# CBRNE NEWSLETTERRORISM

July 2016

E-Journal for CBRNE & CT First Responders




NO THANKS

Rio2016™

www.cbrne-terrorism-newsletter.com

# Scanners more rapidly and accurately identify radioactive materials at U.S. borders, events

**By Rob Matheson**

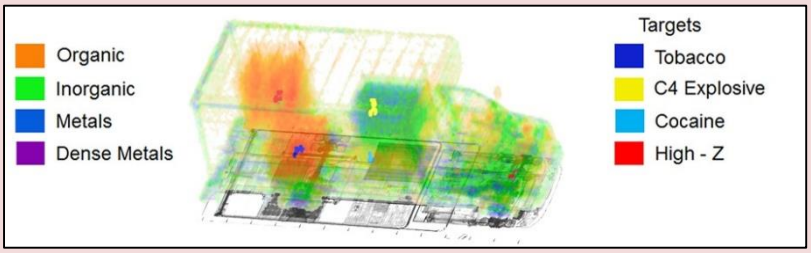
Source: http://www.homelandsecuritynewswire.com/dr20160623-scanners-more-rapidly-and-accurately-identify-radioactive-materials-at-u-s-borders-events

June 23 – In response to the terrorist attacks of September 11, 2001, the U.S. government founded the Department of Homeland Security (DHS) to prevent terrorist attacks on American soil. **Among other things, the DHS increased screening of cargo coming into the country.** At the same time at MIT, the terrorist attacks gave rise to a company dedicated to helping DHS — and, ultimately, other governments and organizations worldwide — better detect nuclear and other threats at borders and seaports.

Launched in 2002, Passport Systems developed a scanner, backed by decades of MIT research, that can automatically "fingerprint" radioactive or other suspicious material through a truck, cargo container, or other concealed package, and alert authorities immediately.

Today, Passport — co-founded by MIT physics professor emeritus William Bertozzi — has two commercial scanners: the cargo scanner, a facility used at borders and seaports; and a wireless radiation-monitoring system used at, for example, public events.

Passport's cargo scanner, called SmartScan, inspects trucks carrying cargo and automatically identifies any radioactive material or "actinides" (radioactive elements) that may signal a dirty bomb, weapon of mass destruction, or explosive. The scanner can also catch contraband such as drugs, tobacco, and firearms. This year, under a contract issued by DHS's Domestic Nuclear Detection Office, Passport deployed its first SmartScan inspection facility at the Port of Boston's Conley Container Terminal.




Cargo scanning today relies primarily on high-powered X-rays, which provide a two-dimensional projection of shapes of objects inside containers. Denser objects, which could harbor nuclear threats or contraband, are further investigated by opening the container. Opening and inspecting each suspicious container can take hours and could be dangerous.

Passport's cargo scanners, on the other hand, offer precision scanning in minutes, without ever opening a container, says Bertozzi, now Passport's scientific advisor and a member of its board of directors. "In about 30 seconds, we can scan a container and provide a three-dimensional map of [the materials inside the cargo]. This information clears the container or alerts you to a region that needs to be examined more carefully. In another 15 seconds, our scanner will tell you whether there's an actinide there. In another half a minute, we can tell you what actinide it is, and if it's a bomb," he says.

Passport's handheld system, called SmartShield, is a network of small gamma-radiation detectors, about the size of a deck of cards, that collects radiation data in real-time and wirelessly connects to smartphones. Typically, law enforcement and first responders wear the detectors on their belts and carry the phones, while walking around and collecting data on background radiation. If a detector identifies gamma radiation, it sends an alert to all other smartphones in the network, as well as a central command station, and displays the GPS coordinates to first responders.

SmartShield was trialed at last year's NASCAR race in New Hampshire, this year's NCAA Final Four Men's Basketball Championship in Texas, and other major events in the nation.

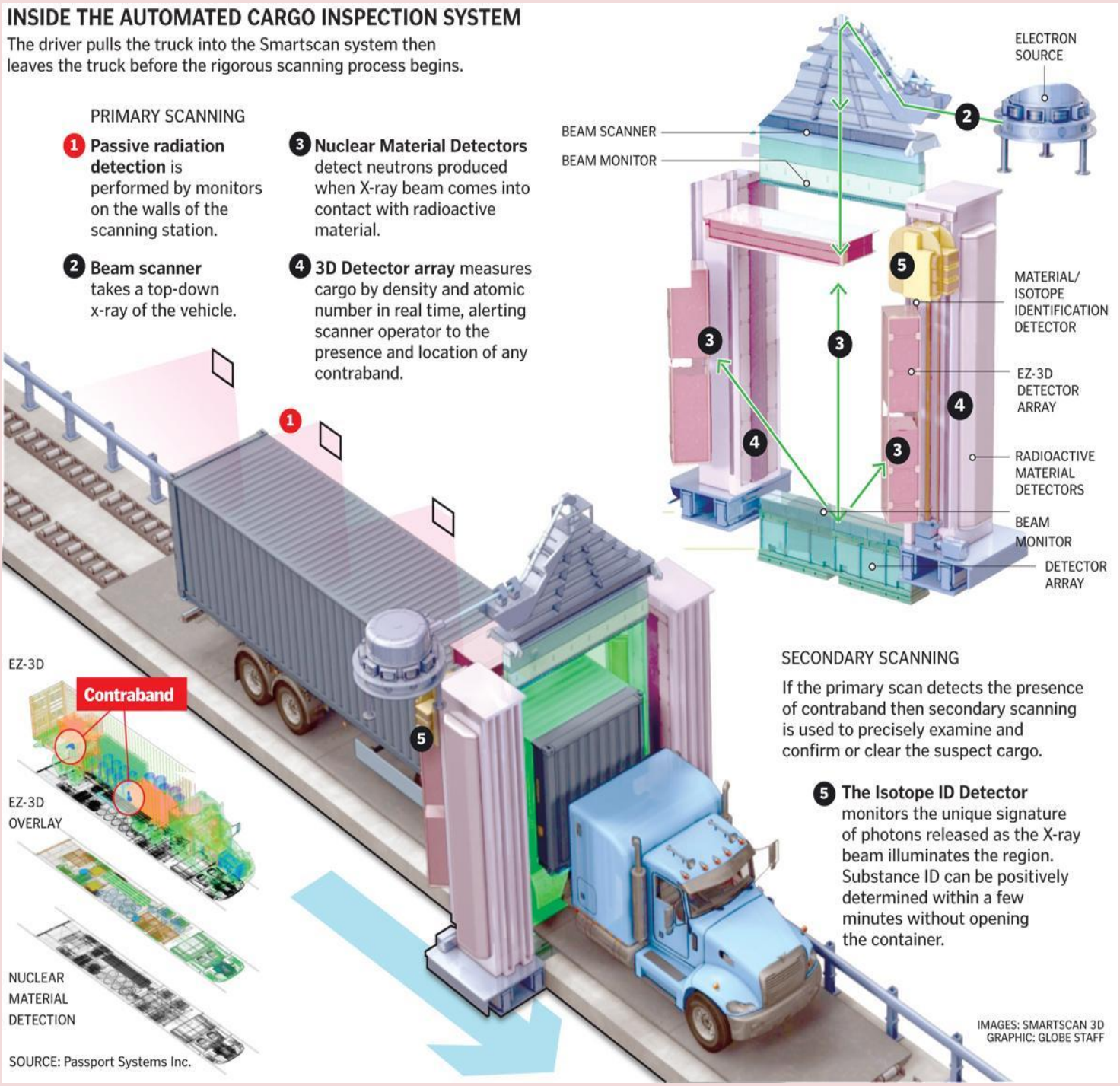
## "Fingerprinting" actinides

**Passport's SmartScan facility at the Port of Boston** is a tunnel about 176 feet long, resembling a drive-through car wash. Trucks carrying land and sea cargo containers are pulled through slowly on a conveyer belt, and scanned by a massive scanner attached to the tunnel's entrance. This scanner combines conventional high-resolution X-rays and other passive radiation

detection methods with scanning techniques pioneered by Bertozzi at the MIT Laboratory for Nuclear Science and by Passport.

As a truck passes through the scanner, Passport's custom EZ 3-D scanning method generates three-dimensional images of a material based on the effective atomic number — called "effective Z" — which could indicate explosives. To do so, an electron beam produces photons that shoot into the material. The electrons of atoms in the material scatter these photons. The system measures the photon signals to determine any anomalies: Photon signals for high-Z materials such as actinides, for instance, are about 10 times higher than signals from low-Z materials such as common metals. "Because these photon signals are huge and prolific, we can tell you where in the container you have materials that are high effective Z," Bertozzi says.

But some of these signals are difficult to differentiate, so, if suspicious materials are present, the system automatically conducts refined, secondary scans.



**The first technique is Prompt Neutrons from Photofission (PNPF),** developed by Bertozzi at MIT in the 1960s. A photon beam causes the actinide nuclei in the material to fission and emit neutrons, which are measured. If the neutrons are produced over a certain threshold of energy, they're from an actinide. Then the system uses another technique developed by Bertozzi at MIT, called nuclear resonance fluorescence (NRF), where the photon beam excites the nuclei, which emit gamma rays at distinct energy levels. Measuring those energy levels gives the "fingerprint" of the actinide. "We can tell you if it's, say, uranium-235, uranium-238, oxygen-17, or carbon-12, because they all have different signals," Bertozzi says.

Drugs and alcohol have specific "fingerprints" too, as do materials such as salt and chlorine, so the scanner is helpful for detecting contraband. A scanner, for instance, could detect chlorine, sometimes used to make methamphetamine, in a truck full of clothing.

Now, the United Kingdom is seeking the systems to look for items such as untaxed tobacco being smuggled across the border, while other countries are looking for the systems to scan for drugs and alcohol. "It serves a security need, but it also satisfies general customs needs," says Passport's CEO, president, and co-founder Robert Ledoux '78, PhD '81, who taught physics at MIT until 1990. "That's made it commercially viable."

Passport's SmartShield detectors use standard photon-detection technology to detect gamma rays. But the innovation comes from the network, which offers numerous benefits, Ledoux says. Working together, the scanners can quickly triangulate the location of a threat. Constantly updated radiation data, from multiple detectors being carried around an area, also makes the system as a whole more sensitive. "With each passing sweep, it can better separate naturally occurring radiation in, say, building materials from hazardous nuclear materials," Ledoux says.

**Coming together at MIT**

Passport's story starts in the mid-1990s, when Bertozzi tried bringing his MIT-invented NRF scanning technology to a company that was trying to commercialize baggage-scanning technologies in U.S. airports. Despite successful tests, the company decided the technology was too expensive to scale, especially since airplane bombings weren't necessarily considered a major threat.

"But then the world changed with 9/11," Ledoux says.

Suddenly, the newly minted DHS wanted all baggage at airports and every cargo unit at the U.S. border scanned for explosives. X-rays and CT scans were used for luggage, but no quick, accurate scanning techniques existed for cargo containers. "It's difficult to detect explosives in a small package. Imagine having a 40-foot container filled with thousands of pounds of things, whipping through the supply chain," Ledoux says.

Seeing that the world was ripe for NRF-based scanners, Bertozzi launched Passport with friend and MIT Sloan School of Management alumnus Gordon Baty '61, SM '63, PhD '67, who is now chair of Passport's board of directors. They pulled in Ledoux as CEO and set up shop in Ledoux's home office.

However, although they could prove the technology theoretically, there was nowhere to test it on a large scale. Then one day Ledoux was on MIT's campus, speaking with a fellow alum about Passport's testing issues, when the alum pointed to MIT's High Voltage Research Laboratory, which was supposedly shut down. "We were literally right across the street," Ledoux says. "So we walked over and rang the doorbell."

Turns out, the MIT facility was still in use. "It became only the third place in the country that we could do the experiments," Bertozzi says.

"The world came together at this small lab on MIT's campus," Ledoux adds.

Throughout the mid-2000s at MIT, a small team including Bertozzi and Ledoux recorded the unique signals of all actinides. From there, the project grew steadily: In 2007 and 2008, Passport received DHS contracts to test a proof of concept of their cargo scanner, at their headquarters in Billerica. In 2009, Passport received a DHS contract to build their SmartScan system.

The company's latest DHS contract, issued in 2013, is for building a system that fuses gamma radiation-detection data with video, to track radiation in vehicles traveling at highway speeds.

# Islamic State And The Threat Of WMDs

**By David Patrikarakos**

Source: http://www.rferl.org/content/islamic-state-threat-of-wmd/27828778.html


The gravest threat would come if IS were able to get its hands on nuclear materials. The greatest danger comes from the most unstable countries with the largest amounts of documented radical activity: Pakistan, Russia, and India -- with Pakistan at the top of the list.

June 29, 2016

From Fallujah to Mosul, Paris to Brussels, the terrorist organization that calls itself Islamic State (IS) murders, maims, and enslaves with wanton abandon, if not exactly impunity. By now the world has woken up to the serious threat that the group poses, not just in the Middle East but also in Europe and the United States.

Islamic State's crimes are horrific enough with its present capabilities, but a question increasingly asked among politicians and military officials is: What if IS were to acquire the unthinkable -- a weapon of mass destruction (WMD)?

Earlier this month I attended the International Luxembourg Forum on Preventing Nuclear Catastrophe in Amsterdam, an NGO set up to tackle exactly this type of problem. And what emerged is that the danger of IS acquiring its most fearsome weapon yet is now a significant one.

According to an expert who participated in the forum, the danger is twofold. The gravest threat would come if IS were able to get its hands on nuclear materials. These would mean, for example, the type of enriched uranium Iran uses in its nuclear program -- from which IS could theoretically make a small nuclear bomb with further enrichment -- or existing weapons-grade plutonium, from which it could do the same.

But the probability of IS being able to do this is slim. **The requisite materials are located in only 24 countries and are in highly guarded facilities. Set against this fact, however, have been several lapses in security.** In 2012 an 82-year-old nun and peace activist, Megan Rice, broke into the Oakridge nuclear reservation in Tennessee. Rice never got near any nuclear material but a lot of systems had to fail for her to get as close as she did. Likewise, according to a British Ministry of Defense report, guards at one of the U.K.'s nuclear facilities were caught sleeping on the job. And then there is the problem of poor levels of security at a host of nuclear research centers in the former Soviet Union.

The probability of IS taking advantage of these lapses in security is low, but not insignificant. The greatest danger comes from the most unstable countries with the largest amounts of documented radical activity: Pakistan, Russia, and India -- with Pakistan at the top of the list.

Moreover, as retired Major General Vladimir Dvorkin, a chief researcher at the Center for International Security at the Russian Academy of Sciences' Institute of World Economy and International Relations, told me: "there is a lot of illegal activity, trafficking in illegal natural material...so [IS] could either pull off a purchase for a significant

amount of money or intercept illegal trafficking. Plus, they seem to have enough money to recruit scientists to build a rudimentary nuclear device. Not a nuclear warhead, but an explosive nuclear device; it may, in fact, only weigh a few tons but it's still something you could assemble close to an urban area, or on a vessel that could then be brought to U.S. or European shores."

**Many Ways To Dirty Bomb**

Another problem would be a conventional weapons attack on a nuclear facility, which could conceivably cause a Chernobyl-like disaster or worse. It remains nearly impossible to attack a nuclear power plant, as they have substantial protection, but attacking nuclear-research facilities that have reactors filled with nuclear materials is far easier, and a lot of cities have these. According to Dvorkin even bombing a nuclear-storage facility with a relatively small bomb would mean the destruction of buildings within a 3-4-kilometer radius and fallout covering a much larger area and creating a lasting effect.

The second and far more immediate threat is that of attack with a radiological device. The materials for this are located in over a 100 countries and, critically found not just in specialized facilitates but in hospitals and research centers used, for example, in treating cancer -- places that, unlike major nuclear facilities, don't have gates, guards, and guns. The expert who attended the forum warned me that IS has many such facilities within the land it already controls and that is where the "dirty bomb" (a radiological as opposed to nuclear bomb) threat is now unequivocally real.

One can easily use conventional resources to make a dirty bomb, use agents to plant it in a major urban center, then simply watch it ignite and cause billions of dollars of damage. The loss of life would likely be modest -- only those in its immediate vicinity would die. But the psychological element would be huge; as a nuclear specialist told me, the public hears "radiological" and immediately panics. Then there would be the cost of demolishing and rebuilding the buildings that had been contaminated in a far wider area.

While nothing is certain when dealing with what is clearly a fanatical organization, it is clear that IS is organized and thinks strategically. As Dvorkin points out, the chances of IS using even a rudimentary nuclear device are accordingly slim. First, it would risk alienating even Sunni Muslim communities across the Middle East that might presently have some sympathy with its aims. Second, what is now a fractious coalition fighting against IS would almost certainly unite and bring its combined weight to utterly annihilate the organization.

Nonetheless, as The New York Times reported in February, a man linked to the November 13 Paris attackers was found in possession of surveillance footage of a high-ranking Belgian nuclear official. With IS any horror is possible, even if it is not probable.

The question more realistically facing us is not whether IS can employ a dirty bomb -- most likely in Europe or the United States -- but will it? And experts fear the worst. According to Dr. Moshe Kantor, president of the Luxembourg Forum, "the threat of a terrorist group, such as Islamic State, staging a nuclear bomb attack on a major European city, such as London, is 'high.'"

Given that IS has already carried out numerous chemical-weapons attacks in Syria, its willingness to use a WMD of some kind is clearly present. As Kantor continued "the threat of a so-called 'dirty bomb' attack is at its highest level since the end of the Cold War."

The world should be worried.

***David Patrikarakos** is a contributing editor at the Daily Beast and the author of Nuclear Iran: The Birth Of An Atomic State. He is working on a book on social media and war.*

# Defense applications met by ultra-reliable handheld radiation detector from Symetrica

Source: http://www.symetrica.com/verifinder-2

June 30 – Symetrica Inc. will exhibit at the forthcoming National Defense Industrial Association (NDIA) Annual Chemical, Biological, Radiological, and Nuclear (CBRN) Defense Conference & Exhibition in Maryland (Booth #55) to showcase the capabilities of its new VeriFinder™ radio-isotope identifier (RIID). The VeriFinder is based on Symetrica's Discovery Technology®,

which is used in Smiths Detection's RadSeeker™ RIID by the U.S. Department of Homeland Security (DHS). The rugged, lightweight VeriFinder delivers outstanding detection accuracy and performance in any operating environment and ensures ultra-reliable discrimination of radioactive threats with zero scheduled maintenance.

Symetrica's unique ability to detect and identify hidden or disguised radiation threat sources has been tested and verified through a number of deployments at independent test facilities and in the field – showing that the company's technology is relevant in battlefield conditions and performs in harsh real-world scenarios.

Products based upon the advanced identification capabilities of Discovery Technology have been selected by the U.S. Government for border protection and Coast Guard missions based upon performance, ease of use, and the patented in-built calibration and stabilization system that completely removes the need for annual servicing. Smiths Detection's RadSeeker, incorporating Discovery Technology, was recently awarded an IDIQ (indefinite delivery/indefinite quantity) contract with a maximum value of $143 million for the technology, its maintenance and associated training by DHS Domestic Nuclear Detection Office (DNDO).

VeriFinder supports enhanced 'in-the-field' decision-making by ensuring mobile detection and identification of radioactive threats with minimal false alarms. The lightweight, portable, and GPS-linked technology is ideal for searching and mapping wide areas and will identify and discriminate specific threats, providing user alerts including audio, vibration, LED and other situation-relevant information on the built-in display. VeriFinder exceeds the performance requirements of the ANSI N42.34 standard for handheld identification equipment.

Commenting on Symetrica's presence at the show, Jeff McCray, Symetrica Inc's Vice President of Business Development said: "We are very much looking forward to meeting government and military professionals and demonstrating our technology at the conference. The ability to rapidly detect masked threats with high levels of accuracy in harsh, real-world operating environments brings enhanced safety and security to all concerned".

The NDIA Annual CBRN Defense Conference and Exhibition promotes the positive exchange of information (scientific, technical, and operational) relating to defense against Weapons of Mass Destruction (WMD) and the ever-growing CBRN threat around the world.

# Nuclear Brexit

**By Hugh Gusterson**

Source: http://thebulletin.org/nuclear-brexit9620

June 30 – Those who voted for a "Brexit," with the avowed goal of "making Britain great again," may have set in motion a course of events that will result in Britain's unilateral nuclear disarmament.

For those who favor disarmament, this would be good. For those who hoped Britain's departure from the European Union would restore its glory on the world stage, it presumably would not.

Much of the public commentary on the prospective fallout of Brexit has focused on the anticipated damage to global markets, the probable shrinkage of British gross domestic product in the years following withdrawal from the EU, and a possible domino effect within Europe as other populations, incited by the British example, mobilize against the Brussels bureaucrats.

Insofar as pundits have speculated about the international security implications of Brexit, they have pointed out that British diplomats will be so focused on renegotiating trade agreements with the rest of the world that they will devote fewer resources to the turmoil in the Middle East and simmering tension with Russia, and that Britain will therefore be a less reliable ally for the United States. (This partly explains why Russian President Vladimir Putin greeted Brexit with a grin.) They assume, though, that Britain will remain strongly committed to NATO.

**One problem with this assumption is that the UK may no longer exist as a country within a few years.** It looks likely that, if Brexit proceeds, Scotland will withdraw from the United Kingdom, and there is a possibility that Northern Ireland will follow suit. In 2014, in a referendum on secession from the United Kingdom, 55 percent of Scots voted to stay and 45 percent voted to leave. But the subsequent referendum on leaving the EU has pushed many Scots to reconsider their position on Scottish independence. **In the Brexit referendum, every single district in Scotland voted to remain in the EU, and a decisive majority of Scots—62 percent—voted to stay**. It now looks as if the only way they can remain in the EU is to secede from the United Kingdom and apply for EU membership as a separate nation. **A poll taken after the Brexit vote found that 59 percent of Scots say they would now vote for independence from Great Britain.** Nicola Sturgeon, the shrewd and charismatic leader of the Scottish National Party, has stated her interest in moving toward a second referendum on Scottish independence.

For 30 years, the Scottish National Party said that an independent Scotland would stay out of NATO. It narrowly reversed that position in 2012, but it remains adamantly opposed to the stationing of any nuclear weapons in Scotland. That could be a problem since all of Britain's nuclear weapons are stationed in Scotland. Until 1998, the United Kingdom maintained a mix of submarine-launched ballistic missiles and tactical nuclear weapons, with some of the mix based in England. In 1998, Prime Minister Tony Blair's government retired the tactical nuclear weapons, leaving only the Vanguard submarines. Those submarines are headquartered at Her Majesty's Naval Base Clyde at Faslane in Scotland, with warheads stored eight miles away at Coulport. There is no obvious alternative site for them in England.

**A British parliamentary report in 2012, written in response to increasing concerns that Scotland might secede from the United Kingdom, concluded that finding a suitable base to replace Faslane and Coulport would be "highly problematic, very expensive, and fraught with political difficulties."** For one thing, it would take 10 to 20 years to construct a new base. And according to a 2014 study, doing so would cost English taxpayers about **£3 billion** (or some $4 billion at today's exchange rate, almost certainly an underestimate)—on top of the £20 billion it will already cost to replace the four decaying nuclear submarines. This money will be particularly hard to find if British GDP declines sharply, as predicted, following disengagement from the European single market.

**That is assuming a suitable new site could even be found, but the three sites that have been discussed in the media all have significant problems.**

**Milford Haven in Wales** is already the site of two oil refineries and two

liquefied natural gas facilities. This raises the danger that a submarine could collide with an enormous oil or gas tanker. (This may sound unlikely, but keep in mind that a French and a British submarine, both carrying nuclear weapons, collided in 2009.) Some British analysts have assumed that the oil and gas facilities would have to close if British nuclear weapons were moved to Milford Haven, hardly an inexpensive proposition.

Moving the submarines to the area near **Plymouth in the South of England** would require converting national trust land to military purposes, demolishing villages and relocating their inhabitants. It would also put a quarter of a million Plymouth residents within 3.5 kilometers (2.2 miles) of a site where live nuclear weapons were being handled, a situation it is assumed government officials would find unacceptable.

At a base at **Barrow-in-Furness in the North of England**, smaller submarines are already being built, but the port there is too shallow to accommodate Vanguard submarines without substantial dredging. (In 1967 a British Polaris submarine ran aground there when it was launched, much to the delight of antinuclear activists.) Also, the dock is small, accommodating fewer submarines at a time than Faslane, and the base is close to a town of 69,000.

In addition to Milford Haven, Plymouth, and Barrow-in-Furness, **two other options** are sometimes mentioned as potential sites for Britain's nuclear submarines, both outside the country. One is in Ile **Longue on the Northern coast of France** and the other is the **Kings Bay base in Georgia on the East Coast of the United States.** It is hard to imagine that the English nationalists who thought leaving Europe would increase British independence would be enthusiastic about moving their nation's "independent nuclear deterrent" to France, the detested rival across the Channel, and they would not be much happier about an American site. One can imagine the pleasure it might give the French to decline such an arrangement with their troublesome and temperamental neighbor.


It is becoming evident that, in addition to all the negative consequences of Brexit opponents warned about, there will be additional unforeseen and unintended consequences that will only become clear over time. In a supreme irony, one of those consequences may be that the English nationalist vote strips Britain of its status as a nuclear power.

**Those who sought to restore England's former glory could end up shrinking its military power, thus giving their critics yet another reason to deride them as "Little Englanders."**

***Hugh Gusterson*** *is a professor of anthropology and international affairs at George Washington University. His expertise is in nuclear culture, international security, and the anthropology of science. He has written two books on the culture of nuclear weapons scientists and antinuclear activists:* Nuclear Rites: A Weapons Laboratory at the End of the Cold War *(University of California Press, 1996) and* People of the Bomb: Portraits of America's Nuclear Complex *(University of Minnesota Press, 2004). Gusterson also co-edited* Why America's Top Pundits Are Wrong *(University of California Press, 2005) and its sequel,* The Insecure American *(University of California Press, 2009). He is currently writing a book on the polygraph. Previously, he taught at MIT's program on Science, Technology, and Society, and at George Mason's Cultural Studies program.*

# Confronting plutonium nationalism in Northeast Asia

**By Fumihiko Yoshida**

Source: http://thebulletin.org/confronting-plutonium-nationalism-northeast-asia9617

June 30 – Although President Obama trumpeted his commitment to nuclear disarmament at this year's Washington Nuclear Security Summit and more recently during his visit to Hiroshima, the White House has so far only discussed in whispers a far more pressing nuclear weapons-related danger—that **Japan and China may soon be separating thousands of nuclear bombs worth of plutonium from nuclear spent fuel each year. If this level of production occurs, South Korea and other countries will likely try to go the plutonium route**. If President Obama is to have a lasting legacy of nuclear threat reduction, his administration needs to do far more than it has to clarify just how harmful this plutonium proliferation would be to keeping peace in East Asia and the world.

**Japan has already accumulated about 11 metric tons of separated plutonium on its soil—enough for about 2,500 nuclear bombs. It also plans to open a nuclear spent fuel reprocessing plant at Rokkasho designed to separate eight tons of plutonium—enough to make roughly 1,500 nuclear warheads a year—starting late in 2018.** The Japanese plutonium program has raised China's hackles. **China's new five-year plan includes a proposal to import a reprocessing plant from France with the same capacity as Rokkasho. Meanwhile, South Korea insists that it should have the same right to separate plutonium as Japan has.**

Each of these countries emphasizes that it wants to separate plutonium for peaceful purposes. Yet in each country, there are skeptics who respond whenever this argument is made by a neighbor. China and South Korea suspect that Japan's large stockpile of plutonium and its plans to operate the Rokkasho plant are designed to afford Tokyo some latent form of nuclear deterrence, i.e. a nuclear weapon option. A huge new Chinese commercial plutonium separation program could give Beijing an option to make far more nuclear weapons than it already has. It is unclear what Russia might make of all of this, or North Korea. One possibility is that either


might use such "peaceful" plutonium production as an excuse to further expand its own nuclear arsenal. China might do the same as deterrence to Japan. If Seoul joined in, it would be even more difficult to cap North Korea's nuclear program.

American officials appreciate these dangers but so far have only hinted at them in public. On March 17th, Assistant Secretary of State Thomas Countryman testified before the Senate Foreign Relations Committee, noting that the United States was considering the possibility of not

renewing its 30-year-old civilian nuclear cooperative agreement with Japan as leverage to encourage a discussion of Japan's plutonium program. In an interview with the *Japan Times*, Jon Wolfsthal, senior director for arms control and nonproliferation at the National Security Council, said that if Japan were to change course, it would "find the United States to be supportive;" he was concerned that if Japan did not, a plutonium race in East Asia might ensue. Meanwhile, Senator Bob Corker, a Tennessee Republican and chairman of the Foreign Relations Committee, and several key Democrats have called for a time out in the commercial separation of plutonium in East Asia.

**So far, Japan's leadership has not reacted to those calls.** Indeed, it is pushing ahead, enacting a new law that mandates that power companies pay for the reprocessing of their spent fuel. The Abe administration also refuses to terminate its plutonium-fueled Monju prototype fast breeder reactor, even though safety and technical problems have prevented its operation for more than 20 years.

Why have Tokyo officials shown such an insensitivity to US concerns? They have made clear that they don't consider any of the statements US officials have made to constitute an official request from the US government, dismissing them as little more than private musings. "There are many different views in Washington policy circles," they said, also noting quite correctly that none of comments from Washington has been followed by concrete actions.

The Obama administration and Congress need to speak more clearly. As Countryman said, "(t)here is a degree of competition among the major powers in East Asia. It is a competition that in my view extends into irrational spheres…"

The United States can stop Japan from separating more plutonium and the spread of "plutonium nationalism" in East Asia only by bringing security issues to the front burner in politics and diplomacy. If the United States clearly announces that operations at Rokkasho constitute a security concern, Japan is almost sure to listen. Having the plutonium discussion between Japan and the United States is critically important; the Abe administration puts a high priority on security issues and is also very pro-United States.

**Now is the time to speak clearly on these security issues—before China and Japan lock themselves into a plutonium production rivalry that will make cooperation between them and South Korea on pressing issues, including North Korea's nuclear program, all the more difficult to secure.**

***Fumihiko Yoshida*** *is a visiting scholar at the Carnegie Endowment for International Peace. He was an editorial writer for the Asahi Shimbun with a special focus on nuclear weapons and arms control issues. He has served as a member of the Advisory Panel of Experts on Nuclear Disarmament and Non-Proliferation for Japan's Minister of Foreign Affairs.*

# Would Russia's undersea "doomsday drone" carry a cobalt bomb?

**By Edward Moore Geist**

*Bulletin of the Atomic Scientists*
*Volume 72, Issue 4, 2016; pp. 238-42.*
*Special Issue: Security at sea, and under it*
Source: http://www.tandfonline.com/doi/full/10.1080/00963402.2016.1195199

June 14 – Following the November 2015 "leak" of a classified slide purporting to show a Russian nuclear-armed and nuclear-powered drone intended to create long-lasting "zones of extensive radiological contamination," both Russian and Western observers have suggested that Moscow may be developing a cobalt bomb. This conjectural device, which served as the basis of the "doomsday machine" in the classic 1964 film *Dr. Strangelove*, would employ radioactive cobalt to create unusually intense long-lived fallout. This article reviews the history and science of the cobalt bomb to assess the likelihood that Russia is developing such a weapon. It argues that while the lethality of the cobalt bomb compares unfavorably to that of "conventional" thermonuclear weapons, it

might actually be a preferred means of creating long-lasting radioactive contamination because it could force an adversary to abandon territory while minimizing the number of immediate fatalities. But

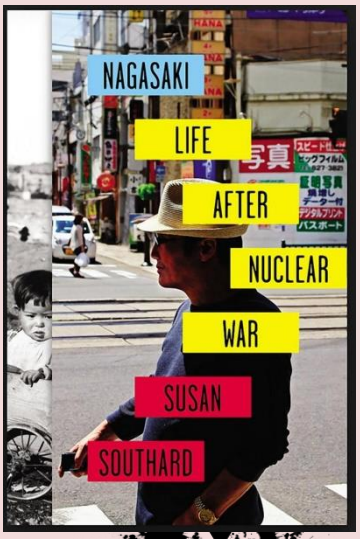

exploiting this principle in practice would be forbiddingly difficult because of the difficulty of predicting the ultimate distribution of the radioactive contamination, particularly for an underwater detonation like that envisioned for the "Status-6" drone seen in the Russian slide. While the underwater detonation of a massive cobalt or "conventional" nuclear weapon might create zones of long-lasting contamination, Russian decision makers would have little confidence that these areas would be in the intended locations, undermining the strategic case for such attacks. These findings suggest that the Kremlin is not pursuing radiological "doomsday bombs," even though the nuclear-powered drone on the slide seems to be a real research project.

## Russia's underwater "doomsday drone": Science fiction, but real danger

**By Igor Sutyagin**

*Volume 72, Issue 4, 2016; pp. 243-46.*
*Special Issue: Security at sea, and under it*
Source: http://tandfonline.com/doi/full/10.1080/00963402.2016.1194617

June 13 – A November 2015 video broadcast of a high-level meeting of Russian military and defense industry officials gave viewers a peek at Russia's ostensive plans for Status-6, an underwater nuclear drone to be armed with a high-yield thermonuclear warhead capable of radioactively contaminating vast coastal areas. The author's analysis is that the video was staged to send an intimidating message to the West, and that the drone itself does not fit the Russian pattern of maintaining absolute, centralized control over nuclear weapons delivery. Nevertheless, the author considers the leaked video to be cause for concern, because it demonstrates a growing Russian willingness to make nuclear threats as a means to achieving political ends.




## Unveiling the aftermath of nuclear war

Source: http://www.tandfonline.com/doi/full/10.1080/00963402.2016.1194049

June 13 – In this interview, author and theater director Susan Southard discusses her book *Nagasaki: Life After Nuclear War*, an award-winning history of the atomic bombing of Nagasaki and its enduring impact over 70 years. Southard talks about the physical

and emotional impacts of the bombing on its survivors; the differences between the Hiroshima and Nagasaki bombings; and the controversy surrounding the American narrative that the bombings were necessary to end the war and save American lives. She emphasizes the importance of survivors' stories for putting nuclear war in historical context, and for understanding the ongoing risk of an intentional or accidental nuclear explosion.

# Fukushima 5 years after

## (and the stupidity of a young photographer...)

Source: http://imgur.com/a/KabxJ

Malaysian photofrapher Keow Wee Loong sneaks into Fukushima's Red Exclusion Zone and shows a town untouched since March 2011 that has never been seen by the public.Never seen before photo of the fukushima exclusion zone. When i enter the red zone, i can feel a burning sensation in my eyes and thick chemical smell in the air. before i went there the authority told me that i need a special permit to visit this town and it take 3-4 weeks to get the approval from the local council,, well too much bureaucracy bullshit for me..so i just sneak in the forest to avoid cops on the road ...AND IT WAS AMAZING !!!!!, I still remember what is like to only have a GPS and google map walking in the wood at 2am in the morning to get into the town of okuma,futaba and namie. Have you ever wonder what is like in fukushima exclusion zone now ??? . to feel what is like to be the only person walking in the town when you have 100% full access to every shop and explore??. when i was young i always had a dream like this, If i'm alone in a supermarket i will eat all the chocolate up XD .... everything is exactly where it is after the earthquake struck this town . the reident started to evacuate the town when tsunami warning came in ....hours later the fukushima daichi power plant

exploded that lead to harmful radiation leaked. The radiation level is still very high in the red zone. not many people seen this town for the last 5 years...is like it vanished ... i can find food,money,gold,laptop and other valuable in the red zone....I'm amaze

that nobody looted this town clean. unlike chernobyl the entire town is been looted clean. this is the difference between chernobyl disaster and the fukushima disaster

# Nuclear weapons have almost been launched accidentally 13 times – it's time to stop believing in the fantasy that Trident keeps us safe

**By Caroline Lucas**

Source: http://www.independent.co.uk/voices/a-recent-report-showed-13-times-nuclear-weapons-were-almost-launched-accidentally-its-time-to-scrap-a7141296.html

July 17 – Today, MPs will be making a decision that will define Britain's place in the world for generations to come. Either we replace our multi-billion pound Trident missile capability or we join the vast majority of other countries in the world and become a nuclear weapons-free state.

The vote takes place at a time of heightened tension across the world, and the security of our country should be at the forefront of every MP's mind when they walk through the voting lobbies this evening.

It is my firm view, based on the best available evidence, that renewing Trident will not only fail to improve Britain's security, but in fact poses significant dangers to us. These weapons of mass destruction have the potential to cause death on an unimaginable scale, and they do nothing to hinder the real threat of lone gunmen or extremists. Their very presence here – and the transport of nuclear warheads on our roads – is not only a target for terrorism but a continued risk of accidents linked to human error or technical failure. A recent report from Chatham House confirms this threat, listing 13 occasions from across the world when nuclear weapons were nearly launched accidentally. These weapons present a huge risk – and there's no evidence to suggest they keep us any safer.

If we're serious about ridding the world of nuclear weapons and fulfilling our obligations under the international Nuclear Non-Proliferation Treaty, then genuine disarmament is non-negotiable. **Keeping these weapons sends a dangerous signal to the rest of the world that security is dependent on being able to use weapons of mass destruction, and thus drives proliferation.**

The UN is currently working on a treaty to ban nuclear weapons. Britain can play a part in ridding the world of

these weapons, but not if we refuse to lay down our own nuclear arms.

Trident isn't only a security risk. It's also a colossal waste of precious resources. **Instead of spending over £100bn on this Cold War relic we could invest in what our armed forces really need: the best possible safety equipment and decent homes for service families.** And we could use the funds to bolster our ailing public services too: **giving vital extra money to schools and hospitals**.

If we scrap Trident, we need to guarantee the jobs and economic security of those working at Faslane, Aldermaston and elsewhere. A Defence Diversification Agency would help ensure a just transition for the 11,000 people whose jobs are directly dependent on Trident.

And there is no shortage of alternative industry. Investing in renewable energy would create millions more jobs than nuclear weapons will ever will. The Clyde region – home to the UK's nuclear weapons system – is a hub in Scotland for the renewable energy industry. **The West Coast of Scotland is by far the best site for wave technology in the UK.**

Trident has become a totem in Britain. For many MPs it signifies safety and security, when it offers nothing of the sort. Arguments in favour of Trident are so bound to a particular, narrow view of "Britain's place in the world" that clear evidence is often dismissed out of hand.

**So before voting, I'd urge MPs to think about this:** would you vote for Trident if we didn't have it already? Imagine you were presented with plans for a brand new weapon that could kill millions but would never be used, that contravenes international treaties and that presents a genuine risk to our population, and takes precious money away from our vital public services. Would you even consider voting for such a proposal if those weapons weren't already in place?

Britain's history as a nuclear weapons state does not have to dictate our future. These missiles shouldn't be our bargaining chip on the world stage. **I am voting against Trident because I believe that we are safer without weapons of mass destruction in our country.** I hope a majority of MPs join me in doing the same.


***Caroline Lucas** is Member of Parliament for Brighton Pavilion and leader of the Green Party of England and Wales.*

**EDITOR'S COMMENT:** What a wonderful article from a politician from another Galaxy!

# 300 nuclear security agents to be deployed for Rio Olympics

Source: http://news.xinhuanet.com/english/2016-07/21/c_135528664.htm

July 20 – **Nearly 300 nuclear security experts will be deployed for the upcoming Olympic Games**, Agencia Brasil reported on Wednesday.

The nuclear security agents, trained in radiation detection, were also deployed at the 2014 World Cup of football.

"Close to 300 agents from the National Nuclear Energy Commission (CNEN) are to be engaged in the Rio 2016 Olympic and Paralympic Games," the agency said.

"Their work will focus on the prevention and identification of nuclear risks and emergency situations, as well as the response to such incidents," the agency added.

In the wake of recent terrorist strikes, Brazil has bolstered its security scheme for the games, including increasing the number of military troops to be deployed in and around Olympic venues and strategic sites.

Following last week's terrorist strike in Nice, France, the government announced it would increase the buffer zone between Olympic venues and circulating traffic, as well as tighten controls for accessing stadiums.

The Olympics will officially kick off with the opening ceremony on Aug. 5, and continue through Aug. 21. The Paralympics will be held on Sept. 7-18.

# Secret side deal cuts Iran's breakout time in half in little more than a decade

Source: http://thehill.com/policy/defense/288191-secret-document-lifts-key-iran-nuke-constraints-report

July 19 – **Key restrictions on Iran's nuclear program will ease in slightly more than a decade, cutting in half the time Iran would need to build a nuclear weapons.**

The AP reported on Monday that it had obtained a document from a source inside the International Atomic Energy Agency (IAEA) in Vienna — a document which was the only secret portion to last year's agreement between Iran and the P5+1 powers. The *Hill* reports that the document said that **after a period of between eleven to thirteen years, Iran could replace its 5,060 older, and inefficient, centrifuges with up to 3,500 advanced centrifuges**.


**Experts note that these advanced centrifuges are five times as efficient as the older centrifuges, thus cutting the breakout time – that is, the time Iran would need to make a nuclear weapon — from one year to about six months.**

U.S. and Western intelligence services have said that Iran currently has no plan to produce a weapon.

The centrifuge replacement provision appears to be part of the deal's "sunset clause," Omri Ceren of The Israel Project, a pro-Israel group campaigning against the nuclear agreement, told the *Hill*.

Critics of the agreement told lawmakers that limits on Iran's centrifuge research and development were too weak even during the first ten years of the agreement, but whether or not one agrees with that assessment, there is little doubt that the centrifuge replacement clause would allow Iran, once it has replaced the old centrifuges with the more advanced ones, to rush toward the bomb if it so decided.

The *Hill* notes that David Albright, president of the Institute for Science and International Security, said as much in testimony before the Senate Foreign Relations Committee on 25 June 2015, one month before the nuclear deal was finalized.

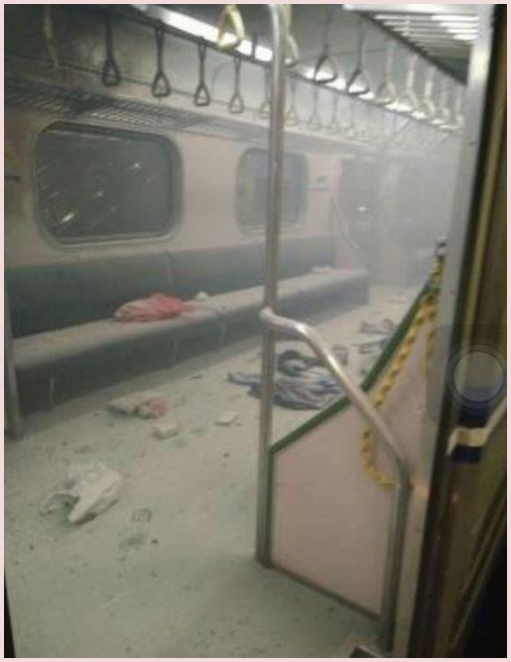
"No bans exist on Iran's research and development of the IR-6 and IR-8 centrifuges, the latter of which is up to sixteen times more powerful than the IR-1 centrifuge," he said.

**"Failing to achieve such bans, the interim agreement does not appear to mitigate the risks of Iran being able to deploy these more powerful centrifuges after year 13, other than some negotiators stating that they believe that Iran will have trouble actually deploying them in the future," he said.**

# Huge blast rips through train in Taiwan

Source: http://metro.co.uk/2016/07/07/huge-blast-rips-through-train-in-taiwan-5993207/

**July 07 – At least 21 people have been injured following an explosion on a train in Taiwan.**
The cause of the blast, at the Songshan railway station in the capital Taipei, is not yet known.



**According to local reports, a man in his forties entered the carriage, put something down and left the train.** Shortly afterwards, a fire broke out and more than a dozen people were taken to hospital.

**Authorities said the blast was most likely caused by a 'firecracker-like device'.**
Pictures from the scene show carriages filled with dust in the aftermath, as firefighters arrive.
'I want to tell the public to rest assured as we have heightened the alert for the security of public areas and transport systems,' Premier Lin said after he visited the injured in hospital.

Police are investigating.

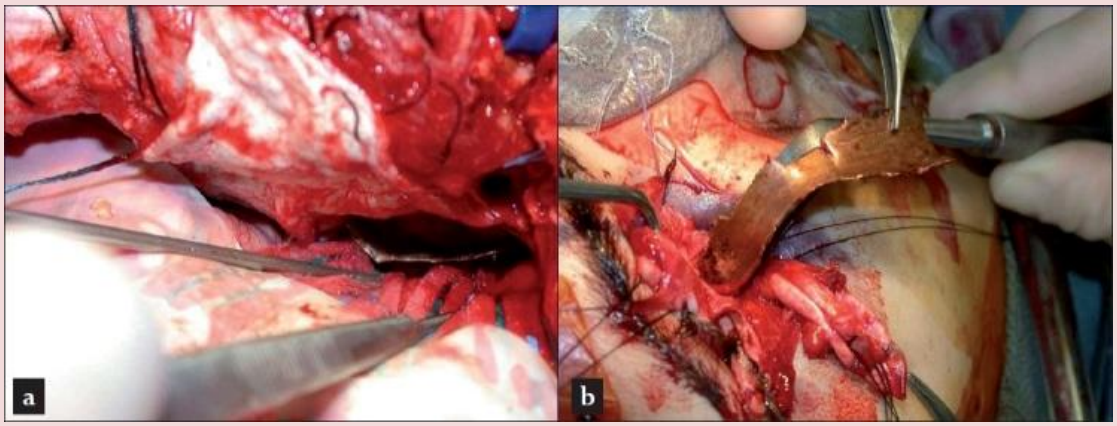
**EDITOR'S COMMENT:** It looks like a "pipe bomb". A pipe bomb is an improvised explosive device, which uses a tightly sealed section of pipe filled with an explosive material. The containment provided by the pipe means that simple low explosives can be used to produce a relatively large explosion, and the fragmentation of the pipe itself creates potentially lethal shrapnel. The bomb is usually a short section of steel water pipe containing the explosive mixture and closed at both ends with steel or brass caps. A fuse is inserted into the pipe with a lead running out through a hole in the side or capped end of the pipe. The fuse can be electric, with wires leading to a timer and battery, or can be a common fuse. All of the components are easily obtainable. For a pipe bomb, the US Department of Homeland Security recommends a minimum of 21 m (69 ft), and preferred distance of 366 m (1,201 ft).

## Notable incidents

- On 4 May 1886, a pipe bomb was thrown during a rally at Haymarket Square in Chicago, Illinois, United States. It reached a police line and exploded, killing policeman Mathias J. Degan. The bomb was made from gas-pipe filled with dynamite and capped at both ends with wooden blocks.

- On 27 July 1996, Eric Rudolph used a pipe bomb in the Centennial Olympic Park bombing during the 1996 Summer Olympics in Atlanta, Georgia, United States. It killed two people and injured 111.

- On 25 July 1997, during the July 1997 riots in Northern Ireland, a well-known loyalist was found dead in Belfast. He is thought to have died in a premature pipe bomb explosion at an arms dump.
- On 5 June 1999, a Protestant civilian was killed when a pipe bomb was thrown through the window of her house in Portadown, Northern Ireland. She was married to a Catholic man. Loyalist Volunteer Force (LVF) members were blamed, although the group denied responsibility.
- On 20 April 1999, Eric Harris and Dylan Klebold used pipe bombs during the Columbine High School massacre.
- On 11 November 2001, an Ulster Defence Association (UDA) member died in a premature pipe bomb explosion during a riot in Belfast, Northern Ireland.
- On 3 January 2002, another UDA member died in a premature pipe bomb explosion in Coleraine, Northern Ireland.
- On 10 August 2006, four pipe bombs were found in and around the city of Salem, Oregon, United States. Some suspected a "serial pipe bomber" was at fault. A man was later arrested and charged.




- On 11 December 2010, a suicide bomber detonated one out of six pipe bombs close to a major shopping district in Stockholm, Sweden, killing himself with no other casualties. The incident is known as the 2010 Stockholm bombings.
- In January 2011, a potentially deadly pipe bomb was discovered along the route of a Martin Luther King Jr. memorial march in Spokane, Washington. The bomb, which was shaped, was defused and there were no casualties.
- On April 19, 2013, the Boston Marathon bombing suspects, Dzhokhar and Tamerlan Tsarnaev, are alleged to have thrown pipe bombs out of an SUV they had carjacked in a shootout with Boston police.
- On September 20, 2013, 18-year-old Skylar Murphy was caught with a pipe bomb at Edmonton International Airport. The Canadian Air Transport Security Authority staff confiscated the device, but permitted him to board his international flight, and only

informed the Royal Canadian Mounted Police four days later. Murphy was arrested when he returned to Canada on September 27, and later sentenced to one year's probation and fined $100.

## Islamic State fighters using drones with IEDs and spy cameras, says Pentagon

Source: http://www.telegraph.co.uk/news/2016/07/07/islamic-state-fighters-using-drones-with-ieds-and-spy-cameras-sa/

July 07 – **Islamic State fighters are posing a growing threat to US and Iraqi forces by deploying small commercial drones armed with improvised explosives devices or spy cameras that can evade detection, according to the Pentagon.**

The threat led the Defense Department office charged with monitoring and countering improvised explosive devices to ask that Congress approve shifting $20 million to provide seed money for a counter-drone effort.

The funds would bankroll moves to "identify, acquire, integrate and conduct testing" of technologies that would "counter the effects of unmanned aerial systems and the threats they pose to US forces," according to a budget document sent to Congress last week. It was part of a request for approval to shift $2.5 billion in defense funds approved for this year from other purposes to reflect changing needs.

The request underscores that commercially available drone technology has proliferated beyond hobbyists to adversaries. In its latest annual report on Iran's military capabilities, the Defense Department said the Islamic Republic is fielding armed drones among other "increasingly lethal weapon systems." At the Pentagon, the police force has posted "no drone" signs around the sprawling complex along with the usual "no photos" reminders.

In the fight against Islamic State, "small and tactical unmanned aerial systems" equipped with improvised explosive devices, or IEDs, "pose a direct threat to US and coalition forces," according to the budget document.

"Just days after the Iraqi forces began occupying Makhmour in Ninevah Province, a video surfaced" on an Islamic State web site "showing forces on the ground there, demonstrating they were using the footage in both reconnaissance and propaganda roles," Army Colonel Chris Garver, the Defense Department's top spokesman in Iraq, said in an e-mail.

The Joint Improvised-Threat Defeat Agency, the Pentagon office that has worked to combat improvised explosive devices since the 2003 Iraq war, has seen Islamic State fly "quadcopters and fixed-wing type drones you can buy commercially" as "both an IED delivery system and for reconnaissance," its spokesman, David Small, said in an e-mail.

**The commercial drones used by Islamic State have weighed about 50 pounds or less, he said**. He didn't provide details on the number of attacks or resulting casualties.

In addition to using drones with full-motion video to look for attack opportunities and to monitor Iraqi Security Forces, Mr Small said the pilotless aircraft are being used to provide target information for vehicles carrying suicide bombs.

Mr Small said "there is a wide array of technology angles we are looking into" to defeat the drones that would be deployed within two years, if not sooner.

## Can next-generation bomb 'sniffing' technology outdo dogs on explosives detection?

**By David Atkinson**

Source: http://www.homelandsecuritynewswire.com/dr20160707-can-nextgeneration-bomb-sniffing-technology-outdo-dogs-on-explosives-detection

July 07 – With each terrorist attack on another airport, train station, or other public space, the urgency to find new ways to detect bombs before they're detonated ratchets up.

Chemical detection of explosives is a cornerstone of aviation security. Typically called "trace detection," this approach can find minuscule amounts of residue left behind after someone handles an explosive. A form of this technology called ion mobility spectroscopy is what Transportation Security Administration officers are using when they swab and test your laptop, hands or other items at the airport. In a few seconds, a sample is vaporized, and the resulting chemical ions are separated by molecular size and shape, triggering an alarm if an explosive compound is detected.

But this method is labor-intensive and slow for large volumes of stuff, and its effectiveness can depend on the sampling skill of the officer. It relies on contact sampling, which requires security personnel to have access to surfaces where residue may have been left. That's not useful if a bomber has no intention of going through a security line and having his personal effects searched.

Some security teams rely on dogs, which can be trained to sniff out explosives using their exquisite sense of smell. But the logistics and training involved with the routine deployment of canines can be arduous, and there are cultural barriers to using dogs to directly screen people.

What researchers have wanted to develop for a long time is a new chemical detection technology that could "sniff" for explosives vapor, much like a canine does. Many efforts over the years fell short as not being sensitive enough. My research team has been working on this problem for nearly two decades – and we're making good headway.

**More and more sensitive**

The one big hurdle to engineering some kind of technology to rival a dog's nose is the extremely low vapor pressures of most explosives. What we call the "equilibrium vapor pressure" of a material is basically a measure of how much of it is in the air, available for detection, under perfect conditions at a specific temperature.

Commonly used by military forces around the world, nitro-organic explosives such as TNT, RDX, and PETN have equilibrium vapor pressures in the parts per trillion range. To reliably sniff out related vapors in operational environments, like a busy check-in area of an airport, the detection capability would need to be well below that – down into the parts per quadrillion range for many explosives.

**High Explosives Acronyms**

- ***TNT*** = *Trinitro Toluene*
- ***PETN*** = *PentaErythritol TetraNitrate*, also known as *pentrite*. PETN is also used as a vasodilator, similar to nitroglycerin. Used as medicine for heart diseases.
- **RDX** = Cyclotrimethylenetrinitramine
- **HMX** or **Octagon** = Cyclotetramethylene-tetranitramine (related to RDX)

These levels have been beyond the capability of trace detection instrumentation. Achieving a 325 parts per quadrillion level of detection is analogous to finding one specific tree on the entire planet Earth.

But recent research has pushed the detection envelope into that part-per-quadrillion range. In 2008, an international team used an advanced ionization technique, called secondary electrospray ionization mass spectrometry, to get better than part per trillion level detection of TNT and PETN.

In 2012, our research team at Pacific Northwest National Laboratory (PNNL) achieved direct, real-time detection of RDX vapors at levels below 25 parts per quadrillion using atmospheric flow tube mass spectrometry (AFT-MS).

Sensitivity for a mass spectrometer is related to how many of the target molecules can be ionized and transferred into the mass spectrometer for detection. The more complete that process is, the better sensitivity will be. Our AFT-MS scheme is different because it uses time to maximize the benefits of the collisions of the explosive vapor molecules with air ions created from the ion source. It is the extent of reaction between the created ions and the explosives molecules that defines the sensitivity. Using AFT-MS, we've now expanded the capability to be able to detect a suite of explosives at single-digit part per quadrillion level.

**Next step: putting it into practice**

So we've moved the state of the art of chemical-based explosives detection into a realm where contact sampling is no longer necessary and instruments can "sniff" for explosives in a manner similar to canines.

Instruments that have the vapor detection capability of canines and can also operate continuously open up exciting new security screening possibilities. Trace

detection wouldn't need to rely on direct access to suspicious items for sampling. Engineers could create a noninvasive walk-through explosive detection device, similar to a metal detector.

The real innovation is in the direct detection of the vapor plume, enabled by the extreme sensitivity. There is no longer a need to collect explosive particles for vaporization – as is the case in past trace detection technologies that use loud air jets to dislodge particles from people. Instead, the greater sensitivity means the air could simply be constantly sampled for explosives molecules as people pass through.

This approach would certainly make airport checkpoints less onerous, improving throughput and the passenger experience. These types of devices could also be set up at entrances to airport terminals and other public facilities. It would be a major security leap to be able to detect explosives that are entering a building, not only when passing through a checkpoint.

A deployed vapor detection capability would also increase safety by adding a second independent form of information to what scanners have available. Currently, most screening techniques, such as x-ray and millimeter wave imaging, are based on spotting anomalies – a TSA operator notices a strange shape in the image. A vapor detection technology would add to their toolkit the ability to identify specific chemicals.

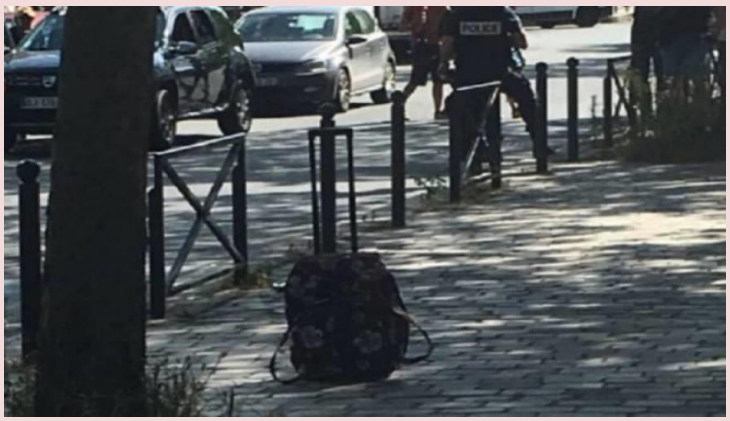
It allows for a two-pronged approach to finding explosives: spotting them on an image and sniffing them out in the vapor plume emitted by a checked bag or a person. It's like recognizing a person you know but haven't seen in a long time; both seeing a recent picture and hearing their voice may be necessary to identify them, rather than just one of those pieces of information on its own.

Inspired by the tremendous detection capabilities of dogs, we've made remarkable advances toward developing technology that can follow in their footsteps. Deploying vapor analysis for explosives can both enhance security levels and provide a less intrusive screening environment. Continuing research aims to hone the technology and lower its costs so it can be deployed at an airport near you.

***David Atkinson** is Senior Research Scientist, Pacific Northwest National Laboratory.*

## Police carry out controlled explosion outside France team hotel

Source: http://www.skysports.com/football/news/19692/10497899/police-carry-out-controlled-explosion-outside-france-team-hotel



July 10 – Police in Paris carry out a controlled explosion on a suspicious bag near the French football team's hotel ahead of the Euro 2016 final.

French police carried out a controlled explosion on a suspicious bag found outside the France team hotel in Paris.

French police became concerned when a bag was left unattended yards from the French team bus and took decisive action, ahead of the national team's final against Portugal at Stade de France.

**EDITOR'S COMMENT:** **Why controlled explosion?** There are portable x-ray detectors (i.e. FlatScan2-TPXi or FlatScan2-15) and remote liquid explosives' systems (using photodissociation followed by laser-induced fluorescence - PD-LIF technology) that can do the job in a safe manner – especially within the urban web. So why choose explosion that poses certain dangers for the personnel involved?

# Super-sniffer mice detect land mines, decode human olfactory system

Source: http://www.homelandsecuritynewswire.com/dr20160712-supersniffer-mice-detect-land-mines-decode-human-olfactory-system

July 12 – Researchers at Hunter College, part of the City University of New York, have **created super-sniffer mice that have an**


**increased ability to detect a specific odor,** according to a study published 7 July in *Cell Reports*. The mice, which can be tuned to have different levels of sensitivity to any smell by using mouse or human odor receptors, could be used as land-mine detectors or as the basis for novel disease sensors.

The technology, **a transgenic approach to engineering the mouse genome**, could also provide researchers with a way to study human odor receptors. "This is one of our five basic senses, yet we have almost no clue how odors are coded by the brain," says lead investigator Paul Feinstein, an associate professor of biological sciences at Hunter. "It's still a black box."

The nature of the odor receptors was discovered in 1991, a Nobel Prize winning feat, but exactly how the olfactory system wires itself still is not well understood. The noses of mammals contain a collection of sensory neurons, each equipped with a single chemical sensor called a receptor that detects a specific odor. In mice, as in humans, each neuron selects only one receptor. Collectively, neurons choose an even distribution of receptors, so each of the thousand distinct receptors is represented in about 0.1 percent of neurons.

Cell Press says that in an effort to understand the mechanism these neurons use to choose a specific receptor, Feinstein tinkered with the mouse genome. He **introduced the DNA for an odor receptor gene transgenically, by injection into the nucleus of a fertilized egg cell.** He also added an extra string of DNA to the gene sequence to see if it would alter the probability of the gene being chosen. After a few attempts, he found a string that, when copied four or more times, worked.

More copies of this extra string of DNA resulted in a series of super-sniffer mice with increasing numbers of neurons expressing the selected receptor, a well-characterized receptor that detects acetophenone, which has a sweet smell similar to jasmine. The mice still maintain a relatively even distribution of other odor receptors. "We don't know how the neuron performs singular gene choice yet, but we can increase the probability of a given choice occurring," says Feinstein.

**In parallel, post-doctoral researcher Charlotte D'Hulst was trying to replace a mouse receptor gene with a human one.** Even though such gene swapping is standard practice in other fields, it did not work. It wasn't the first time researchers had been stymied by olfaction. Repeated attempts in the field to study odor receptors by growing them in cells in Petri dishes have also led to dead ends.

As a result, human olfaction receptors are poorly understood. "Without understanding how odors bind to receptors, people have no rational way of designing new odors," says D'Hulst. "They also have no way of boosting the diminished smell capacity in patients with diseases such as Parkinson's."

So D'Hulst abandoned gene swapping and tried Feinstein's transgenic super-sniffer technique to insert a human receptor gene into the mouse. It worked. "We have developed a system where we can study human odor receptors and finally determine how human odor coding works," says Feinstein.

The team validated that the mice do indeed have an amplified sense of smell for the given receptor. They first used fluorescent imaging in live mice to trace the activation of the amplified odor receptor in response to the receptor's corresponding odor. These tests gave visual confirmation that the receptors are

functional and present in greater numbers than others.

In a standard behavioral test in which animals were trained to avoid an odor known to bind the transgenic receptor, the super-sniffer mice were able to detect the presence of this unpleasant odor in water at levels two orders of magnitude lower than those detectable by mice without super-sniffer abilities. "The animals could smell the odor better because of the increased presence of the receptor," says D'Hulst.

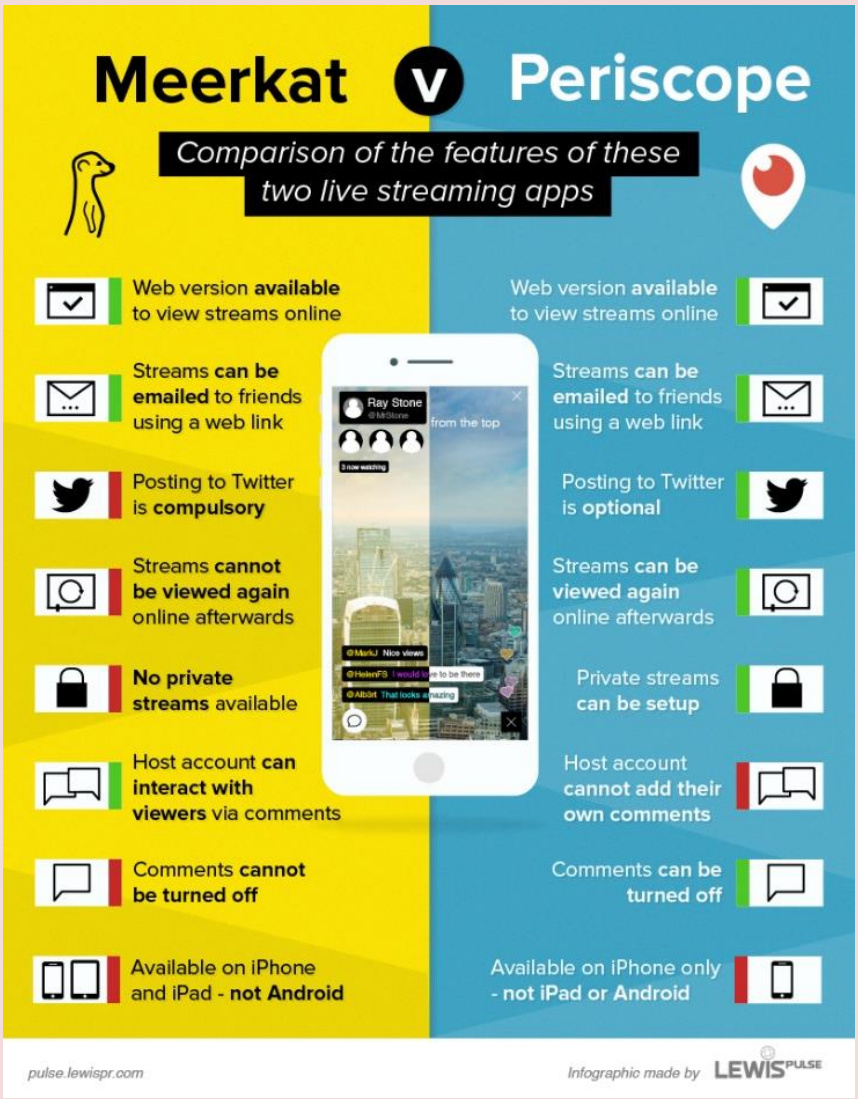
**The team is now working towards commercializing their technology and has founded a company called MouSensor, LLC.** The Feinstein lab has received funding from the Department of Defense to develop super-sniffing rats that can be trained to detect TNT and potentially find land mines. The researchers also envision applications of the MouSensor for developing a type of nose-on-a-chip as a means of diagnosing disease using chemical detection profiling. "We have these millions-of-years-old receptors that are highly tuned to detect chemicals," says Feinstein. "We think we can develop them into tools and use them to detect disease."

*— Read more in Charlotte D'Hulst et al., "MouSensor: A Versatile Genetic Platform to Create Super Sniffer Mice for Studying Human Odor coding," Cell Reports (7 July 2016) (DOI: http://dx.doi.org/10.1016/j.celrep.2016.06.047); see also Michael Price, "These 'supersniffer' mice could one day detect land mines, diseases," Science (7 July 2016).*

# Social Live Streaming: A New Medium for Terrorist Propaganda?

Source: http://www.adweek.com/socialtimes/social-live-streaming-a-new-medium-for-terrorist-propaganda/641333

June 24 – Meerkat and Periscope have opened the doors for social live streaming, and now even Tumblr and all the major social sites are vying for market share. However, a live feed is harder to moderate, and it seems that live streaming has already become an avenue for terrorism and propaganda.




Forbes columnist **Kathleen Chaykowski** reported that a recent terror suspect live-streamed via Facebook Live from the scene of a murder and hostage situation last week, and threats of terror attacks against soccer tournament EUFA EURO 2016 were also posted. Both were removed, but not before being seen by other Facebook users.

A Facebook spokesperson said in a statement:

We are working closely with the French authorities as they deal with this terrible crime. Terrorists and acts of terrorism have no place on Facebook. Whenever terrorist content is reported to us, we remove it as quickly as possible. We treat takedown requests by law enforcement with the highest urgency.

Social networks are constantly facing users uploading and sharing content from terrorists, and live streaming provides another medium for content which may be harder to police than others. Community reporting and automatic detection can help curb most offending content on social networks, but when that content is live, a site would need a constant moderation team ready to shut down any offending stream if they hoped to get ahead of the problem.

Chaykowski noted that Facebook already has a 24-hour moderation team. Unfortunately, that may not be enough to silence the use of live streaming by terrorists and help get information to relevant authorities. According to the journal Science, a team of researchers developed a method for identifying patterns in pro-terrorist groups and created an algorithm that could be used to predict future behavior from these groups.

Algorithms could be a helpful tool, but it's practically impossible to totally eliminate this kind of content from social sites now that extremist groups have realized the power of social. If live streaming is to be a way for users to broadcast and interact with immediacy, any significant impediment to broadcasting could hamper the experience.

In essence, social networks are content gatekeepers, and some have been accused of abusing their position of power. There's a fine line social platforms walk by including live streaming in their suite of tools, between immediacy and control, and between moderation and open communication.

# How will Brexit affect cybersecurity in the UK? What the experts are saying about leaving the EU

**By Agamoni Ghosh , India Ashok**

Source: http://www.ibtimes.co.uk/how-will-brexit-affect-cybersecurity-uk-what-experts-are-saying-about-leaving-eu-1567008

June 23 – Britain's European Union referendum polling day is here and it has the tech industry worried, particularly cybersecurity firms. While the voters' decision to either remain or leave the EU is to be confirmed, the cybersecurity industry in the UK is deeply concerned and largely do not favour a Brexit, just like the tech industry in the UK as a whole.

London's technology sector has openly spoken out against the possibility of a Brexit with an overwhelming opposition against Britain exiting the EU, according to a survey of members of Tech London Advocates. The survey, which was conducted among 3,000 senior members of the capital's tech scene, showed that 87% opposed Brexit amid fears of being unable to attract European customers, attract talent from overseas, and gain cooperation from overseas companies.


Under the IT and tech industry umbrella comes the relatively new but pivotal cybersecurity industry. The community in the UK is relatively compact but fairly inclusive.

The industry actively recruits its staff, especially for R&D (Research and Development) from both within the UK as well as from Europe and elsewhere. Ease of movement between the UK and other EU states is key to security researchers, both for professional as well as private purposes.

**IBTimes UK** spoke to some cybersecurity firms operating in the UK in efforts to understand how Brexit may affect the industry and consequently the security of UK businesses.

Currently, Europe is an important source of talent for the UK which has been experiencing nothing short of a skills crisis in technology. A recent study conducted by the Science and Technology Committee and presented to the House of Commons highlights the alarming lack of "digital skills" among people in Britain.

This dearth of skilled tech labour compels cybersecurity firms to seek labour from other EU as well as non-EU countries. A Brexit could result in these companies operating in the UK engaging in a mass exodus to return to the EU fold. Removing a flow of talent and expertise from Europe could deprive UK tech companies of an essential ingredient for sustained growth.

Additionally, given that Britain's tech scene - especially in London - is quite multicultural, start-up founders worry that leaving the European Union will make it much harder to hire the best employees.

Brian Spector, CEO of Miracl, a cybersecurity firm based and operating in UK in this regard says, "The UK has a well-documented shortage of tech talent that means it simply cannot compete globally without tapping into highly-skilled overseas workers. Splitting away from Europe would make it even more difficult for UK tech firms to compete with the US tech giants, because their talent pool would be so much larger than ours. To cut ourselves off from the rest of Europe therefore does nothing to protect the UK's reputation as being open for business."

Lastline on the other hand is an American cybersecurity firm, but has an established branch in the UK. They are of the opinion that while the firm's sales channels are unlikely to be affected, there is a possibility that "unforeseen issues" may impact the firm's equipment shipping process.

"Our R&D department in Shoreditch, London, comprises of developers from several different EU nations – including Italy, Finland and Germany. These guys live and work in London and travel around Europe for research purposes – as well as to return home to visit family. There is an obvious concern post-Brexit that the rules might change regarding their ability to stay in the UK and

or travel freely around Europe. We will have to wait and see if these concerns are founded or not and will of course support our team to remain employed and productive," says Jamie Moles, security consultant for Lastline.

The firm adds that if a Brexit was to take place, they have solid connections with Academic organisations and Universities throughout Europe and the US to resolve their workforce issues. This indicates that cyber-security companies like Lastline, that have so far had a smooth ride in the UK, may start building a stronger base in other European nations, if they perceive the talent shortage and the cost of operation are mounting.

**Escalating cost of operations**

A considerable number of cyber-security firms currently in the UK fall under the start-up category given the basic capital required for setting up shop is comparatively lower than a traditional hardware or equipment-based tech company. Experts have warned that if a Brexit took place, the operations for UK start-ups may become more expensive, depending on what new laws they have to abide by.

"We are a distributed organisation with employees based throughout Europe, and the prospect of having to apply for visas and fight our way through reams of red tape to access the highly-skilled workforce that's essential to our business, could really slow us down. The UK start-up scene is fast and furious, and to disconnect it from the rest of Europe would be a backwards step," says Brian Spector.

**How Brexit will affect cyber-security data sharing**

**Brexit could also impact data and privacy laws in the country, with the very real possibility of laws undergoing changes, which may in return affect citizens' privacy and security.** EU laws have been traditionally designed to create a "digital single market" and they could take a particularly big hit should the UK leave. For example, data sharing "safe harbor" agreements across EU countries — like the EU-United States which was invalidated earlier this year — might not apply to the UK.

The way data is handled in Britain has so far been modelled on European regulation, with the GDPR (General Data Protection Regulation), a new EU-wide regulatory regime, scheduled to come into force in 2018. If Britain leaves the EU, an air of uncertainty is prevalent, on whether it will simply choose to adopt a regulatory framework for data that mirrors the GDPR - or create a radical new framework of its own.

Highlighting the issue, Spector says, "The right to privacy is a highly developed area of law in Europe. If Britain were to leave the EU, and its extensive human rights legislation, it's likely to make it easier for future governments to access our data as and when they choose. This could mean that any software made by a British company could soon be perceived to be facilitating government spying on its customers' data."

**Threat of cyberattacks post Brexit?**

**Yet another scenario which could impact cybersecurity, is that cybercriminals may be induced to increase focus on conducting cyberattacks on the UK by capitalising on prospective bureaucratic loopholes, which may leave businesses vulnerable to such attacks.** This concern was echoed by security information service provider Comparitech.com.

"When you combine the fact that those in the know say the UK would become more vulnerable to cyberattacks with a reduction in privacy, the data protection landscape in the UK could become a completely different beast," Richard Patterson, director of Comparitech.com told IBTimes UK.

"We could end up in a situation where British citizens have far less protections than their EU counterparts from their own government's intrusions on one hand and on the other, subject to more cyber-crime."

A study by AlienVault earlier this week showed that almost 40% of IT security professionals believed leaving the EU would make the UK more vulnerable to cyberattacks. Moles is of the opinion however, that this would largely depend on how regulations are shaped up.

"The increase in vulnerability from cyberattacks depends entirely on whether EU laws and regulations that protect businesses and individuals are stopped from being enforced in the UK. Criminals will always look to take advantage of weaknesses in the system and the 'easy mark' to make a quick, low-risk profit," he says.

# Majority Of World's Airlines To Invest In Cyber Security: Report

Source: http://www.terrorismwatch.org/2016/07/majority-of-world-airlines-to-invest-in.html

July 06 – Amajority of the world's top airlines plan to invest in cyber security programmes, travel technology provider SITA said on Monday.

According to a survey of the world's top 200 airlines conducted by SITA, a majority (91 per cent) said that they plan to invest in cyber security programmes over the next three years.

The survey "SITA Airline IT Trends 2016" revealed that three years ago, less than half of airlines (47 per cent) had said that they were making advanced preparations to manage cyber risks.

"The focus on cyber security also reflects the move to the 'Internet of Things' (IoT) in which a vast number of physical objects will become connected to the internet," the travel technology major said in a statement.

"This enables tracking, data collection, analysis and control, which necessitates more security. An overwhelming majority of airlines (68 per cent) are investing in IoT programs in the next three years," it added.

# Cybercrime: 8.8m SAfricans victim in 2015

Source: http://www.iol.co.za/business/news/cybercrime-88m-safricans-victim-in-2015-2041922


July 06 – **New research unveiled on Wednesday by antivirus software maker Norton - a Symantec brand - has revealed that 8.8 million South Africans were the victim of cyber crime in the past year, at a cost of R35 billion.**

The Norton Cybersecurity Insights Report shows that this is despite growing concerns over online crime.

Norton's report contains the views of more than 18 000 consumers across 18 markets, including about 1 000 across South Africa.

"The good news is more and more consumers are aware of the risks of cybercrime but the bad news is they neither feel they are doing enough to prevent it, or feel that technology has prevented them from being able to do anything about it," says David Ribeiro, Head of Norton, Middle East and Africa.

"Despite personal experience, many South Africans continue to put themselves at risk when it comes to online activity."

**Other findings include:**

- 76 percent of South Africans believe that identity theft is more likely than ever before;
- 67 percent feel it is more difficult to control their personal information as a result of smartphones and the Internet;
- 78 percent of South Africans acknowledge the need to actively protect their information, but there is still some notion that security is an inconvenience;
- 58 percent of South Africans would rather cancel dinner plans with their best friend than have to cancel their credit/debit cards after their account has been compromised;
- The same percentage would rather endure a terrible date than deal with credit/debit card customer service after a breach or hack.

Norton notes online crimes are increasingly prevalent with more than 1 in 7 people having had unauthorised access to a social network profile.

**At risk**

Compared to their global counterparts, South Africans have heightened sensitivity to online information compromises – 76 percent believed identity theft was more likely than ever before and 67 percent said it was easier to control personal information before smartphones and the Internet.

South Africans are more likely than their global counterparts to consider themselves tech savvy. Despite this, South African millennials are less likely to take personal responsibility for their security - nearly 1 in 3 millennials admits to abandoning an account rather than deleting it simply because it was easier.

Millennials and Generation Xers are equally likely to have been victims within the last year at a staggering 39 percent and 37 percent respectively. However, only 2 percent of South Africans aged 55 and over experienced cybercrime during this period.

**Other findings**

Other findings from the report include:

- Nearly 1 in 5 people do not have a password on his/her smartphone or desktop computer;
- 6 in 10 consumers say it is riskier to share their email passwords with a friend than lend him/her their car for a day;
- Storing credit/banking information in the cloud is viewed as riskier than not wearing a seatbelt;
- South Africans are more likely to own internet-enabled devices than their global counterparts; smartphones and laptops being most common;
- Though most devices are protected, South Africans falter when it comes to protecting home theatre devices, wearables, and Internet-connected video game systems;
- Devices considered easiest to hack are among the most frequently used, such as a smartphones and laptops.

**Too much hassle to be careful**

The research has shown that although there is considerable interest and fear in cybercrime, South Africans consider security measures to be a hassle.

- More than 1 in 3 South Africans admit to password sharing with email account passwords most shared;
- Nearly 7 in 10 change their passwords after they've been compromised… meaning nearly a third don't (32 percent);
- Over half check their accounts after a breach has been announced by the media;
- While nearly half of South African password users always use one that is secure, 1 in 5 still only does so when required;
- Dealing with the consequences of a stolen identity is considered more stressful than many everyday inconveniences.

## Hacking Risk At Rio Olympics, Warn US Officials

Source: http://i-hls.com/2016/07/hacking-risk-at-rio-olympics-warn-us-officials/

July 07 – Before they've even started, the Rio Olympics are already plagued with numerous issues jeopardising the security of visitors, players, and residents alike. From the Zika virus, through political instability, and known terror threats against the Games, to the newest warning issued to travellers: hacking. US intelligence officials are waning American travellers planning to attend the Games and other foreign destination that they could become the targets of hackers and cyber criminals planning to steal confidential information, whether personal or business related.

America's top counter-intelligence official, Bill Evanina, is advising to use "clean" devices while abroad, USA Today reports. The Games, apart from drawing the world's top athletes, will also present a "great playground" for intelligence services and criminals, Evanina says, due to the "sheer number of devices" present.

"When you travel abroad, assume that your personal information will be breached,'' Evanina said.
The US government has now launched a multimedia campaign to warn travellers against the increased risk. The **"Know the Risk; Raise Your Shield"** program advises travellers of the danger and suggests practicing extreme caution.


**Among the precautions** Evanina suggests to take are: leaving unnecessary devices at home, backing up all data and storing copies at secure locations, changing passwords at regular intervals during travel and upon return, avoiding prolonged sessions on local WiFi networks, and submitting company devices for examination on return.
Similar concerns were raised before the 2008 Olympics in China and the 2014 Winter Olympics in Russia, but due to the growing prevalence of smart devices the risk is far greater now.

## Global Terrorism Database Leaked! Reveals 2.2 Million Suspected Terrorists

Source: http://thehackernews.com/2016/06/world-check-terrorism-database.html


June 29 – Researcher Chris Vickery claimed on Reddit that he had managed to obtain a copy of 2014 version of the **World-Check** confidential database, which is being used by banks, governments, and intelligence agencies worldwide to scope out risks including suspected terrorists.
The leaked database contains more than **2.2 Million records** of people with suspected terrorist, organized crime, money laundering, bribery, corruption links, and "other unsavory activities."
According to Thomson Reuters, who run World-Check, its service is used by 4,500 institutions, including 49 of the world's 50 largest banks, more than 300 government and intelligence agencies, and law firms.
Although the access to the World-Check database is supposed to be strongly restricted under European privacy laws, Reuters says an unnamed third-party has exposed an outdated version of the database online.
Vickery does not reveal exactly how he came across the data, but he says: "No hacking was involved in my acquisition of this data. I would call it more of a leak than anything, although not directly from Thomson Reuters. The exact details behind that can be shared at a later time."

Meanwhile, he told BBC that the database was not using any protection like username or password to see the records. However, he clarifies that "this unprotected database was not directly hosted by Thomson Reuters itself."
Vickery also told media outlets that even after disclosing its location to Thomson Reuters, the database is still available online.
"As far as I know, the original location of the leak is still exposed to the public internet," said Vickery. "Thomson Reuters is working feverishly to get it secured."
Along with the number of categories, the World-Check database also contains individuals' dates and places of birth in an effort to help banks and government entities check they are looking into the right people.

**World-Check: A Controversial Global Terror Database**

The World-Check database has repeatedly been accused of falsely designating individuals and organizations as terrorists on the list without their knowledge.
The BBC's Radio 4 first revealed the inaccurate terror designations after it gained 30 minutes of access to the World-Check database in August 2015 from one of the disgruntled customers.
An investigation conducted by Vice News in February 2016 also revealed that there were several individuals on the database list with a terrorist designation, including "an American Muslim civil rights leader praised by George Washington Bush, an economist honored by the British Queen, and a prominent anti-extremism campaigner."
However, the Reuters rejects these accusations. "The worst possible situation that could arise is that someone who may be innocent, but accused of criminal activity in the database, could be permanently branded on a global scale if this database were to be spread publicly," said Vickery.
Vickery has previously tracked down a number of exposed datasets on the Internet. He's the one who reported a huge cache of around 191 Million US voter records and details of around 13 Million MacKeeper users.
In April, Vickey also reported information on 93 million Mexican voters. The records were exposed due to a configuration error in a MongoDB database.

# ISIS uses Whatsapp, Telegram to sell girls and women as sex slaves

Source: http://www.homelandsecuritynewswire.com/dr20160711-isis-uses-whatsapp-telegram-to-sell-girls-and-women-as-sex-slaves


July 11 – ISIS has been using instant messenger apps Whatsapp and Telegram to advertise Yazidi women and girls as young as 12 for sale as sex slaves.
These apps are also being used to share photos databases of women held by ISIS as sex slaves. ISIS uses the apps to distribute these of photographs to ISIS militants manning the group's checkpoints so that these women can be identified if they try to escape ISIS-controlled territory.
Yahoo News notes that Telegram and Facebook-owned Whatsapp both use end-to-end encryption,

preventing the two companies from accessing users' communications.
People who have seen the ISIS advertisement say that in many of the photos the women and girls are dressed nicely and are often heavily made-up.
Analysts estimate that about 3,000 women and girls are at present being held captive by ISIS. Many of the captive women and girls are Yezidis, taken prisoner in 2014 when ISIS fighters attacked their villages in northern Iraq.
UN investigators have concluded that the wholesale killing of the Yezidis in both Iraq and Syria, constitutes an act of genocide.
Whatsapp said they do what they can to combat extremist messaging, and that the company disables accounts once they become aware of the activity.
Matt Steinfeld, a spokesperson for Whatsapp, told the AP: "We have zero tolerance for this type of behavior and disable accounts when provided with evidence of activity that violates our terms.
"We encourage people to use our reporting tools if they encounter this type of behavior."

# Does Hacktivism Really Equal Terrorism?

Source: https://www.hackread.com/does-hacktivism-really-equal-terrorism/

*An act involving hacking of a computer or a website to deliver a religious, political or social message is known as hacktivism but is it an act of terrorism as well?*

July 10 – In early 2015, the United States Federal Bureau of Investigation (FBI) **made a bold move**. It placed self-proclaimed hacktivist, Jeremy Hammond, already in jail, on its terrorism watchlist. While no one can argue that most cybercrime is just that: crime; is it really a logical jump from hacktivism to terrorism? The financial motivations of most cyber crime and the political motivations of hacktivists are where things get murky.

If the FBI can prove that hacktivism really is terrorism, the implications for both hacktivists and the general public are, frankly, frightening.

**Defining Terrorism**

Most of the public knows the basic differences between hacktivism and hacking for profit or criminal gain. Yet do we really know how terrorism is defined by our governments? **The FBI defines terrorism's forms thus: "International terrorism" means activities with the following three characteristics:**

- Involve violent acts or acts dangerous to human life that violate federal or state law;
- Appear to be intended (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and
- Occur primarily outside the territorial jurisdiction of the U.S., or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to intimidate or coerce, or the locale in which their perpetrators operate or seek asylum.*
- "Domestic terrorism" means activities with the following three characteristics:
- Involve acts dangerous to human life that violate federal or state law;
- Appear intended (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination. or kidnapping; and
- Occur primarily within the territorial jurisdiction of the U.S.
- 18 U.S.C. § 2332b defines the term "federal crime of terrorism" as an offense that:

- Is calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct; and
- Is a violation of one of several listed statutes, including § 930(c) (relating to killing or attempted killing during an attack on a federal facility with a dangerous weapon); and § 1114 (relating to killing or attempted killing of officers and employees of the U.S.).

**A close reading of this code reveals that the definition of hacktivism, hacking for political motivations, typically with Denial of Service attacks, is likely not terrorism. Why?**

According to the FBI, in order for an act to be considered terrorism, it must meet all of the requirements of each definition. An act must be illegal and violent or endanger human life, be coercive or intimidating, and occur in whichever jurisdiction fits. The code does not say that terrorism must meet one or all, but "means activities with these three characteristics." Most acts of hacktivism only tick one or two of these boxes, if at all.

**New Definitions Needed?**

It must be noted that the FBI's terrorism definition is at least five years old, published in 2011. While hacktivism has been a part of the world since the 80s, it looks much different in 2016 than it did even five years ago.

One could also argue that most, if not all, acts of hacktivism constitute the commission of a crime. At the same time, the Denial of Service attack on a federal repository that makes no money and offers no sensitive information is not equal to the DoS on state emergency response site. The latter does indeed endanger human life, and if it is defined as illegal in that state, it constitutes a crime.

Yet does either of these constitute an act of terrorism? Taking a broad reading of the FBI's code, the latter might certainly be terrorism. However, DoS attacks rarely do any true damage. That is their nature. They disrupt services, they don't destroy anything tangible. Even the former could be seen as an act of terrorism, though no one is harmed by it. Legally, however, designating hacktivists as terrorists should only occur when all three of those "boxes" are ticked

Should our definition of terrorism change to meet the changes in hacktivism? When large-scale government services are disrupted and endanger lives en masse, hacktivism could indeed be classified as terrorism. Without changing any definitions, many hacktivists will either be jailed or coerced themselves out of the good that can come from their acts. Many of the most current acts of hacktivism are aimed at disrupting the activities of terrorist organizations, ones that meet all the FBI's requirements of the definition.

**It cannot be denied that terrorism is turning digital.** What is at issue is prosecuting and alienating a few people based on a narrow definition. Either the definition needs to become broader, or hacktivism needs to be excepted from it. There is no easy answer.

# Cybersecurity risks in 3D printing

Source: http://www.homelandsecuritynewswire.com/dr20160715-cybersecurity-risks-in-3d-printing

July 15 – Additive manufacturing (AM), commonly called 3D printing, is a $4 billion business set to quadruple by 2020. One day, manufacturers may print everything from cars to medicines, disrupting centuries-old production practices. The Federal Aviation Administration (FAA) recently certified the first 3D-printed part for GE commercial jet engines, and companies like Ford Motor Company are using AM to build products and prototypes.

But the new technology poses some of the same dangers unearthed in the electronics industry, where trusted, partially trusted, and untrusted parties are part of a global supply chain.

NYU says that that finding, along with initial recommendations for remedies, was reported by a team of cybersecurity and materials engineers at the NYU Tandon School of Engineering in *JOM, The Journal of the Minerals, Metals & Materials Society*.

In the paper, the researchers examined two aspects of 3D printing that have cybersecurity implications: printing orientation and insertion of fine defects. "These are possible foci

for attacks that could have a devastating impact on users of the end product, and economic impact in the form of recalls and lawsuits," said Nikhil Gupta, noted materials researcher and an associate professor of mechanical engineering at the New York University Tandon School of Engineering.

Additive manufacturing builds a product from a computer assisted design (CAD) file sent by the designer. The manufacturing software deconstructs the design into slices and orients the printer head. The printer then applies material in ultra-thin layers.

The researchers reported that the orientation of the product during printing could make as much as a 25 percent difference in its strength.

However, since CAD files do not give instructions for printer head orientation, malefactors could deliberately alter the process without detection. Gupta explained that economic concerns also influence how a supplier prints a product. "Minus a clear directive from the design team, the best orientation for the printer is one that minimizes the use of material and maximizes the number of parts you can print in one operation," he said.

Said Ramesh Karri, professor of electrical and computer engineering and a cybersecurity researcher known for improving the trustworthiness of the microchip supply chain: "With the growth of cloud-based and decentralized production environments, it is critical that all entities within the additive manufacturing supply chain be aware of the unique challenges presented to avoid significant risk to the reliability of the product."

He pointed out that an attacker could hack into a printer that is connected to Internet to introduce internal defects as the component is being printed. "New cybersecurity methods and tools are required to protect critical parts from such compromise," he said.

When the researchers introduced sub-millimeter defects between printed layers, they found that the defects were undetectable by common industrial monitoring techniques, such as ultrasonic imaging, which do not require destruction of the sample. Over time, materials can weaken with exposure to fatigue conditions, heat, light, and humidity and become more susceptible to these small defects.

"With 3D printed components, such as metallic molds made for injection molding used in high temperature and pressure conditions, such defects may eventually cause failure," Gupta said.

*— Read more in Steven Eric Zeltmann et al., "Manufacturing and Security Challenges in 3D Printing," JOM 68, no. 7 (July 2016): 1872-81.*

# ISIS computers contain up to 80% porn: former US intelligence chief

Source: https://www.lifesitenews.com/news/heavy-isis-porn-use-linked-to-terrorism-rapes

July 18 – **As much as four-fifths of Islamic terrorists' computers are filled with porn,**


and the former chief of the U.S. Defense Intelligence Agency says their porn use contributes to the atrocities they commit against women and children.

Lt. Gen. Michael Flynn said computers seized from ISIS jihadists contained as much as 80 percent pornography and he speculated to a German newspaper that porn might be the driving force behind the plethora of rapes of women and children by Islamic militants.

"These sick, psychopathic enemies were not only unimaginably hideous but also treacherous and torn. ... Women and children, girls and boys, raped and exploited," Lt. Gen. Flynn said. He then **tied the barbarism of Islamic terrorists to their obsession with pornography.** "Beheadings were stored on a laptop next to pornography. At one point, we actually had determined that the

material on the laptops was up to 80 percent pornography."

Even liberals, after decades of insisting that viewing pornography is a benign activity, are beginning to admit a connection between porn and violence. Former London Mayor Boris Johnson was criticized in early 2015 for observing that Islamic suicide bombers were "obsessed" with pornography. "If you look at all the psychological profiling about the bombers, they typically will look at porn. They are literally wankers. Severe onanists."

Several Islamicists went on porn binges before their attacks. In at least one case, the connection between a terrorist and his favorite porn star was so dependable, the government used the porn star as an agent to monitor and locate the terrorist's cell.

Osama Bin Laden's compound in Abbottabad contained a "fairly extensive porn stash," according to Reuters in 2011.

For years, numerous studies have shown that exposure to sexual violence breeds permissive attitudes toward rape. A 2009 study found a "significant positive association between pornography use and attitudes supporting violence against women."

Research into violent sexual criminals has found the common link is porn. A 1989 study of 2,380 victims and abusers determined that in 68 percent of abuse cases, the attacker viewed pornography immediately before abusing his victim. Serial killer Ted Bundy told James Dobson that his problems began with exposure to pornography at a young age. He also said every prison inmate he knew was affected by porn.

Sixteen years ago, a study was published analyzing women's experiences of sexual violence with their abusers' use of pornography. Data were collected at a rape crisis center from 100 survivors. The study found nearly 30 percent of victims of sexual violence reported that their abuser consumed pornography, and in an alarming number of cases, pornography was imitated in the abuse.

The Michigan State Police found that pornography was used or imitated in 41 percent of the sex crimes they have investigated. The Free Congress Research and Education Foundation found that half of all rapists studied used pornography to stimulate their passions before prowling for their victim.

In 1998, the FBI revealed that 83 percent of serial sexual sadists, 61 percent of serial killers, 90 percent of pedophiles, and 33 percent of serial rapists collected pornography.

In today's world of readily accessible online pornography, the violence has hit home — even in rural America. This year, a southeastern Ohio study entitled, "Adult Pornography and Violence Against Women in the Heartland," concluded that "pornography is a major component of the problem of rural woman abuse."

Religious groups have long recognized the link between pornography and violence. In 1989, the Pontifical Council for Social Communications concluded, "Pornography can act as an inciting or reinforcing agent, a kind of accomplice, in the behavior of dangerous sex offenders — child molesters, rapists and killers."

The Vatican council explained, "A fundamental message of pornography and violence is disdain, the consideration of others as objects rather than as persons. Thus, pornography and violence can eat away at tenderness and compassion and can foster insensitivity and even brutality."

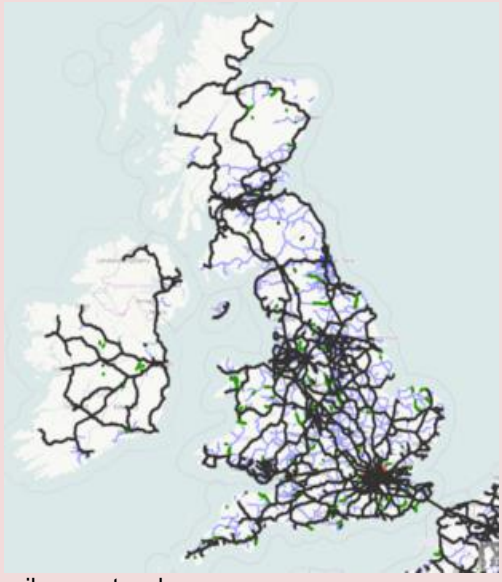
# UK Railway Network Suffered Four Cyber-Attacks in the Past Year

Source: http://www.cybersecurity-review.com/uk-railway-network-suffered-four-cyber-attacks-in-the-past-year

July 18 – Unknown hackers breached the UK railway network four times in the last twelve months, according to Darktrace, a British cyber-security firm, quoted by The Telegraph and Sky News.

According to Darktrace, the attacks were only basic reconnaissance operations, intrusions to detect a network's internal structure and to gather information for future attacks. The company also doesn't exclude that these intrusions were only accidental.

Previous to the UK, attacks on a country's railway network were detected in Ukraine this past winter, as part of the infamous BlacEnergy attacks that also targeted the country's energy grid and airports.



Railway networks are part of a country's transportation system and are considered "critical infrastructure."

**In the case of a real cyber-war, railway networks, along with smart roads and airports, are most certainly going to face cyber-attacks,** along with the other critical infrastructure sectors such as energy, water supply, oil & gas, communications, the chemical sector, food & agriculture, healthcare, and emergency services.

Attacks on a railway network's infrastructure are technically possible.

This past December, at the 32nd Chaos Communication Congress (32C3) in Germany, Russian security researchers from SCADA StrangeLove presented a series of attacks that could cripple a railway network.

# Bulgarian Cabinet adopts cyber security policy

Source: http://www.balkaneu.com/bulgarian-cabinet-adopts-cyber-security-policy/

July 13 – Bulgaria's Cabinet adopted on July 13 a national cyber security policy, entitled "Cyber Resilient Bulgaria 2020", a step taken against a background of repeated cyber warfare attacks on state and government websites.


**Among the most severe attacks on Bulgarian websites was a series in late 2015, as the country held a national referendum on electronic voting.**

Some, including President Rossen Plevneliev, saw the attacks as an attempt to discredit the concept of electronic voting, even though the cyber attacks were of a kind irrelevant to voting online.

Emanating from abroad, the cyber attacks included denial-of-service attacks that took offline the sites of a number of state and government institutions, including bodies in charge of law enforcement, intelligence and elections.

The document envisages the appointment of a national co-ordinator to oversee the implementation of an action plan on cyber security.

The vision for the development of cyber security in Bulgaria is separated into three stages, from addressing the basic vulnerabilities in critical state and society communication and information systems, to achieving a mature state of cyber sustainability – including against attacks from unknown sources – to achieving a leading and innovative role on the issue.

A part-time advisory body will provide guidance on drafting and stating Bulgaria's position in international institutions and organisations in regard to cyber security.

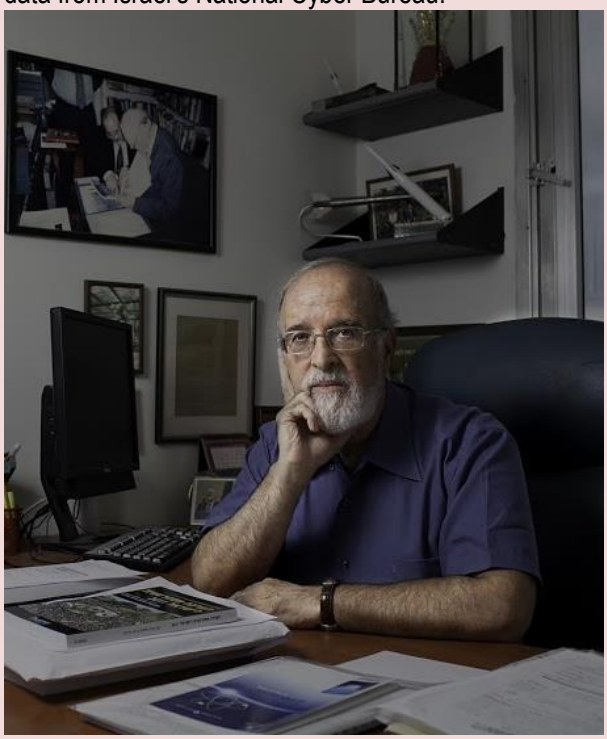
**The council on cyber resistance will monitor trends and developments in cyber threats, risks, methods of counteracting and make proposals to the national security council, if required.**

The new council will prepare regular reports to the national security council and the Cabinet on the state of security in cyberspace, on the development of risks and a summary assessment of the level of maturity and cyber stability achieved.

# Meet The General Who Positioned Israel To Win In $175 Billion Cybersecurity Market

Source: http://www.forbes.com/sites/elizabethmacbride/2016/07/18/five-lessons-on-cybersecurity-from-an-israeli-general/#286961f61b58

July 18 – **When it comes to cybersecurity, Israel sits at the center of the world. Israeli companies exported $6.5 billion a year worth of cyberproducts, about 10% of the world market**, based on data from Israel's National Cyber Bureau.



That's up from only a 1-2% share of the much smaller market five years ago. The cybersecurity business in the United States is obviously bigger, but per capita, Israeli companies' presence in this market — one of the fastest-growing opportunities of the 21st century — is huge.

In short, the Startup Nation has a sub-specialty. How did it get one? It turns out to be a top-down initiative, straight from Prime Minister Benjamin Netanyahu. Last week, I interviewed **Isaac ben Israel**, who's called the father of Israel's cybersecurity business. He recently wrote an academic-style book on the topic called Cybersecurity in Israel.

It was a fascinating conversation in ben Israel's small office, decorated with posters of Albert Einstein (ben Israel has a degree in physics). I walked away thinking about how entrepreneurs and their supporters ought to look at a world in which technology is the biggest friend and greatest vulnerability.

By happenstance, almost, ben Israel, turned out to be an entrepreneurial ecosystem builder. He is a retired Israeli Defense Force major general and a long-time figure in the company's military research and development world. He is now, among other titles, director of the Blavatnik Interdisciplinary Cyber Research Center at Tel Aviv University. In 2002, he said, Ehud Barak called Isaacson to ask him to develop cyber protection for the country's infrastructure. In 2010, Benjamin Netanyahu asked him to launch the National Cyber Initiative. (This article in the New York Times has a good discussion of how much cyber warfare is part of nations' military strategies now — but my interview with ben Israel focused on the industry that is growing up around commercial and military cyber risks.)

## China's First Emergency UAV Rescue Team

Source: http://i-hls.com/2016/06/chinas-first-emergency-uav-rescue-team/

June 22 – Earlier this month, **China has launched the first-in-the-country emergency rescue team that will use unmanned aerial vehicles (UAVs),** Beijing Daily reports.

Six UAVs are now primed and ready for rescue missions at the training base of the Ministry of Civil Affairs located in Changping district. **The drones in the service come in two types: fixed- and rotary-wing,** to cover different mission profile requirements.

**The largest of the aircraft has a 2.96 metre wingspan. It is powered by gasoline to reach speeds of 150 km per hour for a maximum flight radius of 200 kilometres with a payload of 5 kg. It has a flight time of three hours at a maximum altitude of four kilometres.**

The aircraft can airdrop food, water, and other essential supplies to people in need of assistance. "But it requires the trapped to send their location through a mobile phone," said a worker of the team. "After we receive the information, we will be able to input the information into the control platform, which then transmits it to the aircraft, allowing it possible to drop the relief material accurately."

**Other aircraft in the arsenal are battery powered with much smaller ranges: between 10 and 50 kilometres.**

Although only now officially established, the UAV team has already took on an active role in rescue missions during the Lushan earthquake and the Tianjin blasts.

UAVs will play an active and increasingly important role in future rescue tasks, said Han Guangjian, Deputy Director of the Emergency Rescue Promotion Center with China's Ministry of Civil Affairs. He predicted that soon similar rescue teams will be set up in other population centres around China.

## Drones could be cheaper alternative to delivering vaccines in developing world

Source: http://www.medicalnewstoday.com/releases/311163.php

June 23 – **Using unmanned drones to deliver vaccines in low- and middle-income countries may save money and improve vaccination rates,** new research led by the Johns Hopkins Bloomberg School of Public Health and the Pittsburgh Supercomputing Center suggests.

The cost savings would come from drones being able to deliver vaccines more quickly and cheaply than land-based methods limited by road conditions and the need for costly fuel and maintenance, the researchers note in their study, published in the journal *Vaccine*.

"Many low- and middle-income countries are struggling to get lifesaving vaccines to people to keep them from getting sick or dying from preventable diseases," says senior author Bruce Y. Lee, MD, MBA, an associate professor at the Bloomberg School and director of operations research at its International Vaccine Access Center. "You

make all these vaccines but they're of no value if we don't get them to the people who need them. So there is an urgent need to find new, cost-effective ways to do this."

In low- and middle-income countries, there are many challenges faced by immunization programs, which provide childhood vaccines such as hepatitis B, tetanus, measles and rotavirus, and will be utilized in the future as vaccines for dengue, malaria and Zika are developed and brought to market. After entering a country, vaccine vials typically travel by road through two to four storage locations before arriving at clinics where health workers

administer doses to patients. Most vaccines need to remain refrigerated until they are used or they will spoil. Non-vaccine costs of routine immunizations are expected to rise by 80 percent between 2010 and 2020, with more than one-third of costs attributable to supply chain logistics. Supply chain inefficiencies can mean that many vaccines don't even reach the people who need them.

Meanwhile, **unmanned drones have proliferated in recent years because they can traverse difficult terrain, reduce labor costs and replace fleets of vehicles.** They have been used for surveillance and in humanitarian aid delivery and are now being developed to transport medical samples and supplies, though previously little has been known whether this is a cost-effective use of the new technology.

For their study, Lee and his colleagues created a HERMES computer model to simulate a traditional land-based transportation system - a combination of trucks, motorbikes and public transit - and compared it with an unmanned drone system for delivering vaccines as part of an immunization program. Seattle-based non-governmental organization Village Reach helped provide data for the model. They varied characteristics such as geography, population, road conditions and vaccine schedule in order to assess which conditions would most contribute to drones offering the biggest cost savings.

They found that **using drones to get vaccines to the last stop on their journey - vaccination locations - could slightly improve vaccine availability - potentially immunizing 96 percent of the target population as compared to 94 percent using land-based transport - while producing significant savings: eight cents for every dose administered (roughly a 20 percent savings). To save money, the drones would need to carry at least .4 liters of vaccines and the researchers say that the drones could carry at least 1.5 liters. If there were no flight delays for scheduled drone deliveries and the drones carried 1.5 liters, the researchers noted, each flight could cost up to $8.93 and annual infrastructure and overhead costs could cost up to $60,000 and still produce savings.** As a comparison, the researchers studied the traditional land-based immunization system in Mozambique, which has achieved 94 percent vaccine coverage, but they note that many countries currently cover fewer than 60 percent of the population using land-based approaches.

"Currently, in many locations, vehicles that transport vaccines aren't always available or reliable," Lee says. "Assuming that drones are reliable, are capable of making the necessary trips and have properly trained operators, they could be a less expensive means of transporting vaccines, especially in remote areas. They could be particularly valuable when there is more demand for certain vaccines than anticipated and immunization

locations must place urgent orders."

While the computer models are good at theoretically analyzing the cost effectiveness of drone technology, the researchers say that real-world testing must be done to make certain that drones are a viable way to transport vaccines. And many obstacles may exist. Regulatory issues could limit the ability of drones to deliver goods and commodities. Maintaining and operating the equipment would require specialized tools and skills that may be difficult to access in these developing countries. Since no person would accompany a shipment, greater coordination would be needed between those shipping and those receiving the vaccines. Appropriate packing to maintain vaccine quality would need to be developed.

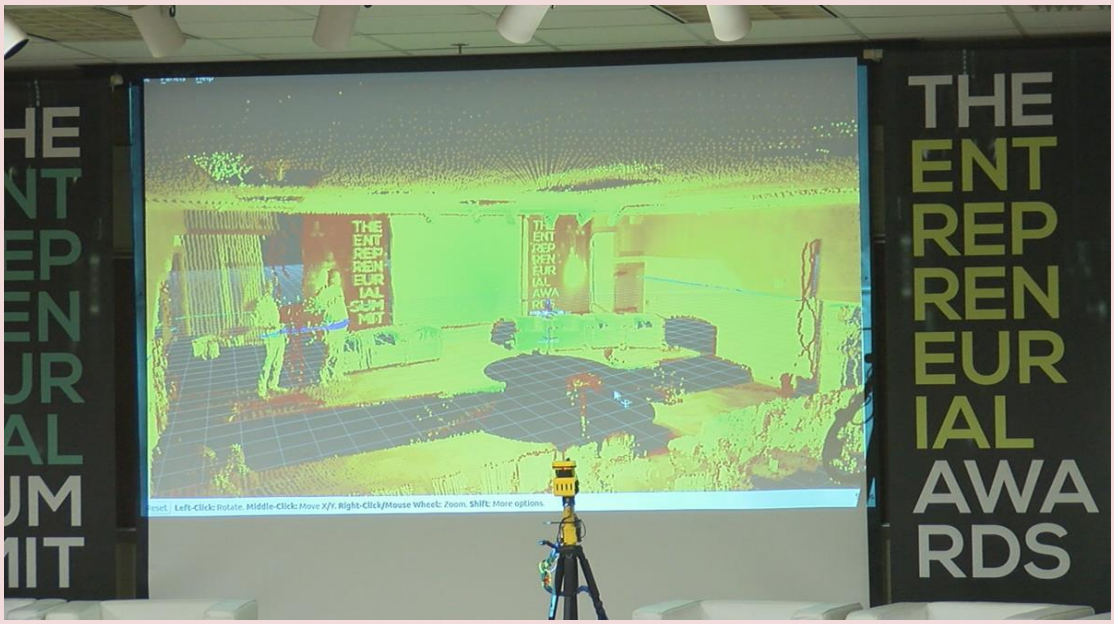
Drones are currently being tested for medical supply deliveries in rural Virginia, Bhutan and Papua New Guinea. UNICEF is testing the feasibility of using them to transport lab samples in Malawi. And **in Tanzania, there are efforts afoot to transport blood and essential medications.**

The research was supported by the Bill and Melinda Gates Foundation, the Agency for Healthcare Research and Quality (RO1HS023317) and the Eunice Kennedy Shriver National Institute of Child Health and Human Development (UO1HD086861 and U54HD070725).

***Article:*** *The economic and operational value of using drones to transport vaccines, Leila A. Haidari, MPH; Shawn T. Brown, PhD; Marie Ferguson, MSPH; Emily Bancroft, MPH; Marie Spiker, MSPH; Allen Wilcox, JD; Ramya Ambikapathi, MHS; Vidya Sampath, MSPH; Diana L. Connor, MPH and Bruce Y. Lee, MD, MBA,* Vaccine, *doi:10.1016/j.vaccine.2016.06.022, published online 20 June 2016.*

# Real Time Mapping For First Responders

Source: http://i-hls.com/2016/07/real-time-mapping-for-first-responders/




NuSpatial created a 3D map of the room it presented in during the TechVet forum.

July 01 – First responders face many challenges in their line of work, and the quicker they need to get the job done the higher the risks they face. When firefighters and rescuers approach a burning building, among the first questions they ask is what is the layout of the building, where are the people in need of assistance located, what are the most pressing dangers, and what are the quickest and safest routes of egress.

Until now, answering these questions required guesswork, trial and error, and sheer luck. But future forces of first responders will have tools that will help them perform their duties quicker, safer, and more effectively.

One of the companies working in this field is NuSpatial. This Alabama-based startup has come up with a solution that can astoundingly quickly map the rooms inside a building. The company says their device can collect measurement data as quickly as you can walk through an interior space.
This speed doesn't harm measurement accuracy, either.
"We can get a lot of really detailed information. We can distinguish faces. We can see letters in the wall," NuSpatial's Tim Coddington said in a recent interview.
The company's technology was initially designed with other purposes in mind. They've intended it to map buildings with no extant plans, update building information models (BIM), and other commercial and industrial applications. But the technology could certainly serve in the line of duty, too.
At this stage the device would be too big and cumbersome to use in dangerous settings, but if NuSpatial successfully miniaturises and hardens it, it could be a real boon for future first responder forces.

# Threats Evolving Faster Than Preparedness

**By Robert C. Hutchinson**
Source:http://www.domesticpreparedness.com/Medical_Response/Public_Health/Threats_Evolving_Faster_Than_Preparedness/

*With the current amount of discussion and media coverage regarding the spreading Zika virus and the mounting concerns over antibiotic drug resistance, public health remains a critical homeland security and emergency preparedness priority. Unfortunately, it is often a fluctuating priority that does not receive consistent attention, action, and funding to prepare for future known and unknown public health threats.*

July 06 – The May 2016 birth of a child in the continental United States reportedly with microcephaly from the Zika virus has once again pushed the subject of preparedness and funding for public health into the op-ed pages and 24-hour news cycle. As Ebola receded in Africa and faded from discourse in the United States, Zika erupted due to its reported grave effects on pregnant women and their developing fetuses. As a result, the public health emergency fund in the United States and its level of funding were once again a topic of intense discussion and political squabbling.
Beyond these current public health challenges and funding questions, another question arises about whether cross-sector planning and preparedness priorities are being properly addressed for the whole of community requirements to prepare for, respond to, and recover from a severe public health threat. Previous research, observations, and experience may not provide the highest level of confidence for a unified response to rapidly emerging and evolving pathogenic threats.

**Changing Focus From Ebola to Zika**
The international priorities and focus continue to transition from the diminishing Ebola virus to the expanding Zika virus and other re-emerging public health concerns such as yellow fever. Director General of the World Health Organization Dr. Margaret Chan identified numerous international public health and policy issues for the world during her address to the 69th World Health Assembly in May 2016, which included the following statements:

- "Drug-resistant pathogens, including the growing number of 'superbugs,' travel well internationally in people, animals, and food."
- "The Ebola outbreak in three small countries paralyzed the world with fear and travel constraints."
- "For Ebola, it was the absence of even the most basic infrastructures and capacities for surveillance, diagnosis, infection control, and clinical care, unaided by any vaccines or specific treatments."
- "The rapidly evolving outbreak of Zika warns us that an old disease that slumbered for six decades in Africa and Asia can suddenly wake up on a new continent to cause a global health emergency."
- "For Zika, we are again taken by surprise, with no vaccines and no reliable and widely available diagnostic tests."
- "Few health threats are local anymore. And few health threats can be managed by the health sector acting alone."

- "Medicines for treating chronic conditions are more profitable than a short course of antibiotics."
- "For infectious diseases, you cannot trust the past when planning for the future."

The Zika virus is not new, but expanding to new locations beyond Africa and Asia largely due to international trade and travel. **The virus was originally isolated and identified in a sentinel rhesus monkey in the Zika Forest near Entebbe, Uganda, in 1947. Although unknown how and when Zika arrived in Brazil, it has been theorized that the virus may have been introduced during a sporting event in August 2014 with numerous competitors from four Pacific nations where the virus was present.** This theory compounds concerns regarding the upcoming Olympic Games and several recently completed international events in Brazil.

Unfortunately, confusion may exist regarding the definite source of an illness and the most appropriate medical treatments. As with Zika and other viruses, the effectiveness and usefulness of broad antibiotic use for an unconfirmed illness, which may be viral, can have significant consequences for the whole society – especially with the explosion of antibiotic-resistant superbugs.

**Expanding Resistance to Antibiotics**

In May 2016, The *Review on Antimicrobial Resistance* issued, "Tackling Drug-Resistant Infections Globally: Final Report and Recommendations." The report, sponsored by the United Kingdom and Wellcome Trust, estimated that **10 million lives per year would be at risk by 2050 due to the rise of drug-resistant infections.** These antimicrobial drugs include antibiotics, antivirals, antifungals, and antimalarials. According to the study, less than five percent of venture capital investments in pharmaceutical research and development between 2003 and 2013 were for antimicrobial development. The report identified 10 interventions or fronts to reduce the demand for antimicrobials, including better incentives to promote investments for new drugs and improvements of existing ones.

The recent finding that an E. coli bacterium superbug, with the mcr-1 gene, was resistant to the last-resort antibiotic colistin only added to the concerns about resistance and the nation's future capabilities. According to the Centers for Disease Control and Prevention, the mcr-1 gene exists on a plasmid, a small piece of DNA that is capable of moving from one bacterium to another, spreading antibiotic resistance among bacterial species. Colistin was reportedly seldom used in humans due to its toxicity, but it has reportedly been utilized in the agriculture environment for decades.

Due to the enormous costs of developing new medicines and treatments, the amount of new antibiotics in the research pipeline appears rather small compared to other drugs. There are reportedly stronger financial incentives to invest in drugs for chronic diseases to recoup research investments over a long period of time. A May 2016 analysis by *The Economist* magazine revealed the limited cumulative profits from antibiotic research from pre-clinical research to off-patent sales.

In May 2016, the World Health Organization issued a research and development blueprint for actions to prevent epidemics. The global strategy and preparedness plan was created to reduce the amount of time required to deliver tests, vaccines, and medicines, and to strengthen emergency response during epidemics and pandemics.

**Epidemic & Pandemic Preparedness**

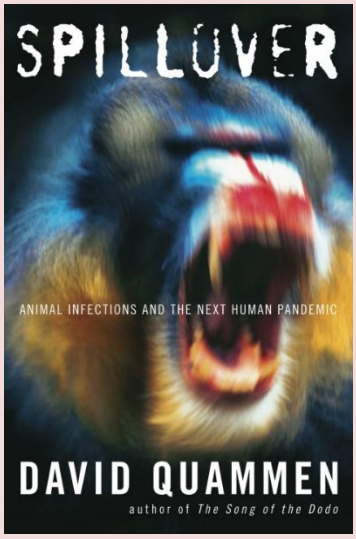
It has been estimated that as many as 100 million people died during the Spanish Flu pandemic outbreak in 1918. It is projected that a similar pandemic outbreak today could result in the death of 360 million people around the world despite the availability of vaccines and antimicrobials. In addition to the world population growth, the pace of urbanization, globalization, and travel only expands the genuine concern for the rapid spread of epidemics and pandemics.

In the November 2013 DomPrep Bio-Training edition, the subject of preparing for Black Swan pandemic and biological threats asked important questions regarding preparedness for a vast array of public health threats. Sadly, many of the same critical questions remain unanswered today, such as, "Have the many lessons from SARS, H5N1, H1N1, MERS, and Ebola truly been learned and implemented?"

Unfortunately, too many still view a pandemic-prone pathogen as the primary responsibility of the public health and medical services organizations. Law enforcement, military, and numerous other public and private sector organizations have critical

responsibilities to execute during a serious public health event – usually in close coordination and collaboration with the other agencies involved for support and response.

As is true of many significant incidents and disasters, there is usually very little if any time to plan and prepare when a new threat suddenly appears, rapidly expands, and eventually overwhelms medical services and public health officials. In addition, quarantine, isolation, and medical countermeasure dispensing procedures may be required to contain a new disease outbreak or biological agent attack and, in some situations, any subsequent public unrest. The experience with Ebola in 2014 in the United States and other recent outbreaks does not indicate a significant level of readiness and coordination. Many of the most controversial and difficult issues have been ignored since the Ebola outbreak.




**Need to Prepare & Respond**

**Ebola and Zika were not new public health threats, but viruses that were isolated to rather limited areas due to emergence, transmission, and travel limitations.** The geographic isolation and infrequent outbreaks may have led to international complacency. Globalization has provided many benefits for the world, but unfortunately there are also grim consequences such as the rapid spreading of novel and re-emerging pathogens.

The prospect of a very serious novel virus with sustained human-to-human transmission could make previous Ebola or Zika outbreaks appear as rather manageable challenges in a globalized world. This concern was well established in journalist David Quammen's 2012 book, "Spillover: Animal Infections and the Next Human Pandemic." He characterized spillover as the moment when a pathogen passes from one species to another. This subject is very important since, in 2005, reportedly three-quarters of emergent pathogens were zoonotic spillovers. It is necessary to be cognizant of spillover public health threats that are both highly infectious and highly contagious, which could greatly threaten global health security.

As concluded by the Council on Foreign Relations in May 2016 regarding the future of global health security:

*"Creating a sustainable and coordinated environment for supporting innovation is key to advancing the goal of improved global health security. This is true whether it is investing in 'just-in-case' preparedness or a 'just-in-time' response to an outbreak. Implementing the hard-learned lessons from the last decade in global health can help achieve this goal while ensuring that the assets, resources, and commitments of partners across various sectors all fully contribute to enhancing global security."*

These public health challenges and threats linger and evolve with little notice and many cascading consequences. The question remains about whether planning and preparedness will get ahead of these current public health threats and the ones on the horizon, or the nation will continue to respond the best way that it can and only add Ebola and Zika to the list with SARS, H5N1, H1N1, MERS, and many others pathogens – with lessons not truly learned. It is necessary to evolve faster than these public health threats – a difficult but critical necessity for global health security.

***Robert C. Hutchinson*** *is a deputy special agent in charge (DSAC) with the U.S. Department of Homeland Security, U.S. Immigration and Customs Enforcement's Homeland Security Investigations in Miami, Florida. He was previously the deputy director and acting director for the agency's national emergency preparedness division. DSAC Hutchinson's writings, media interviews and presentations often address the important need for coordination and collaboration between the fields of public health, emergency management and law enforcement. He received his graduate*

*degrees at the University of Delaware in public administration and Naval Postgraduate School in homeland security studies.*

# 3 Ways to Create Chaos During a Drill

**By Robert Burton**

Source: https://www.linkedin.com/pulse/3-ways-create-chaos-during-drill-robert-burton

July 07 – How many fire drills have you conducted throughout your life? We did them throughout our childhood at school and most of us do them in our corporate or other daily routines. We should also do them at home!

When we conduct fire or other types of drills that require the physical movement of people, we often tend to do them on the same day at the same time and without many other changes to the drill. This is mainly for convenience. Have you ever thought about including a few obstructions or changes to make them more realistic? Changing them slightly will also make people think about how they would deal with different scenarios. Here's a few ideas:

**1. Block an Exit Door or Stairwell**

This can be simulated by having someone stand in position and inform participants that that exit is blocked or that they can hear the sound of gun fire coming from that exit.

**2. Accountability Challenges**

Accounting for personnel or children is critical during any emergency. Prior to the drill, you could ask one or two people to leave before the drill. Ask them not to answer their phones unless you call them. This will test the accountability procedures. If you do have fire wardens, you can also have one of them go missing which will create further challenges. Who are your fire wardens and do they have backups?

**3. Simulate Personnel with Disabilities**

If you have personnel with disabilities, monitor how (or if) they're assisted out of the location during the drill. If you don't have anyone with disabilities, simulate having a number of people with disabilities or other physical challenges. A pregnant lady, someone on crutches or in a wheel chair on a higher floor will also present unique challenges.

**Creating a little chaos from time to time will help personnel start to think outside of the box.**

These small changes don't have to happen every time you conduct a drill. They can take place occasionally which should keep everyone on their toes during every drill.

**Final note:** If you decide to create obstructions during a drill, ensure that you plan them in advance and that you think carefully through your objectives and how you want to achieve them.

***Robert Burton** is Managing Director at PreparedEx, LLC*

**EDITOR'S COMMENT:** A short but interesting article! In a recent live CBRN drill at a hospital abroad, I "secretly" instructed one of the ambulance ambulatory casualties transferred to ED's "warm zone" to collapse the moment he stepped out fo the ambulance. Time was frozen for a second! Is he OK? Did he really fainted? All triage personnel "jumped" over him to help (leaving their other "victims" alone). It is always very didactic to add an unexpected touch to drills (both tabletop and live). Because this is what is happening in real time!

# Doctors Recount Dallas Horror: Didn't Know 'If This was Another Orlando'

Source: http://www.emergencymgmt.com/health/Doctors-recount-Dallas-horror-Didnt-know-If-this-was-another-Orlando.html

July 10 – Dr. Ron Jensen was at home watching television when the newsflash cut in, reporting that there had been a massive shooting in downtown Dallas. It happened at the tail end of what was supposed to be a peaceful rally.

Dr. Alan Jones was already on duty at the Baylor University Medical Center, but visions of 9/11 – or at least the trauma he witnessed – flashed before him as he prepared for a wave of wounded police officers.

Nurse Sherry Sutton wanted to know where her husband was. He is a veteran of the Dallas Police Department.

"We didn't know if this was an isolated event or if this was another Orlando," said Jensen, the head of emergency medicine at Baylor, a level-one trauma center where many of the wounded were taken. " … We had no idea if we were getting five more or 40."

Less than a month after 49 people were killed and scores more were injured in an Orlando nightclub – in what is regarded as one of the worst mass shootings in modern American history – hospitals across Dallas found themselves preparing.

Five people, all police officers, died, in what doctors at Baylor are calling "controlled chaos."

"It was horrific," Sutton said. "And we didn't know what was going to happen next. Just like in Orlando, we had to make sure we had the tools and knowledge to do our jobs. So it becomes second nature. This team shined."

Jensen said by the time he arrived at the hospital, the staff was already there.

None of them had been called.

**"We have drills, so everybody just showed up and did what they were supposed to do,"** said Jones, the director of orthopedic trauma surgery at the hospital. "When you realize that it is not a drill, that is when instincts kick in."

**Jensen said the hospital constantly studies disasters, from Orlando to Hurricane Katrina to Midwestern tornadoes, to prepare.**

"We studied Orlando, but we never saw anything like this happening here," Jensen said. "But we were ready."

Jones has seen things like this before.

He has worked plane crashes. He was part of a trauma unit in Baltimore during the September 11 attacks, so he witnessed the trauma of the Pentagon attack in Washington, D.C.

"The hardest part about last night, was the dozens of officers standing by," Jones said. "The looks on their faces. You know what that look is and you know what they are facing."

Sutton, the nurse manager of the emergency department, recognized those faces.

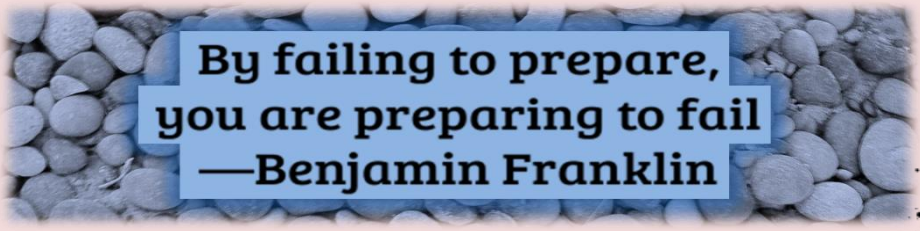
"Those were my husband's guys," she said, about the officers watching. "I knew them all."

She said her husband was on duty Thursday night, but was not injured.

"I don't think this is something you can shake," she said.

On Friday night, ambulances lined the ER door of Baylor. But it was quiet, unlike a night earlier.

"It is absolutely horrific what we are doing to each other as a society," Jensen said, in what could be considered a rare piece of candor from an official in a situation like this. "It is a shame that a group, because of race, religion or lifestyle feels that they are so disenfranchised that the only way they feel they can be heard is to harm officers. We all need to take a deep breath and learn to love one another."



# Bringing Public Health Preparedness Into the 21st Century

**By Emily Lord**

Source:http://www.domesticpreparedness.com/Commentary/Viewpoint/Bringing_Public_Health_Preparedness_Into_the_21st_Century_/

*The probability of certain public health threats, the costs and funding related to such threats, and the "silo" effect of the public health sector all contribute to the preparedness gap between public health and other sectors. It is time to bridge this gap and update preparedness efforts to better prepare for 21st Century threats.*

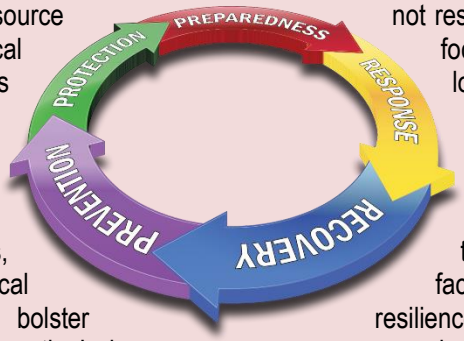
July 12 – **The U.S. disaster and disease health preparedness infrastructure has historically focused on a few key pillars including:**

- Strong national public health presence from the Department of Health and Human Services (HHS) Assistant Secretary for Preparedness and Response (ASPR), and from the Centers for Disease Control (CDC);
- Community-level preparedness by state and local public health departments; hospital system preparedness and healthcare coalitions; and
- Varying levels of engagement and support from emergency management.
- Although these pillars have prepared the United States better than ever before, it is not enough to meet the evolving threats that are now facing the nation.

**Reasons Behind the Public Health Preparedness Gap**

**First**, "disaster dissonance" widens the gap. Health preparedness has historically focused on readiness for catastrophic events. The challenge is that many people do not think they will ever be affected by a catastrophic event. The likelihood of a low-probability, high-impact hurricane like Katrina or Sandy seems small, so the level of preparedness needed for these events may not feel necessary. Thus, people recognize there is a threat, but many choose not to prepare.

**Second**, health preparedness is expensive and time-consuming, and funding is being continually reduced. The Public Health Emergency Preparedness (PHEP) cooperative agreement is the only major source of funding for state and local health departments, and it has significantly declined over the past 10 years. As a result, when unforeseen threats like Zika occur, funding is shifted from existing priorities, and there is not enough political will to raise the money to bolster capabilities, which leaves the nation's long-term preparedness weaker.




**Third**, health preparedness, like many fields, is siloed. Healthcare coalitions are an ideal example. Federal funding from ASPR's Hospital Preparedness Program (HPP) is meant to create a noncompetitive space for different parts of healthcare to plan, exercise, and coordinate for public health emergencies. Unfortunately, coalitions have struggled to breach the siloes within healthcare and bring more than just hospital systems to the table. This failure restricts the ability to assist patients with chronic care needs that would be best served in an outpatient setting like a pharmacy or a dialysis center. Ultimately, this harms the whole community because these other parts of healthcare tend to be less resilient, take longer to recover, or never reopen, which dampens economic recovery.

**Moving Toward 21st Century Preparedness**

Whether it is the term used or not, resilience – not response – should be the major focus going forward. Resilience looks much more broadly at how to create strong, cohesive communities with the goal that the stronger communities are, the better they will bounce back when faced with trauma. Although resilience is built by many different programs, a key component and first step forward should focus on incorporating the changes happening in healthcare such as: expanded coverage options; value-based medicine; Accountable Care Organizations

(ACOs); and the development of electronic health records.

U.S. healthcare reform has led to highest number of insured American's ever. Access to insurance supports and coincides with the growth of traditional provider networks and the development of new modalities such as convenient care clinics in pharmacies and the ability of pharmacists to provide immunizations. By their very nature, these new care delivery centers spread care away from a centralize location and increase resilience. Most importantly, there is a shift toward value-based medicine, which changes how healthcare systems approach patient engagement. Previously, revenue was directly connected to the amount of services provided; now it is shifting to how successful these services are. This is the goal of the newly created ACOs, which coordinate patient care to enhance wellness, avoid duplication of services, and better manage chronic illnesses. ACOs are resilience in action. They project into the community because they are designed to be concerned with patients' health outside the hospital's walls or a doctor's waiting room.

ACOs also help to answer a critically unanswered question in preparedness, "Who is responsible for a patient?" Traditionally, when an outbreak or disaster occurs, if a patient with chronic illness is not hospitalized or in a healthcare facility, there is no one responsible for ensuring that he or she has the life-sustaining healthcare required. Whether medicine, oxygen, or supportive care, patients are left to try to fill the gaps themselves or call emergency services. Efforts like ASPR's emPOWER map, which identifies vulnerable Medicare patients who use electric powered medical equipment, are extremely helpful to identify and assist these patients after an event occurs, but need to be better incorporated into day-to-day care. If the healthcare preparedness community begins to increase focus on collaborating with ACOs and other community-based organizations, it will significantly increase the resilience of communities.

Likewise, the adoption of electronic health records and the expansion of Health Information Exchanges are vital tools for ensuring resilience. With their use, patients can continue to receive the correct care they need by any provider in any region that can access the patient's records. Working to make these systems interoperable and protected by backups in other locations directly influences the level of care patients receive. None of this is easy, but it is critical for protecting patients.

Lastly, because healthcare in the United States is owned mostly by companies, it requires a type of partnership that can feel uncomfortable at first, but public/private partnerships is critical to protect patients. The first step to encourage public health to collaborate with other organizations is by thinking like a business to understand the motivations and limitations of what private healthcare can do. If traditional public health worked to understand these motivations and to prioritize lifting restrictions and assisting healthcare to continue its operations, private sector healthcare companies would be more receptive to working alongside its public partners. The result would be more resilient communities thanks to joint private and public resources being deployed effectively.

Protecting and building the resilience of communities' health is a long-term and incredibly difficult endeavor. It requires agility and the ability to capitalize on rapidly changing healthcare landscape, but it is possible if traditional views on what it takes to be ready can adapt and if funding has sufficient flexibility.

***Emily Lord*** *serves as the executive director of Healthcare Ready, a nonprofit set up in the wake of Hurricane Katrina to ensure that the catastrophic breakdowns in patient access to healthcare would never happen again. As the ten-year anniversary of Katrina approached, she led the expansion of Healthcare Ready's mission to address healthcare supply chain-wide resiliency and response by focusing on public policy and advocating for the adoption of best and promising disaster preparedness and response practices by government and industry. She has also led Healthcare Ready's response to multiple natural disasters including Hurricane Sandy, during which the organization coordinates and works to solve barriers to patient access to healthcare. She holds a Master of Public Administration from The George Washington University and a B.A. from the University of Wisconsin-Madison.*

# Roundup of spring, summer 2016 First Responders Group technology

Source: http://www.homelandsecuritynewswire.com/dr20160714-roundup-of-spring-summer-2016-first-responders-group-technology

July 14 – The Department Homeland Security (DHS) Science and Technology Directorate (S&T) regularly posts a roundup of key updates from projects currently in the development stages in S&T's First Responders Group (FRG). S&T offered this outline of FRG's accomplishments in April, May, and June.

**Hill Day Tech Demo**

On 15 June, S&T ventured to Capitol Hill for a First Responder Technology Hill Day in which congressional representatives had the opportunity to see how FRG is helping first responders. Two members of Congress stopped by to see S&T's tech first hand: Representative Dan Donovan (R-New York) Representative Michael McCaul (R-Teaxas), chair of the House Committee on Homeland Security, also attended and tested out several FRG and S&T technologies.

DHS S&T Under Secretary Dr. Reginald Brothers and Deputy Under Secretary Dr. Robert Griffin attended and spoke on how the event was a prime opportunity for S&T's scientists and engineers and industry partners to illustrate how S&T is addressing the challenges responders face in an effort to keep America safe.

**X-Ray Scanning Rover Operational Field Assessment**

On 10 May, FRG and the National Urban Security Technology Laboratory (NUSTL) conducted an operational field assessment (OFA) of the X-ray Scanning Rover (XSR), technology that quickly and accurately scans packages real-time for explosive devices, while keeping responders out of harm's way. The field tests were conducted in Arlington, Virginia, with members of the Michigan State Police, the New York City Police Department, Montgomery County (Maryland) Fire Rescue Service, and federal partner agencies. The goal: gather feedback on the XSR's overall usability from the responders who may one day use this technology in a real emergency situation.

At the OFA, responders were briefed on operating the technology and answered questions throughout the testing. Moving forward, the company plans to make necessary enhancements to the technology based on input from the operators. NUSTL will compile results from the OFA, are published here.

**Response and Defeat Operations Support**

FRG's Response and Defeat Operations Support (REDOPS) program helps the bomb squad community develop and evaluate technologies for rendering improvised explosive devices (IED) safe. The program achieved a major milestone during the first week in April, when Las Vegas law enforcement officers discovered an unusually configured IED. The officers turned to the FBI Las Vegas Field Office for assistance, and the field office subsequently contacted the FBI Counter-IED Unit. The unit recommended disarming the device using a method based on testing funded by the REDOPS program.

The method worked, and the IED was rendered safe without any injury to people or damage to property. Successes like this are the result of the REDOPS team continually working with the FBI Hazardous Devices School, the National Bomb Squad Commanders Advisory Board, and state and local bomb squads. Such involvement includes participation in technology evaluations and exercises like the Raven's Challenge 2016, a series of interoperability events designed to give military ordnance technicians and public safety bomb technicians the opportunity to evaluate resources and procedures in realistic environments.

**2016 Metropolitan Fire Chiefs Conference**

On 16 May, FRG Director Dan Cotter delivered a presentation at the 2016 Metropolitan Fire Chiefs Conference in Long Beach, California. The conference aimed to address problems and develop potential solutions to the challenges faced by fire departments in major metropolitan cities.

Cotter outlined S&T's mission and key projects in his presentation, including: technologies from FRG's First Responder Technologies division (like the Improved Structure Firefighting Glove and FINDER); how the Next Generation First Responder Apex program is defending against life-threatening hazards; Internet of Things (IoT) new opportunities and challenges; the latest with the International Forum to Advance First Responder Innovation; and much more.

**P25 CAP Advisory Panel Meeting**

On 4-5 May, FRG's Office for Interoperability and Compatibility's (OIC) Project 25 Compliance Assessment Program (P25 CAP) Advisory Panel (AP) held its second quarterly meeting at the Department of Commerce's Boulder Laboratories. P25 CAP is a formal, independent process for ensuring communications equipment advertised as P25 is actually compliant with P25 standards. The P25 CAP AP provides OIC with federal, state, local, tribal, and territorial perspectives on portable, handheld and vehicle-mounted radios and infrastructure equipment. Through the P25 CAP AP, OIC can support the collective interest of organizations that procure P25-compliant equipment. May 5 marked the AP's first meeting between the public sector and industry, creating an opportunity for engagement and a wide range of P25 stakeholder input.

**CAUSE IV Experiment**

The fourth installment of the Canada U.S. Enhanced Resiliency Experiment (CAUSE IV) took place 26-28 April in Sarnia, Ontario, and Port Huron, Michigan. The experiment kicked off with a test of the Public Safety Broadband Network (PSBN) with ambulances from both St. Clair and Lampton Counties. The PSBN test transitioned into a simulated tornado scenario disaster, which occurred on both sides of the border. Through live PSBN video connections, paramedics were able to provide continuous patient monitoring.

The scenario illustrated that connectivity issues should not force an ambulance three miles away from a hospital to head to a hospital that is thirty miles away.

S&T notes that the experiment displayed a great level of coordination and cooperation from both countries. On the final day, digital volunteers played a key role on either side of the border, allowing first responder agencies to analyze data from the tornado disaster area and allocate precious resources more efficiently. The experiment was also followed by an S&T #STTechTalk Twitter chat on 24 May, which provided an open forum for CAUSE IV participants and the public to ask questions and share lessons learned.

**eLoran Demonstration at New York Stock Exchange**

On 19 April, FRG and partners demonstrated eLoran, a precision timing technology for financial transactions, at the New York Stock Exchange. eLoran is a low-frequency, high-power radio navigation signal broadcast by ground-based transmission stations. This allows the signal to penetrate buildings and provide precision timing indoors and throughout urban environments.

**Datacasting System Debuts as an Essential Tool During Houston Flood**

During the week of 18 April, the City of Houston used FRG's datacasting system to securely share information when the city experienced severe flooding. Datacasting provides public safety users with the capability to transmit secure video and data over existing broadcast television signals to a targeted audience. The Houston Fire Department used the tool to survey flooded areas during the storms affecting the city. This capability helps first responders effortlessly communicate, providing situational awareness and access to information they need to make informed decisions when responding to an incident.

**New Virtual Social Media Working Group Report**

In April, the Virtual Social Media Working Group (VSMWG) published its newest report, From Concept to Reality: Operationalizing Social Media for Preparedness, Response and Recovery, which contains best practices and guidance on how to operationalize social media for the public safety and emergency response communities. Government agencies commonly use social media to push information to the public; however, they often hesitate to use information from the public for operational decision-making. The report discusses the

importance of operationalizing and institutionalizing social media for long-term use in decision-making and information sharing. In order for agencies to integrate social media into all aspects of preparedness, response and recovery, the report recommends considering people and processes, governance, and technology.

**SAVER Reports Released**

The System Assessment and Validation for Emergency Responders (SAVER) Program published more than twenty new reports from February to April, providing powerful new resources to inform purchasing decisions. "The list of real-world challenges first responders face is broad and deep, ranging from budgetary and policy issues, to capability and technology limitations, to current environmental, political and social events," S&T says. The most recent SAVER reports provided useful resources for law enforcement, search and rescue, emergency medical services, public safety diving, structural firefighting, security services, and the first responder community as a whole.

# Latest high-rise blaze in Dubai puts focus back on fire safety

Source: http://www.thenational.ae/uae/latest-high-rise-blaze-in-dubai-puts-focus-back-on-fire-safety

July 21 – The latest high-rise blaze in Dubai again focuses attention on the issue of fire safety in tall buildings.

Residents had to be removed from Sulafa Tower in Dubai Marina on Wednesday afternoon as flames spread through the 75-storey, 285-metre high residential building.

Civil defence crews were able to bring the blaze under control in about three hours, with no injuries reported.

Previous to the Sulafa Tower blaze, firefighters have had to deal with three major incidents in the emirate in the past four years, reportedly fuelled by combustible aluminium panelling.

These included The Torch apartment building last year, in which more than 100 flats were severely damaged, and the 2012 blaze that gutted Tamweel Tower in Jumeirah Lakes Towers.

Most notable was the fire that broke out at The Address Downtown Dubai hotel on New Year's Eve, causing severe damage to the tower.

In Ajman, a fire destroyed dozens of apartments in towers eight and six of the Ajman One complex. The exact cause of the fire was not determined by authorities, but an Ajman Police laboratory report stated that flaming material fell from a flat and landed on construction waste in front of Tower Eight.

**An amended UAE Fire and Life Safety Code, which is to be released this year, will include fines levied on building consultants should faulty fire safety material be discovered by civil defence inspectors.**

Manufacturers who sell building materials not approved by authorities will for the first time face prosecution under new provisions in the updated fire safety code.

The speed at which flames took hold of The Address Downtown Dubai hotel led authorities to clamp down on the use of combustible plastic-filled aluminium composite panels.

**Yet the most fire-retardant wall panels were still not being used on buildings across the country despite the fires. Three of the world's top aluminium composite panel makers confirmed that demand for their highest-rated panels was almost non-existent in the region.**

A 2012 building code introduced in Dubai aimed at halting the use of flammable aluminium composite panels was still not being fully implemented because of the high cost of system tests.

# Thirty-one leading scientific societies call for action on climate change

Source: http://www.homelandsecuritynewswire.com/dr20160629-thirtyone-leading-scientific-societies-call-for-action-on-climate-change

June 29 – **In a consensus letter to U.S. policymakers, a partnership of thirty-one leading nonpartisan scientific societies the other day reaffirmed the reality of human-caused climate change, noting that greenhouse gas emissions "must be substantially reduced" to minimize negative impacts on the global economy, natural resources, and human health.**

"Observations throughout the world make it clear that climate change is occurring, and rigorous scientific research concludes that the greenhouse gases emitted by human activities are the primary driver," the collaborative said in its 28 June letter to Members of Congress. "This conclusion is based on multiple independent lines of evidence and the vast body of peer-reviewed science."

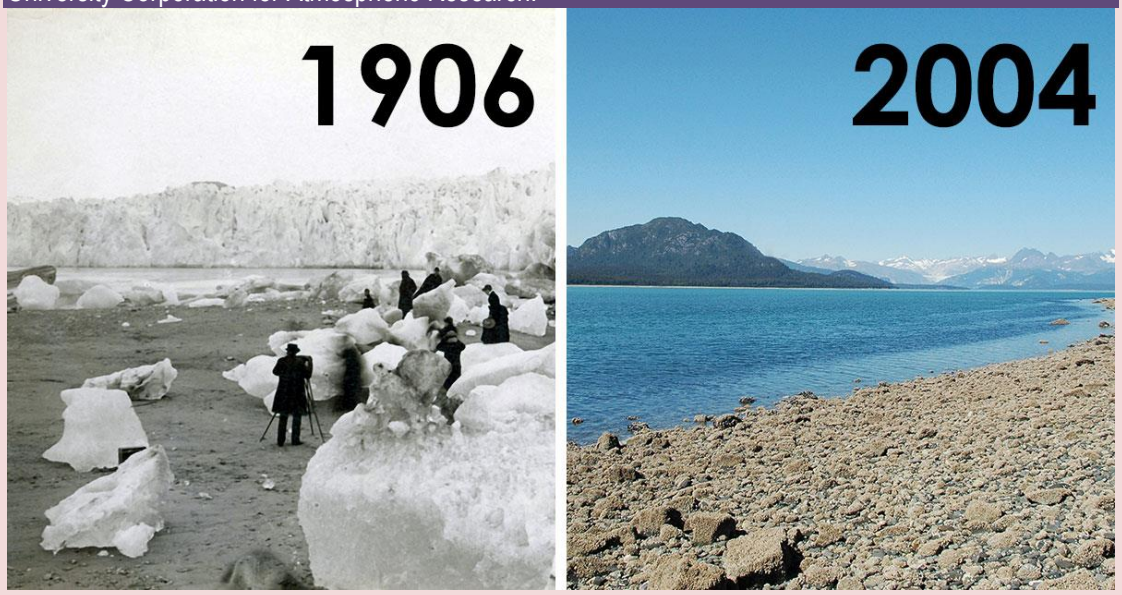
Climate-change impacts in the United States have already included increased threats of extreme weather events, sea-level rise, water scarcity, heat waves, wildfires, and disturbances to ecosystems and animals, the intersociety group reported. "The severity of climate change impacts is increasing and is expected to increase substantially in the coming decades," the letter added. The AAAS reports that the lettercited the scientific consensus of the vast majority of individual climate scientists and virtually every leading scientific organization in the world, including the U.S. Global Change Research Program, the U.S. National Academies, the Intergovernmental Panel on Climate Change, the American Association for the Advancement of Science (AAAS), the American Chemical Society, the American Geophysical Union, the American Meteorological Society, the American Statistical Association, the Ecological Society of America, and the Geological Society of America.

"To reduce the risk of the most severe impacts of climate change, greenhouse gas emissions must be substantially reduced," the group said, adding that adaptation is also necessary to "address unavoidable consequences for human health and safety, food security, water availability, and national security, among others."

The 28 June letter, representing a broad range of scientific disciplines, reaffirmed the key climate-change messages in a 2009 letter signed by 18 leading scientific organizations. The letter is being released again, by a larger consortium of thirty-one scientific organizations, to reassert the scientific consensus on climate change, and to provide objective, authoritative information to

policymakers who must work toward solutions. "Climate change is real and happening now, and the United States urgently needs to reduce greenhouse gas emissions," said AAAS Chief Executive Officer Rush Holt, executive publisher of the *Science* family of journals. "We must not delay, ignore the evidence, or be fearful of the challenge. America has provided global leadership to successfully confront many environmental problems, from acid rain to the ozone hole, and we can do it again. We owe no less to future generations."

**The 28 June letter was signed by leaders of the following organizations:** AAAS; American Chemical Society; American Geophysical Union; American Institute of Biological Sciences; American Meteorological Society; American Public Health Association; American Society of Agronomy; American Society of Ichthyologists and Herpetologists; American Society of Naturalists; American Society of Plant Biologists; American Statistical Association; Association for the Sciences of Limnology and Oceanography; Association for Tropical Biology and Conservation; Association of Ecosystem Research Centers; BioQUEST Curriculum Consortium; Botanical Society of America; Consortium for Ocean Leadership; Crop Science Society of America; Ecological Society of America; Entomological Society of America; Geological Society of America; National Association of Marine Laboratories; Natural Science Collections Alliance; Organization of Biological Field Stations; Society for Industrial and Applied Mathematics; Society for Mathematical Biology; Society for the Study of Amphibians and Reptiles; Society of Nematologists; Society of Systematic Biologists; Soil Science Society of America; University Corporation for Atmospheric Research.




**Leaders of participating organizations offered the following comments:**

"Climate change has far-reaching implications to everyone on our planet, as it is tied closely with national security, economics, human health, and food security. There is consensus in the scientific community – climate *is* changing. Now we need policymakers to act, to invest in research to understand the effects of climate change and opportunities to mitigate its drivers, and to adapt to its impacts."

**— RADM Jonathan W. White, USN (Ret.), president and CEO, Consortium for Ocean Leadership**

"Climate change poses significant challenges to natural and managed ecosystems. Now is the time for scientists and policy-makers to work together to address the issue of climate change in order to protect agricultural productivity, global food security and environmental resources."

**— Harold van Es, president, Soil Science Society of America**

"The environmental, social, and economic challenges posed by climate change are among the most important issues of our time. Comprehensive solutions grounded in understanding of ecological systems – our lands, waters, oceans, and atmosphere — and

society are urgently needed. A sustainable future remains possible if we work together and act now."

**— Monica G. Turner, president, Ecological Society of America**

"This letter, signed by a diverse set of scientific organizations, conveys the solid scientific consensus view that anthropogenic climate change is occurring. How climate change will manifest for specific geographic regions within the next decade and beyond is a topic of intense research. Statisticians are experts in making decisions when specifics aren't clear and stand ready to work with decision-makers."

**— Jessica Utts, president, American Statistical Association**

"Geological studies have demonstrated that climate has changed repeatedly in the past and that future climate change is inevitable. Understanding the complex processes involved in climate change is necessary for adaptation and mitigation."

**— Jonathan G. Price, Ph.D., CPG, President, Geological Society of America**

"The reality of climate change is already upon us, and is affecting not only our lives but that of all life on earth. We must do all that we can to mitigate these effects using scientific knowledge and mobilizing society for action. It is the responsibility of our politicians to move us forward in these actions."

**—Dr. Robin L. Chazdon, executive director of the Association for Tropical Biology and Conservation,**

"The phenomenon of human-mediated climate change is not a matter of opinion, but of careful evaluation of data from a vast spectrum of scientific disciplines. What remains unclear is the degree to which climate change will cause environmental, social, and economic havoc. Estimates range from severe to catastrophic. We owe it to our children and to our children's children to take bold action now so that our descendants do not pay the price for our generation's greed."

**— Anne D. Yoder, president, Society of Systematic Biologists**

"Climate change is one of the most profound challenges facing our society. Consensus on this matter is evident in the diversity of organizations that have signed this letter. Science can be a powerful tool in our efforts to mitigate and adapt to the impacts of climate change, and we stand ready to work with policymakers as they deliberate various options for action."

**— Christine McEntee, executive director/CEO of the American Geophysical Union**

"Climate influences where plants and animals live. Rapid climate change will force species to find new habitat in hospitable conditions, but many species will not be able to and will go extinct. This isn't good. It disrupts our ecosystems, which are the source for our food, and clean air and water."

**— Robert Gropp, Ph.D., interim co-executive director, American Institute of Biological Sciences**

# U.S. suffered at least $8 billion climate-related disasters so far this year

Source: http://www.homelandsecuritynewswire.com/dr20160711-u-s-suffered-at-least-8-billion-climaterelated-disasters-so-far-this-year

July 11 – We are only halfway through 2016 and the United States has already seen eight weather and climate-related disasters* that have each met or exceeded $1 billion in damages. These eight disasters resulted in the loss of thirty lives, and caused at least $13.1 billion, according to an analysis by NOAA's National Centers for Environmental Information (NCEI).

A high number of these events impacted Texas throughout the Spring - most notably - several intense hail storms overly densely populated cities and the 17 April Houston flood event.

NOAA says that the eight billion-dollar disasters in the U.S.(damages for the late-June flooding event in West Virginia, which are still being assessed, are not included) are:

- 22-24 February: Southeast/Eastern tornadoes
- 8-12 March: Texas & Louisiana flooding
- 17-18 March: Southern severe weather
- 23-24 March: North Texas hail storm
- 10-12 April: North/Central Texas hail storm
- 17-18 April: Houston flooding
- 26 April-2 May: South/Southeast tornadoes
- 21-26 May: Rockies/Central tornadoes & severe storms

The first six months of 2016 are well above-average for the number of billion-dollar events compared with the same period in years past.

In 2015 the U.S. experienced a total of 10 individual disasters reaching the $1 billion threshold. These events included a drought event, two flooding events, five severe storm events, a wildfire event, and a winter storm event, resulting in 155 lives lost and costing more than $22 billion in economic damages. To see the newly released costs for each of the ten events, see the NCEI billion dollar disaster table of events for 2015.

**Since 1980 the U.S. has sustained 196 weather and climate disasters in which overall damages/costs reached or exceeded $1 billion. The total cost of these 196 events exceeds $1.1 trillion.**

## Gauging the impact of climate change on U.S. agriculture

Source: http://www.homelandsecuritynewswire.com/dr20160712-gauging-the-impact-of-climate-change-on-u-s-agriculture

July 12 – To assess the likely impact of climate change on U.S. agriculture, researchers typically run a combination of climate and crop models that project how yields of maize, wheat, and other key crops will change over time. But the suite of models commonly used in these simulations, which account for a wide range of uncertainty, produces outcomes that can range from substantial crop losses to bountiful harvests. These mixed results often leave farmers and other agricultural stakeholders perplexed as to how best to adapt to climate change. Researchers have now devised a way to provide these stakeholders with the additional information they need to make

more informed decisions. The new approach tracks key factors affecting crop yields, enabling early adaptation.

To assess the likely impact of climate change on U.S. agriculture, researchers typically run a combination of climate and crop models that project how yields of maize, wheat, and other key crops will change over time. But the suite of models commonly used in these simulations, which account for a wide range of uncertainty, produces outcomes that can range from substantial crop losses to bountiful harvests. These mixed results often leave farmers and other agricultural stakeholders perplexed as to how best to adapt to climate change.

Now, in a study published in *Environmental Research Letters,*a research team at MIT and the University of California at Davis, has **devised a way to provide these stakeholders with the additional information they need to make more informed decisions. In a nutshell, the researchers complement the results of climate/crop model runs with projections of five useful indices of agriculture/climate interaction — dry days, plant heat stress, frost days, growing season length and start of field operations — that clarify what's driving projected yields up or down.**

"It's very difficult to investigate the impact of the climate on agriculture because models don't agree even on the sign of projected yield, or indicate the mechanism behind it," says the study's lead author, Erwan Monier, a principal research scientist with the MIT Joint Program on the Science and Policy of Global Change. "Our work provides an alternative way to look at the fate of agriculture under climate change that provides information that's more relevant to farmers than existing climate/crop models."

Using the MIT Integrated Global System Modeling (IGSM) framework, which accounts for key sources of uncertainty and incorporates all five agro-climate indices, Monier and his collaborators ran simulations to estimate the potential effects of climate change on agriculture in the United States by 2100.

Under a scenario in which greenhouse gas emissions are unconstrained, the model projected that the United States will experience fewer frosts, a longer growing season, more heat stress, and an earlier start of field operations by the end of the century. When greenhouse gas emissions reduction policies — one aimed at capping the rise in global mean surface temperature between pre-industrial times and 2100 at 2 degrees Celsius, the other targeting a 2.5 C cap — were applied, projected changes in four out of the five indices were cut in half.

This suggests that aggressive greenhouse gas mitigation could sharply reduce the effects of climate change — both adverse ones, such as increased heat stress, and beneficial ones, such as a longer growing season.

The research team also determined that these climate mitigation policies would prevent changes in any of the five indices from exceeding those that arise from natural year-to-year variations in the climate that we already experience, thus limiting the severity of climate-related impacts on agriculture for the rest of the century.

Enabling these results is a new, more efficient, integrated approach to modeling the impact of climate on agriculture and estimating the benefits of climate mitigation efforts.

Rather than relying on the traditional approach of using a multi-model ensemble (the standard one, the CMIP5, comprises more than 30 different climate models) to estimate the uncertainty in the impact of climate change on agriculture, the researchers used multiple simulations of a single model where key sources of uncertainty are explored by varying several model assumptions. **These include the response of the global climate system to changes in atmospheric greenhouse gas levels, the natural variability in the climate system, and the emissions scenario selected.**

Bypassing the need to run multiple climate models through international coordinated efforts among multiple climate research institutes, the MIT model delivers a similar range of results with far greater efficiency. And because it integrates both climate and economic projections, it provides a more direct estimate of the economic benefit of climate mitigation.

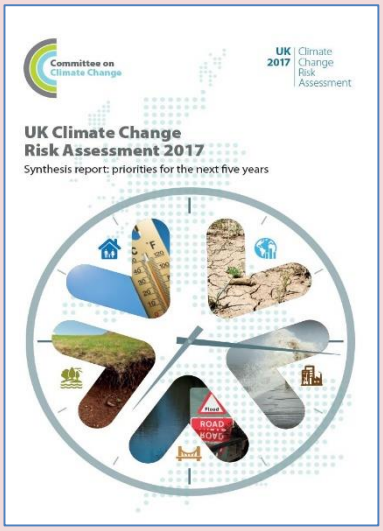
The study was funded by the U.S. Environmental Protection Agency, Department of Energy, and National Science Foundation.

*— Read more in Erwan Monier et al., "Uncertainty in future agro-climate projections in the United States and benefits of greenhouse gas mitigation," Environmental Research Letters 11, no. 5 (26 April 2016).*

# Assessing climate change risks to U.K.

Source: http://www.homelandsecuritynewswire.com/dr20160714-assessing-climate-change-risks-to-u-k

July 14 – **Climate change is happening now. Globally, 14 of the 15 hottest years on record have occurred since 2000.**




The impacts of climate change are already being felt in the United Kingdom, and urgent action is required to address climate-related risks, the Committee on Climate Change's (CCC)'s Adaptation Sub-Committee (ASC) said the other day.

The ASC's new independent report to Government, **U.K. Climate Change Risk Assessment Evidence Report**, sets out the most urgent risks and opportunities arising for the United Kingdom from climate change.

The CCC notes that the report is the result of more than three years of work involving hundreds of leading scientists and experts from the public and private sectors and civil society. The risk assessment has been peer reviewed by U.K. and international specialists.

Changes to the U.K. climate are likely to include periods of too much or too little water, increasing average and extreme temperatures, and sea level rise.

**The report concludes that the most urgent risks for the United Kingdom resulting from these changes are:**

- *Flooding and coastal change*risks to communities, businesses and infrastructure.
- Risks to *health, wellbeing and productivity* from high temperatures
- Risk of *shortages in the public water supply,* and water for agriculture, energy generation and industry, with impacts on freshwater ecology.
- Risks to *natural capital,* including terrestrial, coastal, marine and freshwater ecosystems, soils and biodiversity.
- Risks to *domestic and international food production and trade.*
- Risks of *new and emerging pests and diseases,* and invasive non-native species, affecting people, plants and animals.

**The opportunities for the United Kingdom from climate change include:**

- *U.K. agriculture and forestry may be able to increase production*with warmer weather and longer growing seasons, if constraints such as water availability and soil fertility are managed.
- There may be *economic opportunities for U.K. businesses*from an increase in global demand for adaptation-related goods and services, such as engineering and insurance.

The impact of the recent vote to leave the European Union does not change the overall conclusions of the risk assessment. However, some individual risks may change if EU-derived policies and legislation are withdrawn and not replaced by equivalent or better U.K. measures. The Adaptation Sub-Committee will assess the implications of the EU referendum in its next statutory report to Parliament on the U.K. National Adaptation Program, due to be published in June 2017.

Lord Krebs, Chairman of the Adaptation Sub-Committee of the Committee on Climate Change,said: "The impacts of climate change are becoming ever clearer, both in the United Kingdom and around the world. We must take action now to prepare for the further, inevitable changes we can expect. Our independent assessment today, supported by the work of hundreds of scientists and other experts, identifies the most urgent climate change risks and

opportunities which need to be addressed. Delaying or failing to take appropriate steps will increase the costs and risks for all UK nations arising from the changing climate."

**Background**

- The Climate Change Act requires the U.K. government to compile every five years its assessment of the risks and opportunities arising for the United Kingdom from climate change, known as the Climate Change Risk Assessment (CCRA). The ASC's Evidence Report published earlier this week will inform the government's second Climate Change Risk Assessment due to be presented to Parliament in January 2017. The first CCRA was presented to Parliament by Government in 2012.
- The Climate Change Act places a duty on the Adaptation Sub-Committee to provide independent advice six months in advance of the government's Climate Change Risk Assessment report to Parliament being due. The Evidence Report, consisting of eight individual chapters looking at key areas of risk and opportunity, constitutes the ASC's advice on the government's second CCRA. Each chapter has been written by expert lead authors supported by co-authors with particular specialties. The individual chapters are the product of their expert authors. A Synthesis Report has also been produced by the ASC to highlight the key messages of the Evidence Report.

▶ **The Synthesis Report U.K. Climate Change Risk Assessment Evidence Report, together with the chapters of the full Evidence Report, and associated materials** is available here.

# Breaking records: The first six months of 2016 the warmest half-year on record

Source: http://www.homelandsecuritynewswire.com/dr20160720-breaking-records-the-first-six-months-of-2016-the-warmest-halfyear-on-record

July 20 – **Two key climate change indicators — global surface temperatures and Arctic sea ice extent — have broken numerous records through the first half of 2016, according to NASA analyses of ground-based observations and satellite data.**

Each of the first six months of 2016 set a record as the warmest respective month globally in the modern temperature record, which dates to 1880, according to scientists at NASA's Goddard Institute for Space Studies (GISS) in New York. The six-month period from January to June was also the planet's warmest half-year on record, with an average temperature 1.3 degrees Celsius (2.4 degrees Fahrenheit) warmer than the late nineteenth century.

Five of the first six months of 2016 also set records for the smallest respective monthly Arctic sea ice extent since consistent satellite records began in 1979, according to analyses developed by scientists at NASA's Goddard Space Flight Center, in Greenbelt, Maryland. The one exception, March, recorded the second smallest extent for that month.

NASA notes that while these two key climate indicators have broken records in 2016, NASA scientists said it is more significant that global temperature and Arctic sea ice are continuing their decades-long trends of change. Both trends are ultimately driven by rising concentrations of heat-trapping carbon dioxide and other greenhouse gases in the atmosphere.

The extent of Arctic sea ice at the peak of the summer melt season now typically covers 40 percent less area than it did in the late 1970s and early 1980s. Arctic sea ice extent in September, the seasonal low point in the annual cycle, has been declining at a rate of 13.4 percent per decade.

"While the El Niño event in the tropical Pacific this winter gave a boost to global temperatures from October onwards, it is the underlying trend which is producing these record numbers," GISS Director Gavin Schmidt said.

Previous El Niño events have driven temperatures to what were then record levels, such as in 1998. But in 2016, even as the effects of the recent El Niño taper off, global temperatures have risen well beyond those of eighteen years ago because of the overall warming that has taken place in that time.

The global trend in rising temperatures is outpaced by the regional warming in the Arctic, said Walt Meier, a sea ice scientist at NASA Goddard.

"It has been a record year so far for global temperatures, but the record high temperatures in the Arctic over the past six months have been even more extreme," Meier said. "This warmth as well as unusual weather patterns have led to the record low sea ice extents so far this year."

NASA tracks temperature and sea ice as part of its effort to understand the Earth as a system and to understand how Earth is changing. In addition to maintaining nineteen Earth-observing space missions, NASA also sends researchers around the globe to investigate different facets of the planet at closer range. Right now, NASA researchers are working across the Arctic to better understand both the processes driving increased sea ice melt and the impacts of rising temperatures on Arctic ecosystems.

NASA's long-running Operation IceBridge campaign last week began a series of airborne measurements of melt ponds on the surface of the Arctic sea ice cap. Melt ponds are shallow pools of water that form as ice melts. Their darker surface can absorb more sunlight and accelerate the melting process. IceBridge is flying out of Barrow, Alaska, during sea ice melt season to capture melt pond observations at a scale never before achieved. Recent studies have found that the formation of melt ponds early in the summer is a good predictor of the yearly minimum sea ice extent in September.

"No one has ever, from a remote sensing standpoint, mapped the large-scale depth of melt ponds on sea ice," said Nathan Kurtz, IceBridge's project scientist and a sea ice researcher at NASA Goddard. "The information we'll collect is going to show how much water is retained in melt ponds and what kind of topography is needed on the sea ice to constrain them, which will help improve melt pond models."

Operation IceBridge is a NASA airborne mission that has been flying multiple campaigns at both poles each year since 2009, with a goal of maintaining critical continuity of observations of sea ice and the ice sheets of Greenland and Antarctica.

At the same time, NASA researchers began in earnest this year a nearly decade-long, multi-faceted field study of Arctic ecosystems in Alaska and Canada. The Arctic-Boreal Vulnerability Experiment (ABoVE) will study how forests, permafrost and other ecosystems are responding to rising temperatures in the Arctic, where climate change is unfolding faster than anywhere else on the planet.


ABoVE consists of dozens individual experiments that over years will study the region's changing forests, the cycle of carbon movement between the atmosphere and land, thawing permafrost, the relationship between fire and climate change, and more.

# The growing fear of a physical security incident

Source:http://www.torchmarketing.co.uk/wp-content/uploads/2016/05/WSR%20Jun16.pdf

*The Business Continuity Institute recently published its annual Horizon Scan Report – a report that looks at what the biggest concerns are to business continuity professionals across the world – and yet again it showed that the greatest of those concerns is a cyber attack. In fact, all of the top three concerns relate to IT infrastructure with data breach coming second and IT/telecoms outage coming third.*


Perhaps that is not surprising considering the increasing likelihood there is of such an attack taking place. One study carried out last year by NTT Com Security (Risk:Value Report 2016) indicated that two-thirds of organizations predicted that they will suffer a data breach at some point in the future.

What was a surprising finding in the Horizon Scan Report was the rise of physical security as a major concern for organizations, with security incident such as vandalism, theft, fraud or protest moving from sixth place in 2015 to fifth place this year, and act of terrorism moving from tenth place to fourth. Of course it needs to be borne in mind that the events in Paris at the end of the year will still have been fresh in peoples' minds, and will have got them thinking about what impact an act of terror could have on their organization.

> "Whatever the crisis, it is essential that organizations have plans in place to be able to deal with the consequences."

You don't need to be targeted directly to be disrupted by a security incident or an act of terror, any organization in the vicinity of such an event has the potential to be disrupted. When the hostage situation was taking place at the Lindt Café in Sydney, many offices in the surrounding area had to be evacuated.

Whatever the crisis, it is essential that organizations have plans in place to be able to deal with the consequences.

***Andrew Scott CBCI*** *is the Senior Communications Manager at the Business Continuity Institute who joined after a brief stint working as the Press Officer for a national health charity. Prior to that he had over ten years at the Ministry of Defence working in a number of roles including communications and business continuity. During this time he also completed a Masters in Public Relations at the University of Stirling. Andrew has successfully taken the Certificate of the BCI exam which he passed with merit.*