significantly higher than the less-than-10-percent accuracy of rumor-detecting through hashtag tracking and trending topics, the researchers point out. Furthermore, their software finds fishy statements a lot faster.

“Our method can detect rumors 3.6 hours earlier than methods that use trending topic detection, and 2.8 hours earlier than methods using hashtags as signals,” said Zhe Zhao, a doctoral student in the Department of Electrical Engineering and Computer Science.

The researchers’ key insight is that before social media users decide whether to believe a piece of information is true, many will ask for more information or express skepticism. So they designed their software to listen in on Twitter traffic for signs that users are “questioning the truth value of information.” Words and phrases the program has an ear for include “unconfirmed,” “Is this true?” and “Really?”

Once it zeroes in on a potential rumor, it looks for more tweets about the topic to gauge how widespread the conversation is. The researchers then rely on humans to fact-check.



The point of the effort isn't for a computer to determine whether a claim is true or false, but rather to highlight disputed information before it ends up on popular debunking sites like Snopes.com.

"By the time a rumor gets to Snopes, it's often too late," Mei said.

The release notes that Rumor Lens — the researchers' own Web site — is expected to be available in the next couple of months. The team envisions it serving as a Snopes-like online community of social media observers, academics and reporters who have an interest

in following and debunking rumors. The algorithms would highlight potential rumors and the people in the community would do the fact-checking. The researchers define a rumor as a controversial statement that can be fact-checked.

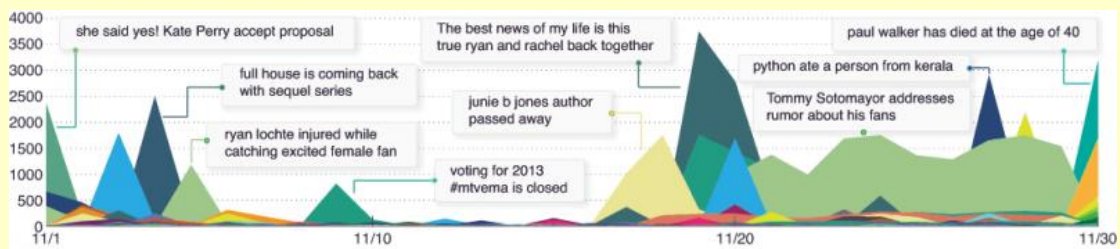
The team presented a paper about the research at the World Wide Web Conference. Paul Resnick, a professor in the School of Information, is also a co-author. The work is supported in part by the National Science Foundation and the Defense Advanced Research Projects Agency.



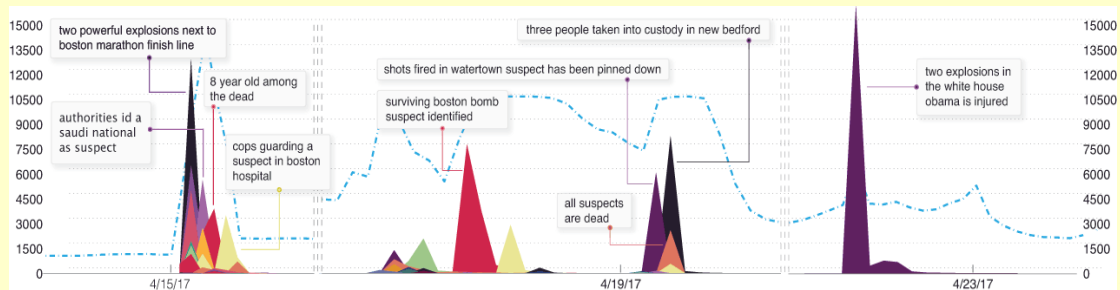
One minute after the hacked twitter account sent out a rumor of explosions at the White House, users were already inquiring about its accuracy. Blue nodes show inquiry tweets. Yellow represent correcting tweets. Red represent spreading tweets. Image credit: Zhe Zhao



Two seconds after the first denial from an AP employee and two minutes before the official denial from AP, the rumor had already gone viral. Red represents the rumor spreading. Blue shows questioning tweets and yellow nodes are correcting tweets. Image credit: Zhe Zhao



Tracking rumors on Twitter during November, 2013, a relatively uneventful period. Image credit: Zhe Zhao



Tracking rumors on Twitter about the Boston marathon bombing. Image credit: Zhe Zhao



— Read more in Zhe Zhao et al., “*Enquiring Minds: Early Detection of Rumors in Social Media from Enquiry Posts*” (paper presented at the International World Wide Web Conference Committee [IW3C2], 18-22 May 2015, Florence, Italy)

**BOOK REVIEW: ‘Terrorism in Cyberspace: The Next Generation’**

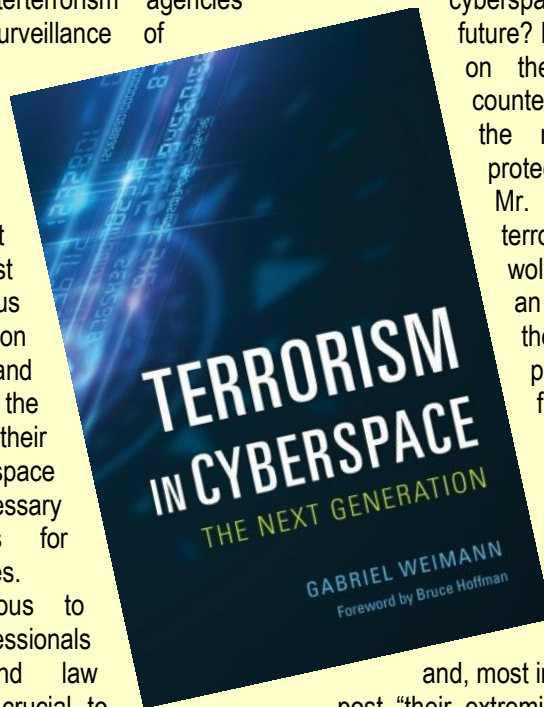
**Author:** Gabriel Weimann

Woodrow Wilson Center Press/Columbia University Press, \$90, \$30 (paper) 296 pages

**By** Joshua Sinai

Source: <http://www.washingtontimes.com/news/2015/jun/1/book-review-terrorism-in-cyberspace-the-next-gener/>

In the United States, Canada and Western Europe, dozens of al Qaeda, al-Shabab- and ISIS-related terrorist plots have been thwarted by government counterterrorism agencies through electronic surveillance of terrorist operatives’ suspicious activities on the Internet. While their activities were likely also monitored “on the ground,” the fact that terrorists of all extremist ideological and religious types are so reliant on using their computers and smartphones to access the Internet for their communications, cyberspace has become a necessary focus of operations for counterterrorism agencies. Because it is obvious to counterterrorism professionals from intelligence and law enforcement that it is crucial to electronically monitor such suspicious activities (with full legal compliance), it is somewhat surprising to see the current controversy in the United States Congress over reauthorization of electronic surveillance operations under the Patriot Act. For this reason, among others, we are fortunate to have Gabriel Weimann’s “Terrorism in Cyberspace: The Next Generation,” an authoritative account of the ways in which terrorists operate in cyberspace, the components of effective countermeasures, and the issues involved in balancing security with civil liberties. Mr. Weimann, whom I know, is professor of communications at the University of Haifa, Israel, where he leads a research program that tracks terrorist activities on the Internet, and is the author of a landmark book on this topic that was published in 2006.



**In his new book, Mr. Weimann addresses the following questions:** How are terrorists exploiting the Internet? What new trends in cyberspace can be expected in the future? How can terrorist operations on the Internet be effectively countered? How can we balance the need for security while protecting civil liberties?

Mr. Weimann explains that terrorist groups — and lone wolves — view the Internet as an ideal arena to exploit for their communications, propaganda, training, fundraising, and mobilizing support for their violent activities because of its ease of access from anywhere around the world, “lack of regulation, vast potential audiences, fast flow of information,” and, most importantly, the anonymity to post “their extremist beliefs and values” and then “disappear into the dark.” They exploit the Internet’s websites, email, chat rooms, virtual message boards, mobile phones, Google Earth, YouTube and other online video sharing sites, as well as social networking sites such as Facebook and Twitter. Such exploitation, however, is not being conducted openly, as their tech-savvy operatives often use encryption tools and anonymizing software to make it difficult for counterterrorism agencies to identify “the originator, recipient, or content of terrorist online communications.”

**Mr. Weimann identifies three new trends in Internet exploitation: narrowcasting (targeting propaganda and recruitment messaging to narrow audiences that are deemed to be especially**





susceptible, such as children, women, lone wolves, and diaspora communities), encouraging the proliferation of lone wolf adherents, such as Major Nidal Hassan, and advancing cyberterrorism.

The proliferation of lone wolves is especially worrisome, according to Mr. Weimann, because “they are extremely difficult to detect and to defend against.” Nevertheless, they are detectable to counterterrorism agencies because they must still “connect, communicate, and share information, know-how, and guidance — all online — on the ‘dark web.’”

Cyberterrorism is the most threatening of the trends, according to Mr. Weimann, because terrorists would be able to use their “computer network devices to sabotage critical national infrastructures such as energy, transportation, or government operations.” Mr. Weimann warns that terrorists are keen to develop a cyberwarfare capability, with the possibility of “money, ideology, religion, and blackmail” being used to recruit such “cybersavvy specialists” in the future.

How can terrorist exploitation of cyberspace be countered and defeated? While the Internet and its online platforms, as Mr. Weimann points out, provide terrorists with “anonymity, low barriers to publication, and low costs of publishing and managing content,” at the same time they also provide counterterrorism

agencies with the capability to damage and block them. Under what Mr. Weimann terms the “MUD” model (monitoring, using, and disrupting), he recommends covertly tracking their activities in order to gain information about their strategies, motivations, internal debates and associations, while disrupting them with ‘hard’ power cyber-weapons to spread viruses and worms against their websites. These would be accompanied by ‘soft’ power elements that conduct psychological operations to discredit their extremist propaganda and offer constructive alternatives to resorting to terrorism

In light of the current controversies over reauthorizing the provisions of the Patriot Act, the book’s final chapter, “Challenging Civil Liberties,” is particularly valuable in discussing the challenges presented by the need to preserve civil liberties when countering online terrorist activities. He cites the impact of Edward Snowden’s illicit revelations of the U.S. government’s counter-online surveillance measures and proposes a set of guidelines to regulate governmental online surveillance.

**“Terrorism in Cyberspace” is a timely and indispensable resource for all those concerned about effectively countering terrorists’ exploitation of the Internet’s and the dark elements that can reside there.**

49

*Joshua Sinai is director of analytics and business intelligence at the Resilient Corporation, in Alexandria, Va.*

## Can the power grid survive a cyberattack?

By Michael McElfresh

Source: <http://www.homelandsecuritynewswire.com/dr20150610-can-the-power-grid-survive-a-cyberattack>

In a 2012 report, the National Academy of Sciences called for more research to make the grid more resilient to attack and for utilities to modernize their systems to make them safer. Indeed, as society becomes increasingly reliant on the power grid and an array of devices are connected to the internet, security and protection must be a high priority.

It is very hard to overstate how important the U.S. power grid is to American society and its economy. Every critical infrastructure, from communications to water, is built on it and every important business function from banking to milking cows is completely dependent on it.

And the dependence on the grid continues to grow as more machines, including equipment on the power grid, get connected to the Internet. A report last year prepared for the president and Congress emphasized the vulnerability of the grid to a long-term power outage, saying “For those who would seek to do our Nation significant physical, economic, and psychological harm, the electrical grid is an obvious target.”

The damage to modern society from an extended power outage can be dramatic, as millions of people found in the wake of Hurricane Sandy in 2012. The Department



of Energy earlier this year said cybersecurity was one of the top challenges facing the power grid, which is exacerbated by the interdependence between the grid and water, telecommunications, transportation, and emergency response systems.

So what are modern grid-dependent societies up against? Can power grids survive a major attack? What are the biggest threats today?

The grid's vulnerability to nature and physical damage by man, including a sniper attack in a California substation in 2013, has been repeatedly demonstrated. But it is the threat of cyberattack that keeps many of the most serious people up at night, including the U.S. Department of Defense.

#### **Why the grid so vulnerable to cyberattack**

Grid operation depends on control systems — called Supervisory Control And Data Acquisition (SCADA) — that monitor and control the physical infrastructure. At the heart of these SCADA systems are specialized computers known as programmable logic controllers (PLCs). Initially developed by the automobile industry, PLCs are now ubiquitous in manufacturing, the power grid and other areas of critical infrastructure, as well as various areas of technology, especially where systems are automated and remotely controlled.

One of the most well-known industrial cyberattacks involved these PLCs: the attack, discovered in 2010, on the centrifuges the Iranians were using to enrich uranium. The Stuxnet computer worm, a type of malware categorized as an Advanced Persistent Threat (APT), targeted the Siemens SIMATIC WinCC SCADA system.

Stuxnet was able to take over the PLCs controlling the centrifuges, reprogramming them in order to speed up the centrifuges, leading to the destruction of many, and yet displaying a normal operating speed in order to trick the centrifuge operators. So these new forms of malware can not only shut things down but can alter their function and permanently damage industrial equipment. This was also demonstrated at the now famous Aurora experiment at Idaho National Lab in 2007.

Securely upgrading PLC software and securely reprogramming PLCs has long been of concern to PLC manufacturers, which have to contend

with malware and other efforts to defeat encrypted networks.

The oft-cited solution of an air-gap between critical systems, or physically isolating a secure network from the internet, was precisely what the Stuxnet worm was designed to defeat. The worm was specifically created to hunt for predetermined network pathways, such as someone using a thumb drive, which would allow the malware to move from an internet-connected system to the critical system on the other side of the air-gap.

#### **Internet of many things**

The growth of smart grid — the idea of overlaying computing and communications to the power grid — has created many more access points for penetrating into the grid computer systems. Currently knowing the provenance of data from smart grid devices is limiting what is known about who is really sending the data and whether that data is legitimate or an attempted attack.

This concern is growing even faster with the Internet of Things (IoT), because there are many different types of sensors proliferating in unimaginable numbers. How do you know when the message from a sensor is legitimate or part of a coordinated attack? A system attack could be disguised as something as simple as a large number of apparent customers lowering their thermostat settings in a short period on a peak hot day.

Defending the power grid as a whole is challenging from an organizational point of view. There are about 3,200 utilities, all of which operate a portion of the electricity grid, but most of these individual networks are interconnected.

The U.S. government has set up numerous efforts to help protect the United States from cyberattacks. With regard to the grid specifically, there is the Department of Energy's Cybersecurity Risk Information Sharing Program (CRISP) and the Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC) programs in which utilities voluntarily share information that allows patterns and methods of potential attackers to be identified and securely shared.

On the technology side, the National Institutes for Standards and Technology (NIST) and IEEE are working on smart grid and



other new technology standards that have a strong focus on security. Various government agencies also sponsor research into understanding the attack modes of malware and better ways to protect systems.

But the gravity of the situation really comes to the forefront when you realize that the Department of Defense has stood up a new command to address cyberthreats, the U.S. Cyber Command (USCYBERCOM). Now in addition to land, sea, air, and space, there is a fifth command: cyber.

The latest version of the Department of Defense's Cyber Strategy has as its third strategic goal, "Be prepared to defend the US

homeland and US vital interests from disruptive or destructive cyberattacks of significant consequence."

There is already a well-established theater of operations where significant, destructive cyberattacks against SCADA systems have taken place.

In a 2012 report, the National Academy of Sciences called for more research to make the grid more resilient to attack and for utilities to modernize their systems to make them safer. Indeed, as society becomes increasingly reliant on the power grid and an array of devices are connected to the internet, security and protection must be a high priority.

*Michael McElfresh is Adjunct Professor of Electrical Engineering at Santa Clara University.*

## Hackers Possibly Gaining in Cyber Attacks

Source: <http://www.voanews.com/content/study-finds-hackers-possibly-gaining-in-cyber-attacks-/2815922.html>

June 10 – A study released Wednesday suggests that despite the growing time and resources companies spend on cybersecurity, they're at best keeping even with the hackers and may in fact be losing ground.

Hackers, the study said, are becoming more skillful and their tools more effective, and the market for their stolen information is flourishing.

The study, conducted by the RAND Corporation, was based on extensive interviews with 18 chief information security officers or CISOs — traditionally the top cybersecurity position in corporate organizations — as well as a review of current cybersecurity products on the market.

The authors of the study, "[The Defender's Dilemma: Charting a Course Toward Cybersecurity](#)," conclude that worldwide corporate spending on cybersecurity now nears \$70 billion annually and is on track to grow at a rate of 10 percent or more each year.

Despite that investment, report authors say, CISOs are relatively pessimistic about their battle against cyberattacks and believe that hackers may in fact gain the upper hand in a matter of a few years.

That last finding was among several that report authors suspected even before the study was

conducted. Other initial preconceptions that were confirmed were that larger businesses often had more options for strengthening cybersecurity than smaller ones, and that walling off specific parts of corporate computer systems from the Internet can help guard against attack.

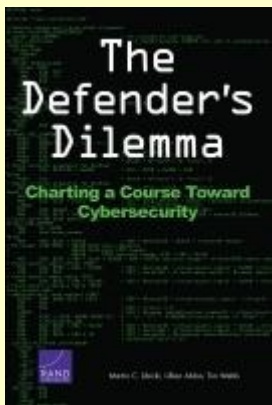
### Reputation

Among the more surprising findings for the report authors was that CISOs often view the greatest damage caused by cyberattacks to be on a corporation's reputation, rather than the actual stolen data or intellectual property.

"The bedrock of cybersecurity is good system software," the authors wrote. "Companies often find themselves having to invest in defensive measures because foundational systems and software are unsecure. The security and solidness of the actual software helps to prevent attackers from gaining a foothold on a network."

The report said that recent high-profile data breaches at Sony Pictures Entertainment, Anthem Insurance and many other private firms have paradoxically strengthened corporations' cybersecurity posture, because corporate boards are taking the issue much more seriously.

"Core software is improving, and cybersecurity products are burgeoning," the authors write.



"The combination is likely to make the attacker's task more difficult and more expensive — which will not solve the problem, but will make it more manageable."

Several recent studies have shown that many companies are more worried about the damage to their reputations from cyber attacks than the actual loss of intellectual property or other valuable information.

A previous study by the Ponemon Institute says the most costly cyber crimes include attacks by malicious insiders and "denial of service" attacks that overwhelm a firm's computer systems. The Ponemon study also says the longer such attacks continue, the more costly they become, with business disruption the largest expense.

Ponemon Institute founder Larry Ponemon said the problem of cyber attacks is huge and getting worse at an "exponential" rate. In a VOA interview, he said such attacks had

already put some small and medium-size companies out of business, and that it was "just a matter of time" before a large firm, like Target, is closed by cyber issues.

A separate report Tuesday from the Standard & Poor's rating agency says global business losses from cyber attacks may run as high as \$400 billion per year.

S&P says it evaluates how management handles all risks, including this complex and growing one, as it determines credit ratings. The rating agency says some insurance companies offer protection for financial losses due to cyber attacks, but that the field is so "fluid" and unpredictable that insurers are having difficulty judging how to evaluate risk and price their products.

Ponemon said insurance protection against cyber attacks is getting better but has a "long way to go."

## Key Findings

### Common Knowledge Confirmed

- Security postures are highly specific to company type, size, etc.; and there often aren't good solutions for smaller businesses.
- Quarantining certain parts of an organization offline can be a useful option.
- Responding to the desire of employees to bring their own devices and connect them to the network creates growing dilemmas.
- Chief information security officers (CISOs) feel that attackers have the upper hand, and will continue to have it.

### Reasonable Suppositions Validated

- Customers look to extant tools for solutions even though they do not necessarily know what they need and are certain no magic wand exists.
- CISOs want information on the motives and methods of specific attackers, but there is no consensus on how such information could be used.
- Current cyberinsurance offerings are often seen as more hassle than benefit, only useful in specific scenarios, and providing little return.

### Surprising Findings

- A cyberattack's effect on reputation (rather than more direct costs) is the biggest cause of concern for CISOs. The actual intellectual property or data that might be affected matters less than the fact that any intellectual property or data is at risk.
- In general, loss estimation processes are not particularly comprehensive.
- The ability to understand and articulate an organization's risk arising from network penetrations in a standard and consistent manner does not exist and will not exist for a long time.

*Doug Bernard covers cyber-issues for VOA, focusing on Internet privacy, security and censorship circumvention. Previously he edited VOA's "Digital Frontiers" blog, produced the "Daily Download" webcast and hosted "Talk to America", for which he won the International Presenter of the Year award from the Association for International Broadcasting. He began his career at Michigan Public Radio, and has contributed to "The New York Times," the "Christian Science Monitor," SPIN and NPR, among others.*



## The biggest heist of secret US personnel data in cyber history is still ongoing

Source: <http://www.debka.com/article/24666/The-biggest-heist-of-secret-US-personnel-data-in-cyber-history-is-still-ongoing->



June 12 – **The White House has admitted that systems containing deeply personal information, submitted by current, former and prospective federal government employees for security clearances, had been “exfiltrated.”** If the breach of the Office of Personnel Management (OPM)

was conducted by hackers linked to China, as suspected, access to the Standard Form 86 submitted by an estimated **41 million federal employees** provided them with what may be the world’s largest stolen data base of US intelligence and military personnel. This is a “gold mine” of unencrypted data that leave US intelligence officers, for example, open to blackmail or coerced recruitment. While officials speak of two hacks, debkafile’s cyber security and intelligence experts report that it was a single breach and is still ongoing. Known to experts as an “Advanced Persistent Threat,” it amounts to slow, continuous penetration by a computer virus, planted in an individual computer of a network which duplicates itself gradually and insidiously. Access may have been initiated by sowing particles of malicious code months or even years ago in the mega network of thousands of computers and terminals holding all the records of US federal employees. It could have happened when A OPM staff member surfed rogue Internet sites, opened a contaminated Word or Excel file – or even inserted a Memory Stick (Disk On Key).

The bad news is that it is not over and the damage may not be reversible. Not only was it discovered belatedly, but more of those malware particles are certainly buried inside communications and data bases serving OPM, waiting for a remote signal from the hackers’ command and control centers, which are believed to be working for China.

According to our experts, it is almost impossible to totally sanitize all the affected computers, servers, switches and other components. The only practical remedy would



be for the OPM to totally segregate its computers from the public Internet and severely restrict and supervise data transfers into the system’s different segments. This device would act like highway roadblocks that allow police officers to inspect each individual vehicle.

According to the information published by cyber intelligence magazines, the hackers got away with copies of every Standard Form 86 filed by US intelligence and security personnel and passed it on to an unknown destination.

This form lists mental illnesses, drug and alcohol use, past arrests and bankruptcies. Applicants are required to list contacts and relatives, potentially exposing any foreign relatives of US intelligence employees to coercion. Both the applicant’s Social Security number and that of his or her cohabitant are required, as well as driver’s license, passport and phone numbers. The hack made available to a foreign agency all the personal particulars including photos of every officer employed by US security agencies.

“Recent events underscore the need to accelerate the administration’s cyber strategy and confront aggressive, persistent malicious actors that continue to target our nation’s cyber infrastructure,” the White House statement said.

However, the global ramifications can’t be overlooked of a weapon that knows no borders. In February, the big US medical insurance firm Anthem reported that the administrative data of “only” 80 million clients were hacked. Smaller breaches may not be reported at all, but are believed to be taking place daily. In all, America’s government, health and financial infrastructure is under tremendous constant cyber attack.

China is believed to possess the biggest data base in the world, larger even than the US National Security Agency. Its super computers are operated and maintained by thousands of staff around the



clock, their data bases constantly supplemented by information hacked from

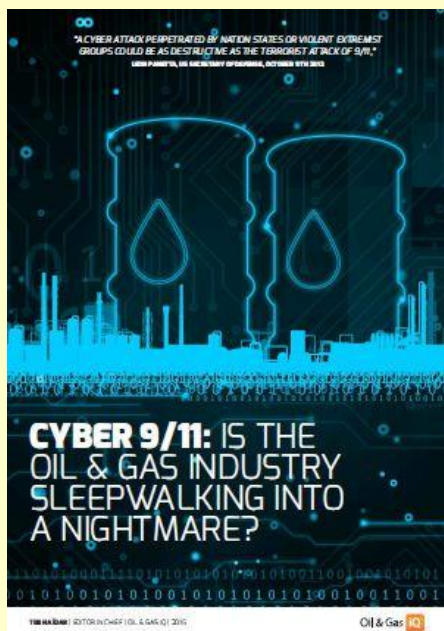
every US institution, public or private.

## Cyber 9/11: Is The Oil & Gas Industry Sleepwalking Into A Nightmare?

Source: <http://www.oilandgasiq.com/strategy-management-and-information/white-papers/cyber-9-11-is-the-oil-gas-industry-sleepwalking-in/>

*"A cyber attack perpetrated by nation states or violent extremist groups could be as destructive as the terrorist attack of 9/11,"*

*Leon Panetta, US Secretary Of Defense, October 11th 2012*



Cyber Security within the oil and gas industry is a threat that is, in many cases, being ignored. It has a direct effect in the creation of government regulation and legislation, can have deep financial impact and – in some cases – can even cost lives.

The 2014 Verizon Data Breach report states that 40 per cent of the attacks performed in the manufacturing and mining industry are cyber espionage based. **A UK survey revealed that 81 per cent of large companies were digitally attacked, at an average cost of £1 million per company. Similarly, 62 per cent of small and medium-sized enterprises (SMEs) were digitally attacked in 2014 at an average cost of more than £100,000 per incident.**

Cyber 9-11 is coming, and it's a "when" and not "if" scenario. It is debatable whether anybody can be totally prepared for an event of such magnitude, but our research has shown that the oil and gas industry is unfortunately often unprepared in its basic prevention and mitigation abilities.

54

► You can freely download this report from source's URL.

## State Department stays away from Chinese-owned Waldorf Astoria

Source: <http://www.homelandsecuritynewswire.com/dr20150619-state-department-stays-away-from-chineseowned-waldorf-astoria>

June 19 – **The U.S. State Department said American diplomats and State Department officials, for the first time in decades, would not be staying at New York's Waldorf-Astoria hotel during this year's UN general assembly.**

The State Department gave no reason for the decision, but the writing was on the wall since Hilton Worldwide last year sold the high-end Midtown hotel for \$1.95 billion to the Chinese group Anbang Insurance Group. The sales

contract allowed for "a major renovation" by the Chinese, and American security experts had no doubt as to the purpose of these "renovations": As is the practice in China, the Chinese owners, working on behalf of China's intelligence services, were going to plant listening devices in every room and ball room, and wire every phone, Wi-Fi hot spot, and restaurant table in order to eavesdrop on hotel guests.



Foreign diplomats also preferred to stay at the Waldorf while in New York, and they, too, will



likely look for another place now.

The *International Business Times* reports that the switch to the New York Palace Hotel will affect hundreds of American diplomats and support staff who travel to New York for the General Assembly each September and stay at the Waldorf.

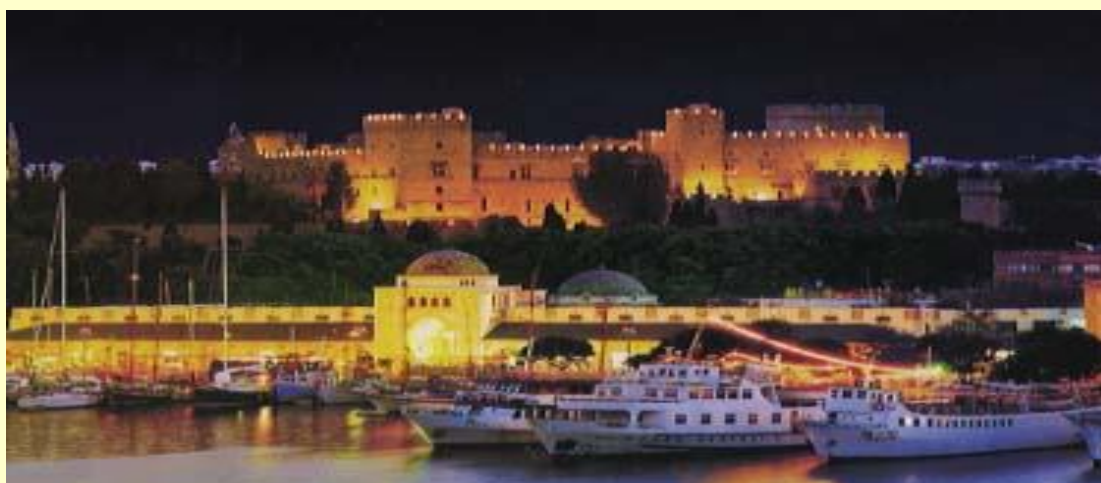
U.S. diplomats and American businessmen traveling to China are routinely warned by the State Department about the Chinese physical and electronic surveillance capabilities, and about the fact that many hotel rooms in China are wired by the Chinese intelligence services. "Hotel rooms (including meeting rooms), offices, cars, taxis, telephones, Internet usage and fax machines may be monitored onsite or remotely, and personal possessions in hotel

rooms, including computers, may be searched without your consent or knowledge," the department says in its warning to travelers to China. "Business travelers should be particularly mindful that trade secrets, negotiating positions and other business-sensitive information may be taken and shared with local interests."

Adam Segal, a China and cybersecurity expert at the Council on Foreign Relations, told the *Guardian* that the

Waldorf-Astoria's ownership did not necessarily indicate that it was or was not subject to surveillance. Segal said that the sale of the Waldorf-Astoria to Anbang Insurance Group gave U.S. officials a sense that there were greater chances for spying, but actually hacks had little to do with who owns a particular building. Segal said moving their location to the Palace Hotel "may provide the perception of greater security, but not any guarantee of it."

"Because the Chinese have made so many cyberattacks and eavesdropping against the United States, it's very prudent for the United States to make sure that all these important bilateral meetings with heads of state don't take place where they're going to be transmitted to China," foreign affairs analyst Pamela Falk told CBS New York.



Greece – Rhodes Island



## Robots to the rescue in disaster situations

Source: <http://www.homelandsecuritynewswire.com/dr20150526-robots-to-the-rescue-in-disaster-situations>



May 26 – Real-life disaster scenarios have awakened the robotics community to the limitations of existing emergency-response robots. This edition of *CORDIS Express* highlights the EU-funded researchers who are redoubling efforts to ensure that disaster response robots can better support rescue workers in future emergencies.

Research in the lab and on-site simulations have helped in improving the capabilities of

like robot. This robot is capable of robust locomotion and dexterous manipulation in the rough terrain and austere conditions characteristic of disasters. The TRADR project team, meanwhile, is focusing on developing novel science and technology for human-robot teams to assist in disaster response efforts over multiple missions.

These and other project teams may take interest in the EURATHLON project which is



56

emergency-response robots in recent years. *CORDIS* notes that when real disaster strikes unexpected, however, complications lay bare the limitations of test scenarios. In light of the lessons learned following the Fukushima nuclear accident, EU-funded researchers are following a range of different pathways to advance emergency-response robotics.

The CENTAURO project (photo left below), for example, is developing a human-robot symbiotic system in which a human operator is tele-present with its whole body in a Centaur-

supporting and encouraging the robotics community through its outdoor robotics competition, and which invites teams to test their robots in realistic mock emergency-response scenarios. The final EURATHLON competition will require a team of terrestrial, marine, and aerial robots to work collaboratively to survey a disaster scene, collect environmental data and identify critical hazards. This EURATHLON 2015 Grand Challenge will take place from 17 to 25 September 2015.

This week's edition of *CORDIS Express* takes a look at these and other projects and stories that focus on emergency-response robotics:

- [Long-Term Human-Robot Teaming for Robot-Assisted Disaster Response](#)
- [WALK-MAN sets the bar high for DARPA's Robotics Challenge Finals](#)





- [Support Action for a Targeted Intelligent Autonomous Robotics Contest: The European Roboathon](#)
- [Robust Mobility and Dexterous Manipulation in Disaster Response by Fullbody Telepresence in a Centaur-like Robot](#)
- [Trending Science: Three European teams demonstrate progress in emergency response robotics since Fukushima disaster](#)
- [TIRAMISU demonstrates new demining tools in Brussels](#)

## Operational Lessons Learned in Disaster Response

Source: [http://www.usfa.fema.gov/downloads/pdf/publications/operational\\_lessons\\_learned\\_in\\_disaster\\_response.pdf](http://www.usfa.fema.gov/downloads/pdf/publications/operational_lessons_learned_in_disaster_response.pdf)

This report follows extensive research by the U.S. Fire Administration (USFA) of after action reviews from major disasters of the past decade into lessons learned. The disasters studied were weather-related events that required responding firefighters to assume duties for which they were unprepared or for situations they never anticipated.

The relative frequency and severity of extreme weather events and their consequent impact on the U.S. population provide ample reason to study what other responders have experienced and what they could or could not do in the face of such challenges. While after action reviews produce valuable lessons, lessons alone are not the end of the story. In fact, lessons learned should rightly be the beginning of a new chapter in a fire department's operational behaviors. Lessons without a corresponding change in operational behavior are not lessons learned.

This report encompasses and updates the information from two existing USFA publications, "TR-162: Fire Department Preparation for Extreme Weather" and "TR-159: After Action Reports — Lessons Learned." The USFA acknowledges the effort of the individuals responsible for producing those legacy works. The updated content from those two publications is coupled in this report with a stronger focus on learning from lessons

learned.

The lessons learned by first responders and emergency managers in the April 2011 tornado outbreak in the southeastern United States provides a rich resource for the fire service to study and apply. Research for this report relied heavily on USFA's publication, "Fire Service Operations for the Southeastern Tornadoes — April 2011," for operational lessons learned from that event.

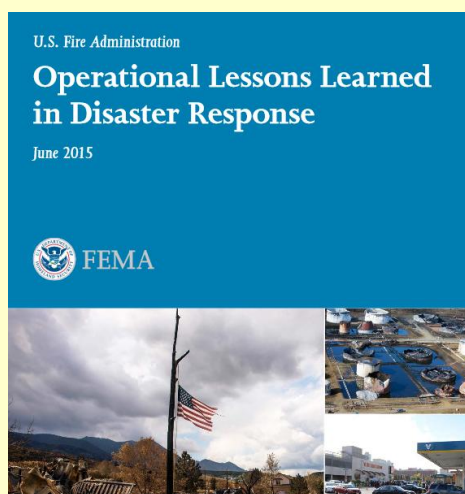
In the process of researching lessons learned in disaster response, it readily became apparent that while we have plenty of lessons learned there is a gap in applying those lessons to disaster response and recovery operations. The material here on applying lessons learned references the research work of Amy K. Donahue and Robert V. Tuohy. Their extensive interviews with Incident Commanders (ICs) as reported in "Lessons We Don't Learn: A Study of the Lessons of Disasters, Why We Repeat Them, and How We Can Learn Them" is published in Homeland Security Affairs, Vol. II, No. 2, July 2006.

## How to Change Response Tactics in Times of Civil Unrest

By Michael E. Cox Jr.

Source: [http://www.domesticpreparedness.com/First\\_Responder/Fire\\_HAZMAT/How\\_to\\_Change\\_Response\\_Tactics\\_in\\_Times\\_of\\_Civil\\_Unrest/](http://www.domesticpreparedness.com/First_Responder/Fire_HAZMAT/How_to_Change_Response_Tactics_in_Times_of_Civil_Unrest/)

**Unlike responses to hurricanes, floods, or other natural hazards, civil disturbances are more likely to place emergency responders in harm's way as the situation rapidly and unpredictably changes. To avoid becoming a target for angry crowds with projectiles and gunfire, personnel within the area of active fighting or unrest must be able to make decisions and triage incidents without hesitation.**



Civil disturbances have been defined by the U.S. Department of Defense as: group acts of violence or disorder that are prejudicial to the public law and order. Civil disturbances typically take on one of two categories: (a) simple disobedience for the law; or (b) uncontrolled anarchy and rioting. There are numerous reasons for civil disobedience, which include: unruly fans at concerts or sporting events; unpopular decisions within college communities; different types of public protest/celebrations gone bad; unpopular court verdicts; out-of-favor political decisions; and recently the negative perception of law enforcement interactions by some citizens within communities.

Regardless of the reason, civil disturbances are not limited to a single particular area and have been known to occur from coast to coast in urban, suburban, and rural areas. All emergency response agencies must be prepared for this type of incident and be aware that civil disturbances may create situations whereby, emergency responders must function in a modified response mode in order to better ensure safe and efficient operations. At times, this may create confusion for response agencies that are not prepared, as these incidents require a change in tactics from the normal day-to-day operational framework that fire and emergency medical systems (EMS) personnel are accustomed to working within.

### **Managing a Crisis – Hazard Planning & Communication**

In order to prepare and mitigate civil disturbance incidents successfully, fire/EMS response agencies need to implement some tried and tested initiatives. One of the first initiatives that must be employed is planning.

**Planning is a key component for all significant initiatives and starts long before an incident occurs.** This process should begin with the development of a hazard-specific annex or a section of the jurisdictions emergency operations plan/emergency management plan dedicated to civil disturbances. Civil disturbance incidents are labor intensive, usually involve multiple jurisdictions, and extend into multiple operational periods. These incidents also generate intense media coverage around the clock.

Planning for incidents include, but is not limited to: departmental call-backs, holdovers, up-staffing, automatic/mutual aid assistance from throughout the region and/or state, as well as the implementation of these plans through regular tabletop exercises. Planning continues at lower levels of the government through the development of policies or procedures in the fire, EMS, and law enforcement agencies; whereby, specific actions and steps are taken in the event such an incident occurs. By developing these policies and procedures in a tiered fashion, planners are able to address all types of civil disturbances, as well as any operational changes that may be implemented during an incident.

The plan also includes communications and an appropriate incident management structure. Incidents such as this require good

communications and a unified command structure. Open and clear lines of communication coupled with an effective unified command presence would enhance strategic decision making and overall command and control of the incident. In some cases, it may be beneficial to open all emergency operation centers (multiagency coordination centers) in both the affected jurisdiction and at the state level. Emergency operation centers in surrounding jurisdictions also may need to open with at least a skeleton crew. By opening these centers, personnel are better equipped to facilitate requests in a timely fashion, thus preventing delays in assistance or additional resources that may be needed.

### **Joining Forces – Area Command & Multijurisdictional Response**

Similarly, the National Incident Management System (NIMS) area command concept is an excellent way to manage incidents that are dispersed over large geographic areas and evolve over multiple operational periods. They are frequently used to manage multiple incidents within a particular geographical area competing for the same resources where large-scale coordination of the overall incident is conducted at a higher jurisdictional level.

Moreover, another resource that could aid jurisdictions that find themselves inundated with a civil disturbance incident that lasts for a long duration (more than two or three days) is local or regional incident management teams. These teams are a component of the NIMS and consist of highly trained personnel who are capable of managing large manmade or natural disasters.



They typically are called upon to allow agency administrators and key appointed/elected officials to remove themselves from the actual management of an incident, in order to provide decision making/support of an incident from a macro or jurisdictional level.

Response assignments using task forces is another initiative to be employed at civil disturbance incidents to improve responder safety. Task forces usually are assembled at pre-designated staging areas outside the immediate troubled area. They often are made up of two engines, one ladder truck, one battalion chief, and a compliment of law enforcement units. Likewise, task forces for EMS incidents may include: (a) an engine company, medical transport unit, medical supervisor, and law enforcement; or (b) multiple medical transport units, a medical supervisor, and law enforcement.

The key thing to remember is that there is safety in numbers, and no fire or EMS unit should be operating alone in a theater of operation involving civil disturbances. The task force concept was used successfully in California during the 1992 Los Angeles riots (following the acquittal of law enforcement officers in the Rodney King trial), as well as within numerous other jurisdictions across the country since that time.

#### **Enabling Decision Making Within the Hostile Area**

Another initiative to be implemented during civil disturbances is operational changes that increase situational awareness and responder safety. There is an old saying that "all politics are local," this also seems to hold true when it comes to the safety of responders. Personnel operating in a particular geographic area inside an area of rioting have firsthand knowledge of the citizens in the area and when things are about to turn bad. Fire/EMS responders should be made aware of what sparked these incidents and remain ever vigilant not to exacerbate or escalate the situation.

It is important to push decision making at an incident scene to the lowest levels, giving incident commanders on scene the ability to quickly retreat from a hostile area if necessary. Responders then could maintain an increased level of situational awareness by assigning one person on each call as a lookout or observer. These individuals warn and inform crew members or the incident commander of

pending safety issues with roaming crowds or bystanders at the scene. They also advise if law enforcement personnel are called away to another incident, thus leaving fire/EMS personnel to operate alone in a hostile area involving protesters and/or rioters.

Another method to help ensure safety of fire/EMS responders is to initiate the hit-and-run and swoop-in/swoop-out tactics during responses in areas of civil disturbances. These tactical considerations focus on preventing conflagrations and/or the removal of injured people from the area of active fighting or unrest. Fire suppression activities focus on preventing the spread of fire and protecting critical infrastructure. Defensive operations – for example, no interior firefighting, self-contained breathing apparatus usage, roof operations, or the laddering of structures – should be mandatory as these tactics allow fire/EMS personnel to become possible targets for projectiles or gunfire.

Operations instead should focus on quick a "knockdown" (or extinguishments) followed by a quick exit from the hazardous area. During EMS operations, crews should focus on rapid extrication/transportation from a troubled area. SWAT medics and armored personnel carriers may be needed to extricate critically injured victims on the frontlines, when it is unsafe for medical transport units to enter an active hostile area near the police lines. If personnel were not immediately able to enter the active riot area, casualty collection points outside the area would provide care for people who are injured.

#### **Triaging Incidents – Let It Burn**

Another initiative to be implemented during times of civil disturbance is dispatch/response changes. Changes in emergency dispatches allow jurisdictions to better manage the increased call volume typically seen with civil disturbances. Sending a reduced assignment such as a task-force response permits additional units to remain available or respond to the additional call volume they may experience. Likewise, call triaging allows car, dumpster, or rubbish fires that are not a threat to any structures or people continue to burn in lieu of handling higher priority calls where structures and or life-safety issues need to take precedence over such "nuisance" incidents. These fires can be



extinguished later after the higher priority calls have been mitigated and the area is safe to operate in.

Fire/EMS operations can present real challenges during times of civil unrest. Regardless of where or when these incidents occur, responder safety must remain the highest priority. Civil disturbances require fire/EMS organizations to function outside their normal comfort zones by making operational changes that enhance responder safety, protect critical infrastructures, manage risks,

ensure effective communications, and develop appropriate incident management structures. Preparations must begin long before these emergency-response incidents occur. Jurisdictions and/or organizations that fail to plan and respond to these events in an appropriate fashion run the risk of becoming overwhelmed by the magnitude of such incidents. This lack of preparation and response could translate into a higher number of casualties and the loss of critical infrastructure.

*Michael E. Cox Jr. is a 30-year veteran of the fire service and currently serves as a faculty member at the University of Maryland's Fire and Rescue Institute, where he works as a lecturer/section manager. He began his fire service career as a volunteer at age 16 in Anne Arundel County, Maryland. He joined the Anne Arundel County Fire Department as a career employee in 1988 and advanced through the ranks to become the 10th fire chief of Anne Arundel County, where he led a combination career/volunteer force of 1,400 personnel until his retirement in December 2014. He holds an associate's degree in emergency medical services from Anne Arundel Community College, a bachelor's degree in fire science from the University of Maryland, and a master's degree in executive fire service leadership from Grand Canyon University. He is a nationally registered emergency medical technician paramedic, a state-certified emergency services instructor, and a graduate of the National Fire Academy's Executive Fire Officer Program. The national Center for Public Safety Excellence also has designated him as a Chief Fire Officer.*

## Drones for emergency services

Source: <http://i-hls.com/2015/06/drones-for-emergencies/>

60



The emergency service of Ireland is currently researching the use of the remote-controlled aircraft, also known as "Quadcopters", for major incidents in what have been described as "interesting times ahead" for the service.

It is believed members of the fire brigade will soon receive training in how to use the craft.

The introduction of drones could offer a great opportunity to assess information from significant incidents and large-scale events, providing additional information to fire services.

While the use of drones has been supported for their ability to complete tasks more efficiently, concerns have also been raised over surveillance, safety and privacy issues.

Drones have already been introduced by fire authorities in Boston.

According to sUAS, the department decided to purchase the drones for operational purposes after they were successfully implemented by the Brewster Ambulance Service.

Dublin Fire Brigade confirmed on its Twitter account that it was researching the use of such drones here, in response to the report about the experience in Boston.

The Irish Aviation Authority (IAA) defines drones as "any aircraft and its associated elements, other than a balloon, kite or small aircraft which is intended to be operated with no pilot on board".

**In Ireland, small drones (under 20kg) can generally be used non-commercially if kept below 120 metres in altitude, within 500 metres from the operator and at least 150m away from anyone else or any "structure or vehicle".**



They cannot be used “over any assembly of persons”, in “densely populated” residential areas or near airports unless special permission is granted. The IAA also suggests that third party insurance be taken out when purchasing one.

Irish criminals have also exploited the technology, with one gang using the device to try to transport drugs into a prison last year.

The drone, valued at around €2,000 crash landed in an exercise yard in Wheatfield Prison last year.

## 76 Percent of North Dakota's First Responders Are Volunteers

Source: <http://www.emergencymgmt.com/disaster/76-Percent-North-Dakotas-First-Responders-Are-Volunteers.html>

Nancy Thompson, 32, teared up instantly at the memory.

The first responder knew a train had collided with a school bus in Larimore, N.D. She knew there might be injuries.

She and her husband — also a first responder and a firefighter — were among the first emergency personnel at the scene. The train conductor, engineer and a few homeowners who lived near the crash site were the only others present.

It was one of her worst nightmares come true, she said.

"It was chaos," she said.

But despite her initial shock, she had a job to do, she said. Thompson, who was four months pregnant at the time, had to pronounce the bus driver, Max Danner, 62, and Cassidy Sandstrom, 17, dead. A dozen other children, ages 5 to 16, were also injured in the crash. An investigation attributed the cause to driver error.

"We knew the parents and the kids, and I knew the bus driver personally from the school," she said.

Once she returned home, she hugged the first person she saw — fellow first responder Nichole Jorgenson, Thompson said.

This accident was extreme. But the ongoing stress of the job — especially after treating familiar faces — wears on first responders and leads to burnout, some responders said. Coupled with recruiting struggles, this poses a significant threat to a state that sees fewer volunteers.

**In 2011, 86 percent of emergency personnel were volunteers in North Dakota, according to a state rural emergency services report. Today, it's 76 percent, according to the state Department of Health.**

**Estimates of other states vary, with some officials saying 80 percent of emergency personnel volunteer nationwide.** In

Minnesota, about 60 percent of emergency personnel and paramedics volunteer for the state's ambulance services, according to a news report.

First responders often turn to each other or the North Dakota Critical Incident Stress Management program to work through stress, but the program often goes unused, said Kari Kuhn, an administrative support supervisor for CISM.

"First responders are used to doing what they need to do," she said. "They don't always consider themselves as needing help."

### Crisis team assistance

Crisis team members provide first responders with first-level counseling, Kuhn said.

The CISM team is volunteer-based, located across the state and consists of mental health workers, clergy and other emergency workers who meet with first responders and provide follow-up later if necessary. Members get paid mileage and meals for travel.

"A lot of times it's a one-time thing, and also to find out if (first responders) are seeking professional help," she said.

On average, the team responds to calls about three times a month. This doesn't necessarily reflect the need, though — first responders can be reluctant to ask for help, and the western part of the state is particularly silent, but "they're also really busy," Kuhn said.

Several who responded to the call in Larimore — an effort that included five from Altru Ambulance Service, local firefighters and other emergency personnel — debriefed with each other at the scene. It's unclear how many used the CISM team.

Finding volunteers for the state CISM team is tough, especially as the service isn't used every day. That makes it hard for newly trained personnel to feel comfortable in that role,



Kuhn said. The ability to offer training sessions depends on state and federal funding, and even the state crisis program doesn't receive automatic funding, she said.

"People don't necessarily think of those first responders as ones that need help, because there is no proof of the help — there is no way to measure effectiveness," she said. "But if they were all gone, what would people do? We need them out there. Not everybody wants to be in that job. It's a tough job."

### Someone to talk to

Dozens of emergency personnel from the area responded to the accident in Larimore.

Jorgenson, 31, was among them. She had arrived on the scene just as the last ambulance pulled out, and she assisted the injured and made sure the crew was physically and mentally OK, she said. The response was among the best they'd had, she said.

Jorgenson and Thompson, who live in Larimore, are among 10 to 15 active first responders in the area. They're also among a few who can offer advanced life support assistance.

As they talked to the Herald in March, U.S. Sen. Heidi Heitkamp, D-N.D., along with Alejandro Mayorkas, deputy secretary for the Department of Homeland Security, stood a few feet away. Speaking before several first responders at the fire hall, Mayorkas and Heitkamp wanted to hear about the challenges they face and asked for ideas on how to better serve the national emergency community.

First responders in Larimore frequently get calls from elderly residents, mostly regarding heart attacks or respiratory difficulties, Jorgenson said. But they must be ready for anything and be able to shut down their emotions in an instant — an ability that's part self-discipline and part personality trait—and that narrows the candidate pool. High stress, low pay and being constantly on-call can also make the job less appealing, they said.

"There are so many volunteer services around the state, some are closing their doors because they don't have enough volunteers," Jorgenson said.

But in Larimore, every emergency call comes from a familiar face. Jorgenson and Thompson know nearly every resident by address and feel like they're caring for family, which also makes their job more meaningful, they said.

Members of Jorgenson's family also hold emergency personnel positions, so "it's in her blood," she said.

"There's definitely tough aspects of it, but good aspects make up for it," she said.

Knowing they ease the fear or pain someone at a time of need is one of the most fulfilling parts of the job, they said. But sometimes, a simple act can make the biggest difference for first responders and the people they help.

"The best thing is having somebody say, 'Thank you for helping me through this,'" said Jorgenson. "Sometimes, somebody just wants someone to talk to."

## Orchestrated Emergency Response Doesn't Just Happen, It Takes Practice

By Jim McKay

Source: <http://www.emergencymgmt.com/training/Orchestrated-Emergency-Response-Doesnt-Just-Happen.html>

As emergency management evolves as a profession and grows in diversity, there's a blending of personalities, viewpoints and different structures that come to the fore. People will come from different backgrounds, experiences and professions and have different styles and perspectives. They can blend to become a healthy whole, said Nim Kidd, Texas Division of Emergency Management chief, in a keynote address at the 2015 National

Homeland Security Conference this week in San Antonio.

Kidd came from the fire service and acknowledged that his experience and style is different from others rising in the emergency management ranks from the military, law enforcement, health care and academia. None of those have the market cornered on the "right way" to do things, and there are advantages and disadvantages to how each



communicates and approaches situations. For instance, law enforcement isn't known for being the best at communicating information, for good reason and sometimes not so good. The military and fire service bring invaluable experience to the emergency management field, and what health care and academia lack in experience, they make up for in knowledge and information.

The key is to bring it all together as a whole. Kidd likened this to a sixth-grade concert he attended, where the participants practiced on their own for weeks or months but had not played together until the concert. It worked out because of the coordination brought about by the conductor and music was played. But in emergency management it's important for the orchestra to have practiced together or at least get a feel for who is who prior to an incident. It's been said a lot but it can't be overstated: It's important to develop relationships and understandings prior to a disaster and not during one.

Several speakers at the conference noted how, even now, attendees sit with those with whom they are familiar. Communication is improving but the term "turf war" still surfaces. That might always be the case, and if money for training continues to dwindle it's going to be even more crucial for stakeholders to reach out to one another. Sometimes, Kidd pointed out, those in emergency management and related fields can be their own worst enemy.

In another keynote, Edward Gabriel, principal deputy assistant secretary for preparedness and response for the U.S. Department of

Health and Human Services, winced when so few in the audience acknowledged having heard of his department's National Disaster Medical System Response Teams. These are local medical personnel, including doctors, nurses and EMTs, who volunteer beforehand to assemble during a disaster. The teams include:

- the Disaster Medical Assistance Team composed of medical personnel to give support during a disaster;
- Disaster Mortuary Operational Response Teams that help set up temporary morgue facilities, help with victim identification, etc.;
- International Medical Surgical Response Teams are federal employees used intermittently to assist during public health emergencies; and
- National Veterinary Response Teams that assist emergency responders with veterinary needs during and after a disaster.

Gabriel urged attendees to contact the response office to learn more about the program and sign up.

In a rather alarming general session, a panel of medical experts said it's a matter of time before the U.S. suffers through another pandemic and that we're not prepared to handle all the sick and the fallout from the situation, including the estimated 40 percent of those who would miss work for one reason or another. The lethal event could include causes like botulism, anthrax or H1N1, and wouldn't necessarily originate from a third-world country.

*Jim McKay is the editor of Emergency Management.*



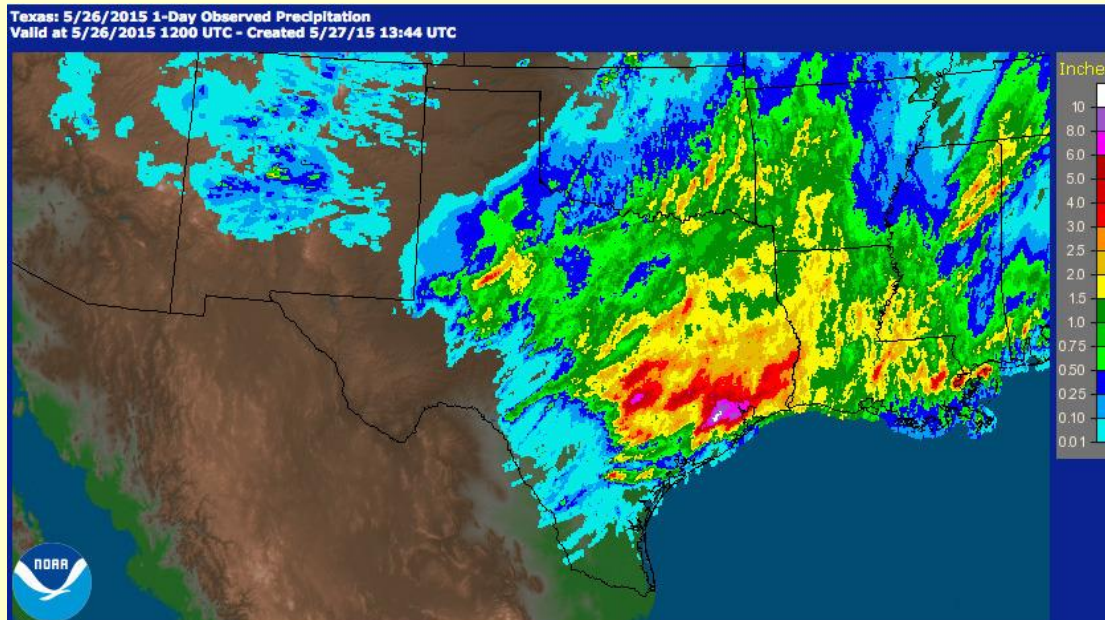
**Greece – Parthenon (Athens)**



## Climate change, a factor in Texas floods, largely ignored

By Neena Satija and Jim Malewitz

Source: <http://www.homelandsecuritynewswire.com/dr20150602-climate-change-a-factor-in-texas-floods-largely-ignored>



June 02 – Climate change is taking a toll on Texas, and the devastating floods that have killed at least fifteen people and left twelve others missing across the state are some of the best evidence yet of that phenomenon, state

George W. Bush in 2000. “And it’s consistent with what we would expect from climate change.”

But the state’s Republican leaders are deeply skeptical of the scientific consensus that human activity is changing the climate, with top environmental regulators in Texas questioning whether the planet is warming at all. And attempts by Democratic lawmakers during the 2015 legislative session to discuss the issue have come up short.

“In part, it’s ideologically driven and intellectually lazy,” said state Rep. Rafael Anchia (D-Dallas), who earlier this year invited national security experts to the state Capitol to testify at a hearing on the risks of climate change. “My question is: What are people scared of? Are they scared of the truth?”

climatologist John Nielsen-Gammon said in an interview last Wednesday.

“We have observed an increase of heavy rain events, at least in the South-Central United States, including Texas,” said Nielsen-Gammon, who was appointed by former Gov.

Asked about the role of climate change in the floods, U.S. Sen. Ted Cruz declined to weigh in Wednesday. “At a time of tragedy, I think it’s wrong to try to politicize a natural disaster,” the Republican presidential candidate





said during a news conference in San Marcos after surveying damage.

Extreme weather events, and more of them, are among the most agreed-upon effects of global warming in all the scientific literature on the subject, said Nielsen-Gammon, who is also a professor at Texas A&M University. Part of the explanation is that ocean temperatures are rising, bringing more moist air into the state that can create storm systems. In the past century, precipitation in Texas is up 7 to 10 percent, and the frequency of two-day heavy rainfall spells has nearly doubled.

The scientific consensus is much stronger on this point than on whether climate change can directly cause droughts. Nielsen-Gammon's own research has shown that warmer temperatures due to global warming did make the drought in Texas measurably worse than it otherwise would have been.

But for the last several years, legislation calling for climate-change studies has not succeeded in the Capitol. Two bills that Anchia proposed on the subject — one that creates a global task force to study climate change and another directing Texas to follow new federal climate regulations — didn't make it out of the committee he chairs. Two other pieces of legislation that would have directed state agencies to consider climate forecasts never received a public hearing.

The only climate-related bill that made it to the House floor would have required state agencies to include climate variability considerations in their strategic plans.

The International Trade and Intergovernmental Affairs Committee voted unanimously in support of the bill, and no one testified against it — though a number of industry and conservative groups registered in opposition.

When the bill reached the floor, it failed 84-47. There was no debate.

"It didn't even mention climate change. It was just about planning," Anchia said of the bill, which was authored by state Rep. Eric Johnson (D-Dallas).

Among the no votes was Republican Jason Villalba of Dallas, who said Wednesday he didn't recall voting against the bill.

Republican Todd Hunter of Corpus Christi also didn't remember his no vote. But he said that after this week's flooding, he's taking the need for planning for extreme weather seriously. "I'll certainly have it on my radar," Hunter said. "When you see these strange weather patterns, it's important to keep all of these things in mind."

Leigh Thompson, a policy analyst at the conservative Texas Public Policy Foundation who opposed the bill, called it "far too speculative." Thompson said the state doesn't have the means to project climate and water conditions twenty to fifty years from now and "predict these effects on all those different organizations."

But Nielsen-Gammon said there are definitely known impacts of global warming in Texas, and the state could be doing more with that knowledge. "We have the advantage of having non-zero information about how the climate's changing, and we're acting as though the information content is zero," he said.

While there's no way to ever be sure exactly when, where or how much rain will fall, Nielsen-Gammon pointed out that California state agencies are all incorporating climate change into their long-range planning.

"It certainly would be useful to know what we're getting into with climate change," he said. "Hopefully we can learn from California's experiences."

*Neena Satija covers the environment, and Jim Malewitz covers energy, for the Texas Tribune. Patrick Svitek contributed reporting.*

## Water security key to unlocking African prosperity

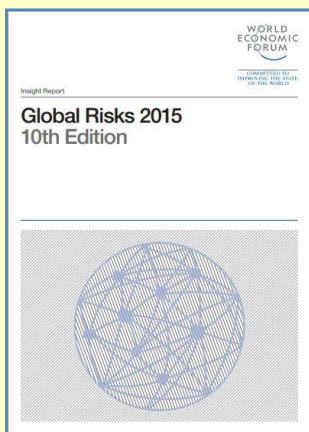
Source: <http://www.homelandsecuritynewswire.com/dr20150605-water-security-key-to-unlocking-african-prosperity>

June 05 – With coordinated action, better water provision in Africa will strengthen economic growth and unlock the path to prosperity for millions, according to SABMiller's Chief Executive Alan Clark.

Speaking today at the World Economic Forum (WEF) on Africa in Cape Town, Clark highlighted that water security and resource efficiency have become and will remain a



priority for SABMiller in Africa as climate change exacerbates competition for resources. **This year's WEF Global Risks Report ranked water scarcity as the biggest single risk to societies and economies.**



While growing production volumes, SABMiller has cut its global carbon emissions by 35 percent since 2008, reducing absolute emissions by nearly one million tons. Over the same period it cut water use per liter of beer by 28 percent, now

using 3.3 liters of water to make one liter of beer, exceeding its 2015 target. In the last year alone, the company reduced its water use by twenty-nine million hectoliters — the equivalent to the water used by over 116,000 Africans each year.



SAB Miller says that this has translated into tangible gains for the company — SABMiller saved \$117million in the last financial year compared with 2010 through water and energy related initiatives as a key part of its overall cost reduction plans.

Leading a panel discussion on the Future of Water, Alan Clark said:

“The business case for conserving water both within our own operations and in the communities where we work is clear and compelling. Companies from all sectors are facing up to the risks that water scarcity poses to their business — even more so with the impact of climate change. Now is the time to

step up and make clear commitments to reduce overall water use and improve efficiency.”

He also stressed that companies need to look beyond their operations if they want to effect real change:

“There has been progress on water in Africa but it is neither universal, nor consistent. Hundreds of millions of people in Africa, especially in rural and poor households, lack access to safe drinking water. Tackling water scarcity can release untapped prosperity at every level — not just for business, but for communities, societies and national economies. Yet businesses are still too focused on their own operations – only by working with local partners and communities will they bring about real change.”

SABMiller says that in providing both financial and operational support, it is a leading contributor to the Strategic Water Partners Network, a partnership between the South African government and private sector. It aims to close the gap between water supply and demand, which is forecast to reach 17 percent by 2030. Through more efficient water use, reduced leaks and improved water management, the network will work to close this gap.

Clark pointed to mounting evidence of the risks posed by water scarcity to business and economic growth, quoting a 2012 projection by the International Food Policy Research Institute that 45 percent of total GDP — \$63 trillion — will be at risk due to water stress by 2050.

► Read more on 2015 Global Risks at: <http://reports.weforum.org/global-risks-2015/>

## ISIS closes gates on Ramadi dam, cutting off water to towns loyal to Baghdad

Source: <http://www.homelandsecuritynewswire.com/dr20150605-isis-closes-gates-on-ramadi-dam-cutting-off-water-to-towns-loyal-to-baghdad>

June 05 – Global security analysts have warned for some time now that water scarcity due to climate change will be used as a tool of war in regions with poor governance. The ongoing wars in Iraq and Syria provide the first examples of the strategic and tactical use of water as a tool of war, as militant groups operating in both countries – and, in Syria, to government of Bashar al-Assad — have been

using the denial of water as a tool against areas and populations they regard as hostile. “ISIS has established a blueprint that can be used by other entities to take advantage of drought and water scarcity,” writes one researcher. “For all the conversation about ISIS taking control of oil refineries, one could argue that their control of water is



even more significant, as it deprives the population of a resource necessary for daily sustenance and gives the militant group significant leverage over local governments and populations.”

Last month ISIS militants captured a dam on the Euphrates River to the north of the Iraqi city

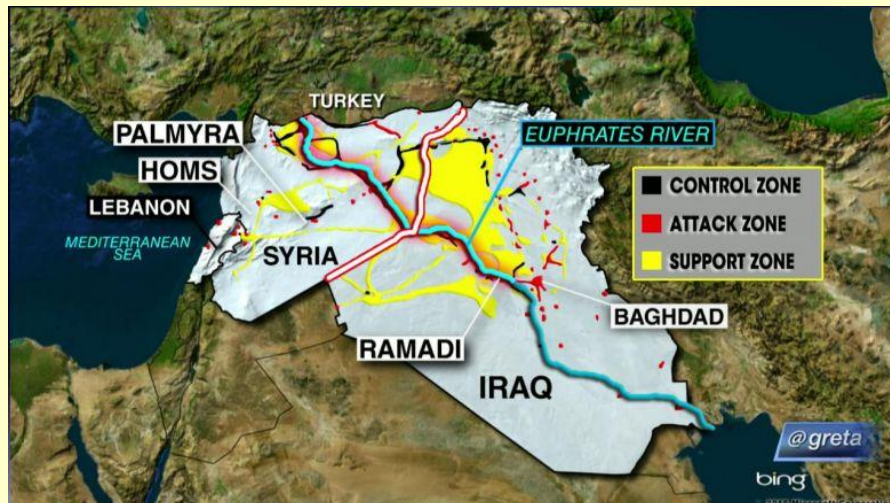
ISIS to prevent river water to flow from ISIS-controlled areas north of the dam, but allow just enough water to flow downstream to ISIS-held towns like Falluja.

al-Fahdawi said that the level of water in the Euphrates was now so low, ISIS militants could walk across it to attack the pro-government

towns of Husaybah and Khalidiyah as well as the large security forces base

at Habbaniya.

CBSNews notes that this is not the first time that water has been used as a weapon of war in Mideast conflicts, and in Iraq in particular. Earlier



of Ramadi, and last week they began closing most of its gates, cutting water supplies to pro-government towns and villages downstream. Iraqi officials say that the move will also make it easier for the Islamists to attack forces loyal to Baghdad.

The large dam has twenty-six gates, but ISIS have kept only two or three gates open for brief periods of time daily.

The head of the security council in the town of Khalidiyah, Sheikh Ibrahim Khalaf al-Fahdawi, told

this year, ISIS reduced the flow through another lock outside the militant-held town of



CNN on Thursday that by closing most of the gates, and leaving two or three open, allows

Fallujah, also in Anbar province. But the extremists soon reopened it after criticism from residents.

The reduced flow of water allowed to flow through the dam on the Euphrates River will threaten irrigation systems and water treatment plants in nearby areas controlled by troops and tribes opposed to the extremist group, provincial council member Taha Abdul-Ghani told the AP. He said, though, that there would be no immediate effect on Shiite areas in central and southern Iraq,



saying water is being diverted to those areas from the Tigris River.

“The use of water as a tool of war is to be condemned in no uncertain terms,” the spokesman for the UN secretary-general,

Stephane Dujarric, told reporters. “These kinds of reports are disturbing, to say the least.”

He said the UN and humanitarian partners will try to “fill in the gaps” to meet water needs for the affected population.

## Floods as tools of war: Many floods in the Netherlands in past 500 years were deliberately caused during wartime

Source: <http://www.homelandsecuritynewswire.com/dr20150610-floods-as-tools-of-war-many-floods-in-the-netherlands-in-past-500-years-were-deliberately-caused-during-wartime>



Aerial photograph of flooded land in the Saeftinghe region, southwestern Netherlands (Credit: A. de Kraker)

June 10 – **A new study shows that, from 1500 until 2000, about a third of floods in southwestern Netherlands were deliberately caused by humans during wartimes.** Some of these inundations resulted in significant changes to the landscape, being as damaging as floods caused by heavy rainfall or storm surges. The work, by Dutch researcher Adriaan de Kraker, is published yesterday (9 June) in *Hydrology and Earth System Sciences*, a journal of the European Geosciences Union (EGU).

An EGU release reports that during the Eighty Years' War, as the Spanish army fought to recapture territory in what is now northern Belgium and southwestern Netherlands in the late sixteenth century, the Dutch rebels led by William of Orange decided to use the low-lying, flood-prone landscape to their advantage. In an attempt to liberate Bruges, Ghent, and Antwerp from Spanish dominance and defend their territory, the rebels destroyed seawalls at strategic places from 1584 to 1586 to cause deliberate, large-scale floods.

“The plan got completely out of hand,” says de Kraker, an assistant professor at the VU University Amsterdam in the Netherlands. “It came at the expense of the countryside of northern Flanders, now Zeeland Flanders, some two thirds of which was flooded.”

**Floods can result in loss of life and damage homes and businesses, and when the water remains inland for a long time, it can change the landscape through erosion and deposition, forming new tidal channels and creeks.** The area flooded during the Eighty Years' War became part of a strategic line of defense and remained inundated for more than 100 years in some places, with profound consequences for the landscape. After the waters receded, a thick layer of clay covered all remnants of buildings and roads in the area. As sea water was used, soil salinity increased, affecting agricultural yields.

“Strategic flooding is a highly risky tactic. It can only be successful if there's a well-thought-out backup plan and a plan for fast repairs,”



warns de Kraker. However, that was not the case here, he says: “I desperately looked for evidence of backup plans for the repair of the dykes and who was going to pay for the costs incurred. I could find hardly any records of such plans.”

De Kraker has been studying historical floods — occurring from the year 1500 to 2000 — in southwestern Netherlands since the 1980s to find out their causes and outcomes. Mostly below sea level, and dominated by three river estuaries populated with islands and a system of dykes and dams that protect the fertile land from the sea, this region is particularly susceptible to floods.

In his research, de Kraker used documents relating to land ownership and land use, accounts of maintenance of sea defenses, and correspondence between stakeholders, such as rebels, Spanish officials, and mayors of besieged towns. He also used aerial photographs of the area, historical maps and maps of soil and landscape changes.

As reported in the new *Hydrology and Earth System Sciences* article, he noticed the main floods in the area in the past 500 years could be grouped into those caused by storm surges (twenty-one events) and those happening

during wartimes (eleven events). The former had natural causes and the latter were created by humans, but de Kraker says human action played a major role in both.

**The most damaging flood occurred in the winter of 1953, when strong winds blew for two days causing a long-lasting storm surge, which resulted in extremely high water levels. More than 1,800 people died, 100 000 were evacuated and damages reached the equivalent of €700 million.**

While the cause of this flood was natural, de Kraker says human factors contributed to the extent of the damage. He reports that officials were slow at responding to the event, failing to take mitigation measures such as raising the dykes fast enough. Weak building construction and inadequate rescue procedures contributed to the material damage and human toll.

The study also shows floods in the Netherlands were used as a weapon as recently as the 1940s.

“Strategic flooding during the Second World War undertaken by the Germans remained purely defensive, while the Allied flooding of the former island of Walcheren in the southwest of the country sped up the Allied offensive,” says de Kraker.

— Read more in A. M. J. de Kraker, “Flooding in river mouths: human caused or natural events? Five centuries of flooding events in the SW Netherlands, 1500–2000,” *Hydrology and Earth System Sciences* 19 (9 June 2015): 2673-84.



## Risk of major sea level rise in Northern Europe

Source: <http://www.homelandsecuritynewswire.com/dr20150619-risk-of-major-sea-level-rise-in-northern-europe>

June 19 – Global warming leads to the ice sheets on land melting and flowing into the sea, which consequently rises. New calculations by researchers from the Niels Bohr Institute show that the sea level in Northern Europe may rise more than previously thought.

**There is a significant risk that the seas around Scandinavia, England, the Netherlands, and northern Germany will rise by up to about 1.5 meters in this century.** The results are published in a special issue of the scientific journal *Climate Research*. Sea level rise is a significant threat to the world’s coastal areas, but the threat is not the same everywhere on Earth — it depends on many regional factors.

“Even though the oceans are rising, they do not rise evenly across the globe. This is partly due to regional changes in the gravitational field and land uplift,” explains Aslak Grinsted, associate professor at the Center for Ice and Climate at the Niels Bohr Institute, University of Copenhagen.

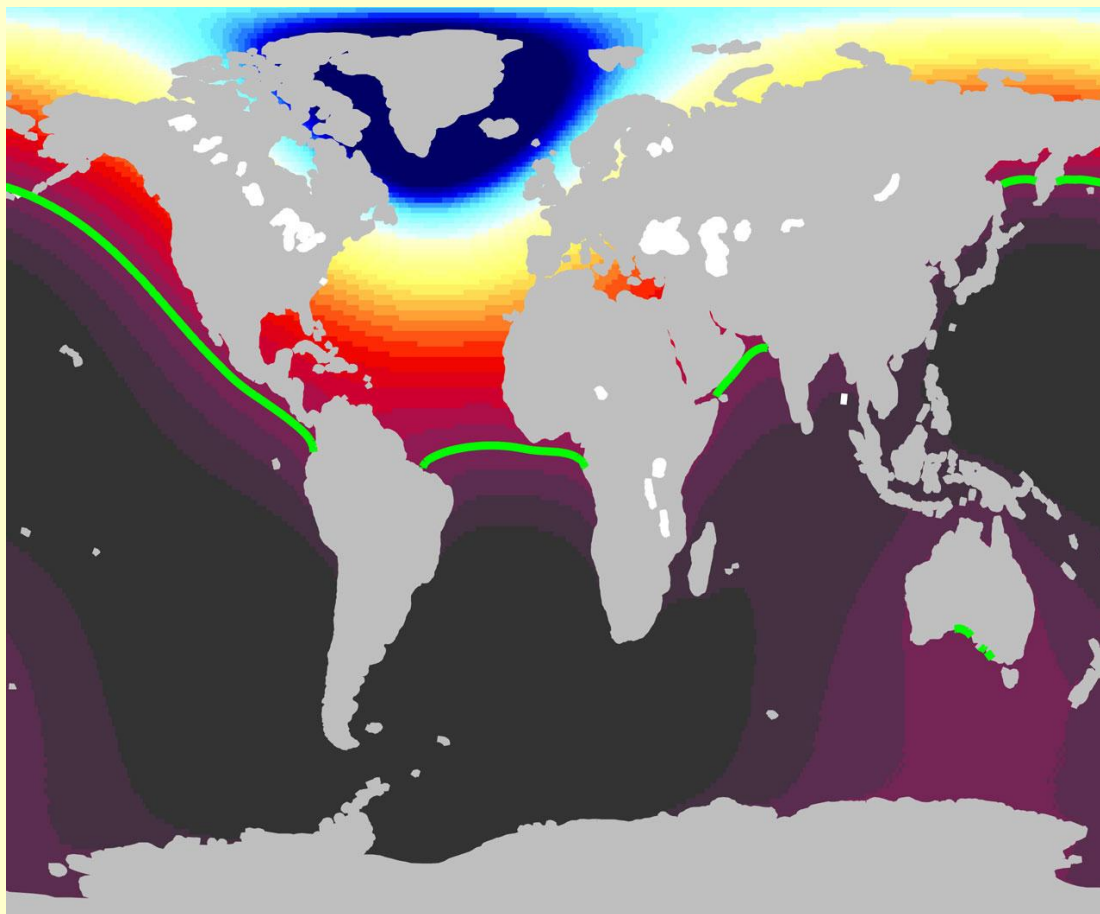
### Sea distributed unevenly

He explains that gravity over the surface of the land and sea varies due to differences in the subsurface and surroundings — the greater the mass, the greater the gravity. The enormous ice sheet on Greenland attracts the sea, which consequently



becomes higher around Greenland. When the ice sheet melts and flows out to sea as water, this attraction is reduced and even though more water has entered the sea, the sea level around Greenland would fall.

regional changes in the gravitational field and land uplift, we have calculated how much the sea will rise in Northern Europe," explains Grinsted.



A University of Copenhagen release reports that another very important effect for Northern Europe is that during the ice age we had a thick ice sheet that weighted down the land. When the weight disappears, then the land rises and even though it has been more than 10,000 years since the ice disappeared, the land is still rising. The calculations show that in the Gulf of Bothnia the land is still rising faster than the expected sea level rise.

The UN Intergovernmental Panel on Climate Change (IPCC) has estimated that the average global warming in this century will rise by 4°C in a business-as-usual scenario. That is to say, if we continue to emit greenhouse gases as we have up to now. The effect will be a rise in sea levels.

"Based on the UN climate panel's report on sea level rise, supplemented with an expert elicitation about the melting of the ice sheets, for example, how fast the ice on Greenland and Antarctica will melt while considering the

**Higher increase than expected**

**The calculations show that there is a real risk that what have been regarded as high scenarios in the Netherlands and England will be surpassed.**

"For **London**, the calculated best estimate is that sea level will rise by 0.8 meters. In England, a sea level rise of more than 0.9 meters in this century has been considered highly unlikely, but our new calculation shows that there is a 27 percent chance that this limit is surpassed and we can not exclude a sea level rise of up to 1.75 meters this century," explains Grinsted.

For the **Netherlands**, the best estimate of sea level rise is 0.83 meters, but the calculations show that there is a 26 percent chance that it will exceed the existing high-end scenario of 1.05 meters and a sea level rise of up to 1.80 meters cannot be excluded.



“Both countries have already established protections for the coasts with barriers, sluice gates, and dikes, but is it enough? I hope that our calculations for worst-case-scenarios will be taken into consideration as the countries prepare for climate change,” says Grinsted.

**Copenhagen** is slightly less exposed. Here the best estimate is that sea levels will rise by 0.68 meters, but there is a risk of increases up to 1.6 meters.

Even though the sea level around the world will rise by an average of 80 cm, however, the sea level in the Gulf of Bothnia in **Finland** is expected to fall by 10 cm due to land uplift. The land is rising faster than the sea is rising.

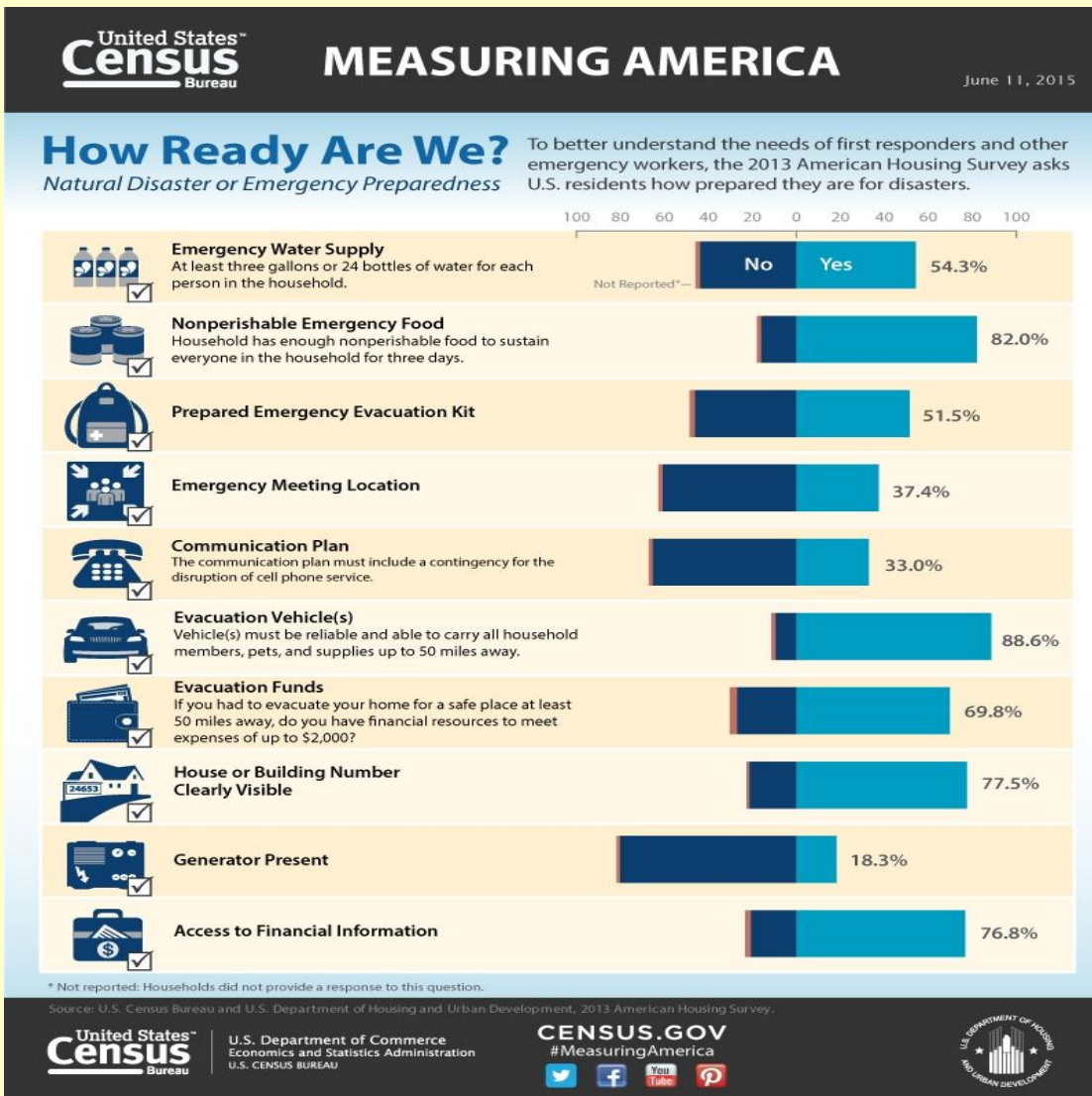
The reduced gravitational attraction of the Greenland ice sheet will result in lower sea levels as far away as 2000 km from Greenland in Ireland, Scotland and Norway. This means that the melting from Greenland will contribute 14 cm to the global sea level, but locally in **Edinburgh** it will result in a fall of 4 cm.

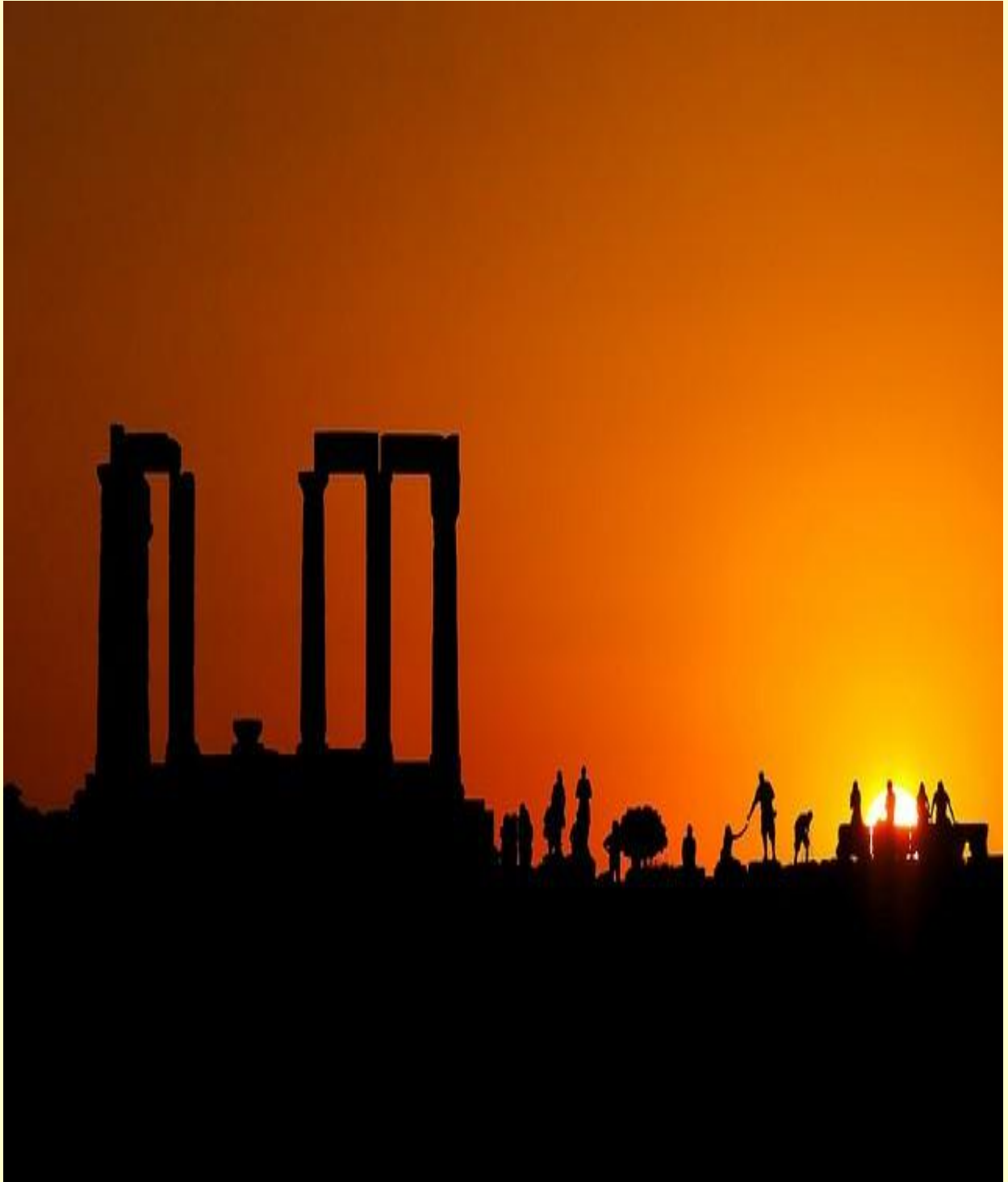
Grinsted explains that the great uncertainty in relation to future global sea level rise is how quickly the ice on Antarctica will melt and whether it will happen in a large collapse. Even without a collapse of the ice on Antarctica, however, vulnerable countries should prepare contingency plans in their coastal defense for the worst-case-scenario.

**EDITOR'S COMMENT:** SE Mediterranean is quite "red" (map) but nobody seems to really worry about it.

## Measuring America: How Ready Are We?

Source: [http://www.census.gov/library/infographics/how\\_ready\\_are\\_we.html](http://www.census.gov/library/infographics/how_ready_are_we.html)





72

Greece – Temple of Zeus (Athens – Cape Sounion)





## Texas Attack Highlights Potential for Terrorist Action

Joe Shust, Editor

Source: <http://www.continuityinsights.com/articles/2015/05/texas-attack-highlights-potential-terrorist-action>

The Islamic State in Iraq and Syria (ISIS) is claiming responsibility for an attack in Garland, Texas in which two gunmen opened fire on an event where attendees were asked to draw the prophet Muhammad.

The two men, Elton Simpson and Nadir Soofi, were killed by police before they were able to enter the Culwell Event Center, where members of the American Freedom Defense Initiative (AFDI) were holding a competition asking members to draw Muhammad, which is considered offensive to Muslims. The AFDI has been classified as an anti-Muslim hate group by the Southern Poverty Law Center. While there has been no proven link between the duo and ISIS, the terrorist organization has claimed responsibility for the attacks.

"I think that they will probably end up finding that these guys were being enticed by ISIS, but weren't actually members," Robert Edson of Mission Mode said. "It begs the question from a business continuity standpoint 'where can this happen again?' You can find radical fundamentalists in any place and attracting two or three people out of those groups to do this kind of stuff on a random basis is far more dangerous because of its ability to happen unexpectedly."

Edson said he thinks future terrorist attacks on American soil will be similar to the one in Texas, as the current climate makes them the most practical for the attackers.

"These aren't what I would consider a lone wolf attack," Edson said. "I think this a new breed of the way terrorism is going to start to manifest itself in the United States. You're going to find groups of people willing to carry out smaller attacks until a stronger weakness to do something bigger. I think the proliferation of those attacks could become more substantial and more random."

The proliferation of social media also allows groups like ISIS to get their message to anyone, anywhere. In a tweet posted just before the attack, Simpson pledges allegiance to "Amirul Mu'mineen," or "the Leader of the Faithful." Some believe this is a reference to ISIS leader Abu Bakr al-Baghdadi.

"Finding disenchanted people who are easily enticed on social media in different parts of the world is kind of ISIS' model," Edson said. "It's not like they can send 50 jihadists over here without somebody noticing. It's not overly challenging to find radicals to do something like that, especially considering the group that they attacked. It's not like they walked into a police station or the state department."

Edson said attacks like this will eventually push business continuity and physical security professionals to work towards a closer relationship.

"I think this is going to force business continuity professionals and physical security professionals to work together more often," Edson said. "It will force us to evaluate basic questions like how do we shut down a building, how do we evacuate a building, how do we do more things on a simple holistic level. It's going to be hard to sit there and write up a business continuity plan for this because it's too random."

He likened the potential randomness of a terrorist attack with potential weather incidents, which often leave business continuity professionals little time to prepare and force quick and decisive action.

"Your average business continuity professional on a day-to-day basis is probably going to have a lot of concern about something random like one of these attacks," Edson said. "It's almost like trying to plan for a tornado. You don't know when it's going to drop out of the sky and you might have three minutes warning, so what are you going to do? You can't take out an 80-page business continuity plan and figure out what to do when you have three minutes to respond."

ISIS claims to have more than 70 agents operating in as many as 15 states, although that is impossible to substantiate. However, their random and potentially deadly nature should make potential terrorist attacks a concern for business continuity professionals.

"As professionals, we get so wrapped around the axle with all



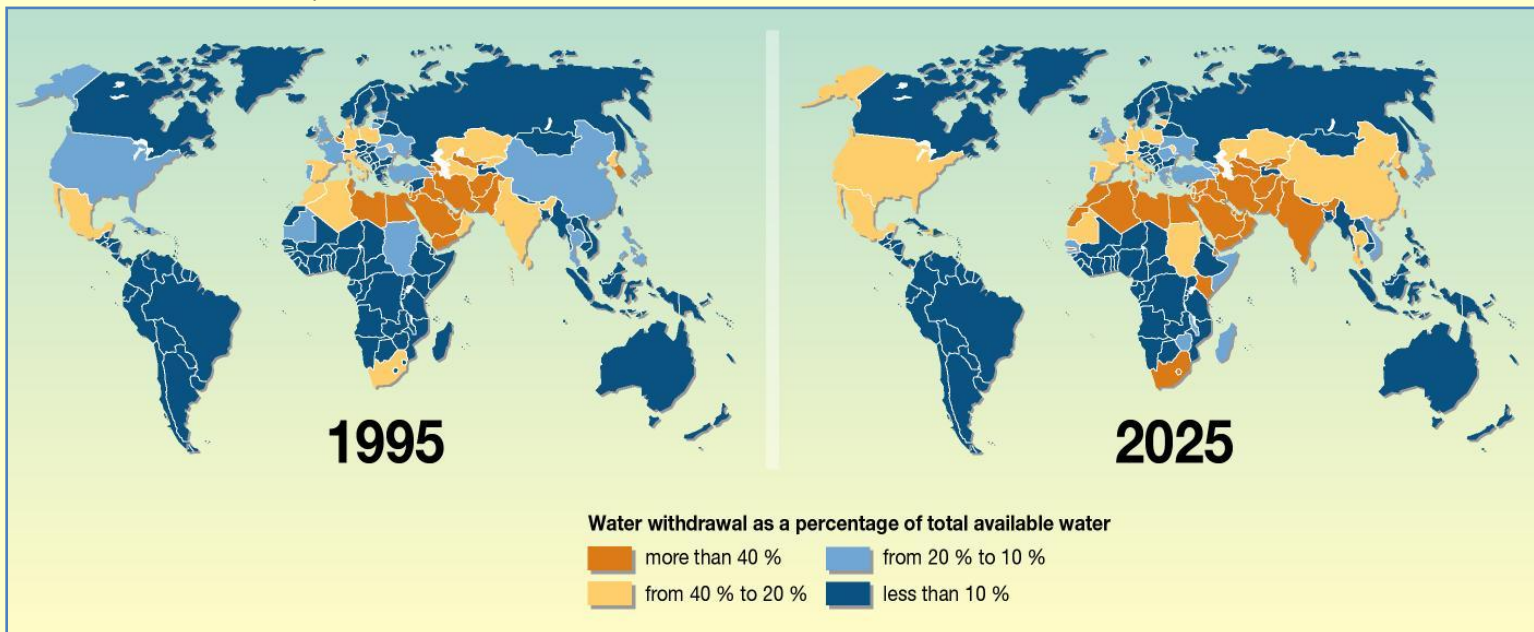
these BIAs and all these things we think we need to go do as a company,” Edson said. “You need to maintain the simplicity of locking down a building and you need to exercise.

Locking down a building with an active shooter in the area is the surest way to reduce casualty counts.”

## Could Water Scarcity Impact Business Continuity Professionals?

Joe Shust, Editor

Source: <http://www.continuityinsights.com/articles/2015/04/could-water-scarcity-impact-business-continuity-professionals>



Resource management is a critical concept when it comes to resilience. An organization can't function properly without the things it needs to do so.

While resources are important, there are few that are as universally needed as water. Nathaniel Forbes of Forbes Calamity Prevention argues that the impact of restricted access to water is something more business continuity professionals should focus on.

“Could water motivate someone to consider committing an act of terrorism? Could interruption of water supply break a company's supply chain? Could management of water give an entire country a competitive advantage?” Forbes said. “I think so. Those are three important aspects of business continuity.”

Lack of water could present serious challenges to an organization, especially one that operates in an area where access is scarce. Like any resource, proper management could result in a competitive advantage.

“Imagine a day when a business continuity manager in Las Vegas has to say to a hotel owner or manager ‘we are not going to continue to operate unless we do something about our water supply,’” Forbes said. “Say, hypothetically, the Sands manages their water resources better than the MGM Grand, would that give them a competitive advantage? Should a business continuity manager be able to contribute to that discussion of increasing a businesses' resilience? I certainly do.”

Lack of access to water having an impact on a business is nothing new according to Forbes, who said it has happened on a large scale before.

“In 1984, the Coca Cola Company had to shut down a bottling plant in India because there was insufficient water to provide for the farms in the area and their bottling,” Forbes said.

“The government made the choice to support the farmers, who are their constituents, rather than the company. At that point Coca Cola tried to truck in water to



bottle. The villagers started hijacking the water trucks because they had limited water themselves. They eventually abandoned the business.”

Forbes believes lack of water access could potentially be a reason for someone to commit an act of terrorism. Terrorism is a serious concern for BC pros, particularly those whose organizations have assets abroad.

“If you were a homeland security professional and your mission was to prevent your fellow employees and colleagues from getting hurt or killed, you would be looking for causes of terrorism and eliminating them,” Forbes said. “I would suggest that lack of water is a cause and will be a bigger one in the future.”

Water is a resource that is needed in almost every capacity and water scarcity is something worth keeping an eye on for business continuity professionals.

“You can go three minutes without air, three days without water and three weeks without food,” Forbes said. “From a business continuity manager’s standpoint, the recovery time objective for water is about three days, after which the consequences become very severe. That doesn’t leave a business continuity manager much time to do much planning if they hadn’t thought about water sources or water security.”

## Disaster Planning a Continuing Focus for BC Pros

Joe Shust, Editor

Source: <http://www.continuityinsights.com/articles/2015/06/disaster-planning-continuing-focus-bc-pros>

Recent disasters, like the **earthquakes in Nepal** and **floods in Texas and Oklahoma**, have once again put the focus on businesses staying operational during and recovering from drastic events.

Preparing for these events can be crucial, as disasters can cost businesses financially as well as other ways. Some businesses never recover from large storms or natural disasters. However, not all organizations recognize that and many don’t have proper plans in place.

“The biggest thing we see is building even a simple plan and making sure it is somewhere you can get to in the case of a disaster,” Mark Campbell, CTO of Unitrends, said. “A lot of times people simply don’t plan or even worse, they keep their plan on a computer on the premises and then they get flooded and it gets wiped out.”

Many managers fail to provide their employees with basic needs to do their jobs, delaying recovery and increasing down time.

“If you start with people, what are the basic resources that staff is going to need in the event of an outage?” Campbell said. “If people don’t have a place to sit, if they don’t have phones, if they don’t have internet access, anything advanced technology isn’t going to help very much if those basics aren’t there.”

Campbell said one of the most important motivators is making sure employees are paid during recovery. The process is often an

afterthought, but can become difficult during and after disasters.

“We don’t always think about paychecks,” Campbell said. “For a lot of people if they don’t get their paycheck they will be hurting.”

Part of what makes disaster planning difficult for even seasoned business continuity professionals is that no two industries are alike. What is an important process for one kind of business isn’t necessarily critical to another.

“A manufacturer is going to tell us they can’t ship products, they are going to look at their whole supply chain, what their second sites look like and what their ability is to use a second or third site,” Campbell said. “On the other hand, if you are in professional services you can’t get your consultants out to the customer site without understanding who’s doing what. Typically, if you start with the simple question and look from the top down, companies understand what is important to them.”

While most businesses, even those without strong business continuity programs, understand that a natural disaster will have some impact financially. However, most don’t think about how the downtime they cause damages their reputation.

“There are a lot of studies that show the cost of downtime,” Campbell said. “You talk about reputational damages. If you are

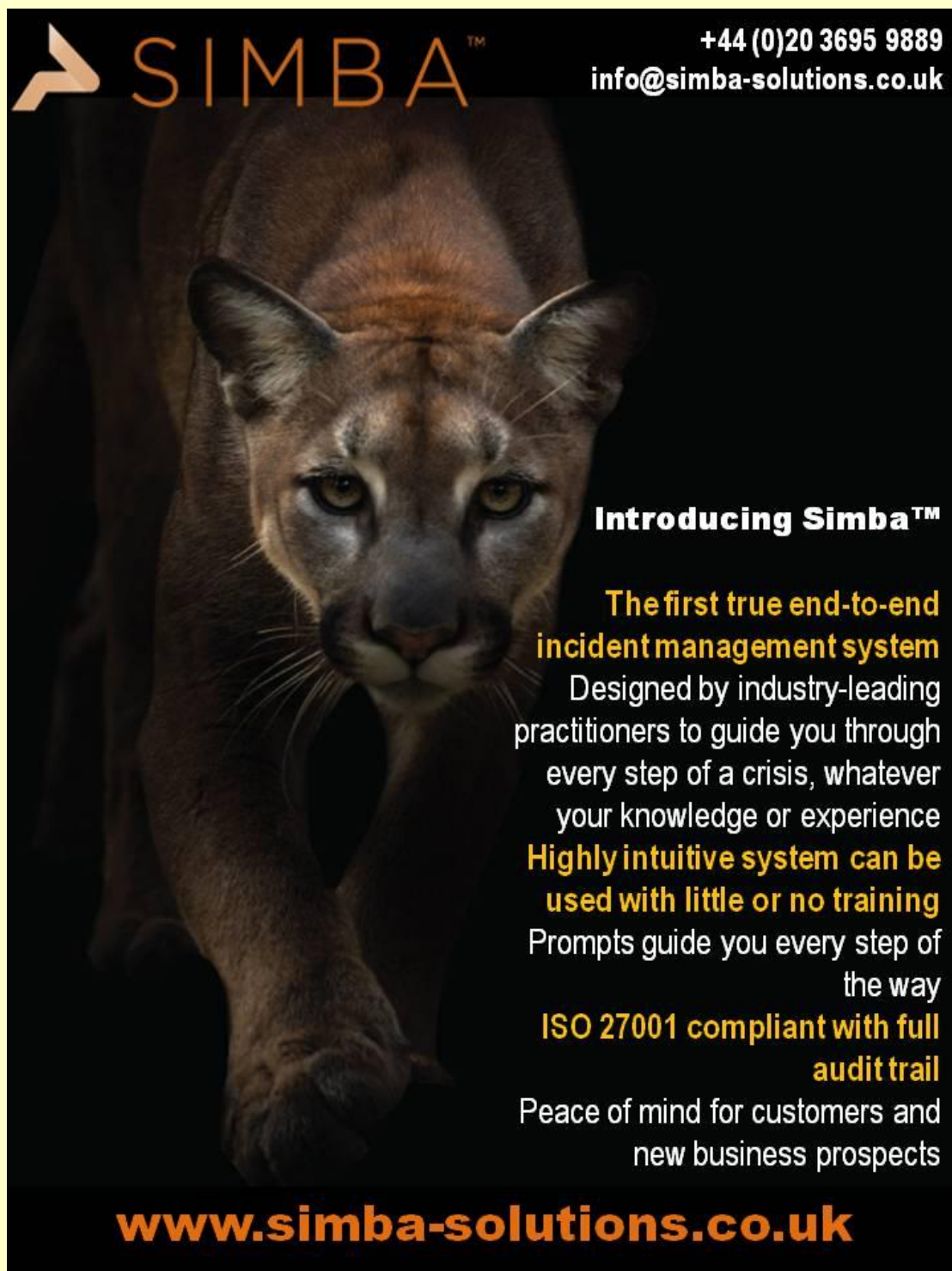


a professional services company and people can't reach you for a day, it's not only what percentage of customers are you going to lose that day, it's what percentage of customers are you going to lose forever when they believe you are fundamentally unreliable. What we are finding is that it is so competitive out there that reputational damage is starting to get more noticed."

The need for a fast and efficient recovery plan has become even more important as today's

high speed, high connectivity society demands it.

"Before a lot of these businesses could envision themselves being down for a day or two and not suffering," Campbell said. "Now it has moved from days to hours. That doesn't mean you have to recover to your full capability, but you need to recover enough to be able to communicate."



**SIMBA™** +44 (0)20 3695 9889  
info@simba-solutions.co.uk

**Introducing Simba™**

**The first true end-to-end incident management system**  
Designed by industry-leading practitioners to guide you through every step of a crisis, whatever your knowledge or experience

**Highly intuitive system can be used with little or no training**  
Prompts guide you every step of the way

**ISO 27001 compliant with full audit trail**  
Peace of mind for customers and new business prospects

**www.simba-solutions.co.uk**



## Tragic Derailment Presents Business Continuity Challenges

Joe Shust, Editor

Source: <http://www.continuityinsights.com/articles/2015/05/tragic-derailment-presents-business-continuity-challenges>



Details are still being revealed after an Amtrak train derailed near Philadelphia leaving seven dead and more than 200 injured.

Amtrak train 188 was traveling to New York when it derailed after attempting to go around a curve at a high rate of speed. According to reports, the train was traveling at 107 miles per hour, more than twice the 50 mile per hour speed limit for the turn. The train's engineer, identified as Brandon Bostian, 32, of New York, applied the emergency break before the train derailed. Bostian has refused to be interviewed by detectives and suffered several injuries in the crash including a concussion. His lawyer said Bostian has no recollection of his speed or the aftermath of the crash because he lost consciousness. Drugs and alcohol are not believed to have been a factor. Investigations into the incident are ongoing and Amtrak has said little at this point. They have set up an emergency hotline for those with questions about individuals on the train.

### A Host of Disruptions

For business continuity professionals, train derailments present a unique set of problems, particularly when they involve passenger trains. One incident can result in a host of different potential disruptions.

"There are a host of Business Continuity issues that can arise from train derailments of any kind," Robert Edson, Vice President at Mission Mode, said. "Obvious concerns include supply chain problems, and the potential for serious utility infrastructure issues. Beyond that, depending on proximity to the derailment, there may be a whole host of issues from building evacuations to duty of care issues and HR concerns if commuters use the rail to get to work."

Edson also said derailments can lead to unseen or long term disruptions, as all of their consequences aren't immediately evident.

"Assessing your impact and potential vulnerabilities rapidly can be challenging because an event like this can have far more widespread impact than it appears on the surface," Edson said. "Communication and accountability are key. Events like this should jar the fillings loose of any BCP program that doesn't have an effective Incident Management platform that can keep things in a manageable light. Only twenty percent of the market has one though. That's going to start to change when organizations realize the complexity events like this can cause."

77



It is too early to determine what impact this derailment could have long term, but it is likely that it will result in more debate about infrastructure in the United States. The day after the crash, lawmakers voted to cut Amtrak's funding by 15 percent, about \$252 million. Amtrak is publicly funded, but operated and managed as a for-profit corporation. In the short term, the crash will cut off a major line of transportation between New York and Philadelphia.

"Locally this will disrupt travel in the area for weeks I would imagine," Edson said. "Hopefully long term these kind of incidents make us stronger as we learn from them. It's incredible if you actually look at rail in America, so much of our economy depends on rail and more infrastructure than we'd like to admit is tied to rail. Telecom for instance, and power grids, single points of failure that in this dependent world can make for real BCP headaches."

#### **Traveling Employees**

The incident will also bring the importance of traveling employees into the limelight for business continuity professionals.

"BC leaders need tools to help traveling employees. One important tool is an organization-wide travel risk management policy," Mike Keating, Vice President of Business Continuity for Reinsurance Group of America, said. "This policy establishes your authority to oversee this risk area which is important given its nature as crossing several places in the org chart. The policy should authorize both tools to protect and assist employees, and tools to protect the company from the loss of a large number of employees, especially key employees, in any one event."

Keating recommends using travel risk tracking software like those provided by iJet and International SOS, which allows companies to know where their employees are at all times and in some cases, actually monitor their geolocation. If an incident does happen and employees are injured, Keating said it is the responsibility of the organization to be there and provide for them.

"It is important that the company establish an onsite presence as soon as possible to help the injured employee, especially if it will require a hospital stay of more than a day. Employers should be in touch with family members to find out whether they are interested in coming to the hospital where their loved one is being

treated, and make whatever financial or other commitments are necessary to permit this," Keating said. "Sometimes this involves unconventional items such as paying for extended family to travel to the employee's home so a spouse is freed up to come to the hospital. Employers owe employees a duty of care when they travel on company business and employers who shortchange their response to caring for injured travelers could find their decisions penny wise and pound foolish when the downstream legal and employee morale implications are better understood."

The company also needs to be aware of employees who may be stranded due to travel related incidents and make sure those people are taken care of as well.

"This is one reason why it's so important to monitor employee travel," Keating said. "Within hours every hotel room and rental car in the area is probably booked. Only those who knew about a stranded traveler early and took action would be able to access the most user friendly and cost effective strategies."

#### **Health and Wellness**

Employee health will be of particular concern for Amtrak. Incidents like the Germanwings crash have put mental and physical health of employees under a microscope. Even if Bostian's health isn't a factor, Amtrak very well could be liable for his actions.

"Why was it going so fast? Was it the mental condition of the conductor? Physical? Or was it because the internal pressure to perform on time was too great and that pressured an otherwise responsible employee to act irresponsibly?," Edson said. "When does corporate profit concern overtake the safety factor of operations? How much damage control will Amtrak have to do if the conductor was going too fast to make up lost time and not be late for fear of losing his job? Is that an appropriate policy, if it exists, at Amtrak? There's a lot to consider and the key thing is not to take anything off the table at this stage." Keating says it is too early to say, but this incident could cause companies to re-evaluate the way their employees travel.

"If we later learn that a company had a large number of people on the train, it will certainly reinforce the need to ensure there is a limit to the number of employees on any one vehicle," Keating said. "It could



also increase the likelihood that companies already monitoring traveler concentration for air travel, sometimes referred to as the 'Same Flight Rule,' is extended to trains and other long haul ground transit."

Edson said he thinks it is important to take a look at the entire incident and determine what needs to be fixed.

"The critical thing is to understand the cause of the crash in its entirety then have an honest look internally to see if any trends are identifiable, and then address them," Edson said. "Honest evaluation of these things is critical. Companies never really lose from an incident like this so long as they learn from them."



**Greece – Acropolis Museum (Athens)**

