CBRNE NEWSLETTERRORISM

June 2016

E-Journal for CBRNE & CT First Responders

www.cbrne-terrorism-newsletter.com

Symetrica presents wearable neutron detector system for first responders

Source: http://www.symetrica.com

May 23 – **Symetrica has introduced a prototype wearable detector system that provides high-**

sensitivity, high-accuracy and resolution for an improved source detection performance. The compact and lightweight Neutron Vest, which has been officially presented at the 2016 IEEE Symposium on Radiation Measurements and Applications (SORMA), will provide security professionals an alternative to backpack and handheld systems guaranteeing the same level of performance against the ANSI standard but with substantially reduced weight and bulk.

Neutron Vest is a radiation detector system comprised of up to four wearable neutron detector modules. When worn on the torso, the system provides comparable sensitivity to a backpack system with the advantages of being ultra-light – each module weighs 1lb – and supporting an intuitive smartphone interface.

Based upon Symetrica's Discovery Technology®, each neutron detector module comprises a thin LiF/ZnS thermal neutron detector, a silicon photomultiplier (SiPM) array as well as pulse-shape discrimination logic and internal health monitoring. The lightweight internal battery

allows over twenty hours of operation from a four-hour charge.
The use of multiple detectors allows the system to provide directional information in the horizontal plane to support the search for threats. By analysing the relative counts from each module, direction can be determined with a resolution of 45 degrees. Additionally, the data from the Neutron Vest is combined with timestamps and GPS data to create a radiation map that can be further processed to estimate the threat location. An inbuilt Bluetooth connection allows the data to be transmitted to Symetrica's handheld radio-isotope identification device (RIID) VeriFinder™ or a smartphone, where advanced anomaly detection and background monitoring algorithms are run and presented to the operator via an intuitive GUI.
The integrated health-check algorithms ensure that the Neutron Vest continues to operate optimally without the need for costly and disruptive in-field recalibration, thus reducing operational costs and boosting user confidence.
Commenting on the Neutron Vest announcement, Jeff McCray, Symetrica's VP of Business Development, said: "Throughout this development program, the Neutron Vest is achieving impressive results. The source detection performance meets ANSI N42.53-2013 and IAEA NSU-NSD (v3). Gamma-ray rejection (measured at $1:10^8$) also meets the ANSI and IAEA standards. Neutron Vest is a further example of how Symetrica's advanced Discovery Technology® can be honed for real-world applications, bringing simplicity, accuracy, reliability and convenience to the operator."
SORMA West 2016 focuses exclusively on radiation detection for homeland and national security applications. The high profile conference showcases technology solutions with presentations and plenary talks, including Dr Mark Foster, Symetrica's Neutron Vest program leader, presenting a paper on the Neutron Vest.

Dirty Bombs – Myth versus Fact

By P. Andrew Karam
Source: http://www.cbrneportal.com/dirty-bombs-myth-versus-fact/

May 25 – There have been a LOT of stories about radiological terrorism in the news lately. We heard that ISIS was surveilling Belgian nuclear power plants, that they killed a nuclear worker to steal his identification, and even that they might be using "nuclear" drones to drop radioactive materials from above upon the unsuspecting. What is often missing in these stories is a realistic – that is, a scientifically informed – discussion about how dangerous attacks such as these might actually be. There is a broad assumption in the press and among the population as a whole that any radiological attack is likely to lead to untold deaths; from radiation sickness in the short term and from radiation-induced cancer over the ensuing decades. As a long-time radiation safety professional, these assumptions are amusing at best, insulting at worst. Not only that, but these assumptions can lead us as a society to make decisions regarding radiological attacks that could be ruinously expensive and disruptive both socially and politically. In this editorial (and hopefully in follow-on pieces) I would like to address some of these concerns to help you sort out what you really need to worry about.

▶ **Read the full article at source's URL.**

Andrew Karam *is a radiation safety expert with 35 years of experience, beginning with 8 years in the US Navy's Nuclear Power Program that included 4 years on an attack submarine. He has published over two dozen scientific and technical papers and is the author of 16 books and several hundred articles for general audiences. He has worked on issues related to radiological and nuclear terrorism for over 10 years.*

Triangular UFO With Egyptian Symbols Circling Around UK Nuclear Bunkers

Source: http://clapway.com/2016/05/26/ufo-egyptian-symbols-uk-nuclear/

May 26 – The truth may be out there. And people are beginning to speak up. This is the case with the most famous UFO sighting in British history. It was dubbed the British Roswell, ex-police officer breaks silence over RAF Bentwaters UFO claims. Gary Heseltine, a former British police officer has come forward. Highlighting new information regarding the triangular UFO with Egyptian type hieroglyphics. What were the aliens after? New claims suggest that the RAF Bentwaters American military base once held the largest stash of nuclear weapons in Europe. This could explain the UFO flybys.

British Nuclear Whistleblower

To the disdain of the British and American government, there have been a few whistleblowers regarding the UFO sighting. Some have foretold alien Egyptian spaceships. And others shed light on the nuclear weapons the aliens may have been after. Heseltine, a former British Transport Police officer with nearly 24 years of service came forward about the nuclear news. Heseltine said that a Colonel Halt explained that the Suffolk airbase had a large stockpile of nuclear weapons. The largest in Europe, according to reports.

UFO Flyby a Possible Attack

The source of the information came from a U.S. Air Force commander. Were the nuclear weapons another government cover-up? The original stories regarding the UFO at the British Roswell were supported by a few witness accounts. One account came from Staff, Sergeant Jim Penniston. Penniston said that the triangular spacecraft was smooth to the touch. And it had Egyptian-like hieroglyphics on it. Despite the Hollywood type description of the UFO. It may have been a possible alien attack. The aliens may have wanted to get their little green hands on the largest nuclear weapon cache in Europe.

A Growing Nuclear Space War

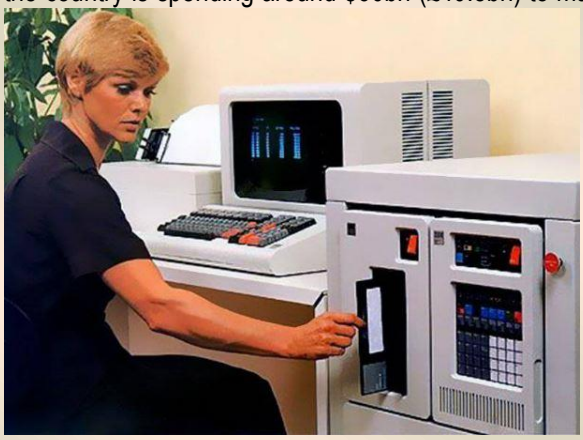
Elon Musk may be the next intergalactic commander of a space army fighting a nuclear war. Or not. The UFO sighting, as convinced as the witnesses are, is most likely another hoax. Or if not a hoax. Will remain covered-up by the British and American governments forever. If aliens were so sophisticated, why would they want our weapons anyway? They most likely have their own weapons of mass destruction. One's far more deadly than what we have here on Earth. Like Trump for example. He may be a super high-tech alien weapon of mass destruction. More Trump alien news to follow.

US nuclear arsenal controlled by 1970s computers with 8in floppy disks

Source: https://www.theguardian.com/technology/2016/may/26/us-nuclear-arsenal-controlled-by-1970s-computers-8in-floppy-disks

May 26 – The US military's nuclear arsenal is controlled by computers built in the 1970s that still use 8in floppy disks.

A report into the state of the US government, released by congressional investigators, has revealed that the country is spending around $60bn (£40.8bn) to maintain museum-ready computers, which many do not even know how to operate any more, as their creators retire.



The Defense Department's Strategic Automated Command and Control System (DDSACCS), which is used to send and receive emergency action messages to US nuclear forces, runs on a 1970s IBM computing platform. It still uses 8in floppy disks to store data.

We're not even talking the more modern 3.5in floppy disk that millennials might only know as the save icon. We're talking the OG 8in floppy, which was a large *floppy* square with a magnetic disk inside it. They became commercially available in 1971, but were replaced by the 5¼in floppy in 1976, and by the more familiar hard plastic 3.5in floppy in 1982.

Shockingly, the US Government Accountability Office said: "Replacement parts for the system are difficult to find because they are now obsolete."

The Pentagon said it was instigating a full replacement of the ancient machines and while the entire upgrade will take longer, the crucial floppy disks should be gone by the end of next year.

Given that magnetic media has a finite shelf life, and that disks and the drives needed to read and write to them are older than some of the operators of the machinery, the floppy revelation makes you wonder whether the US could even launch a nuclear attack if required. An "error, data corrupted" message could be literally life or death.

Should South Korea be Iran's next nuclear energy partner?

By Duyeon Kim and Ariane Tabatabai

Source: http://thebulletin.org/should-south-korea-be-irans-next-nuclear-energy-partner9495

May 31 – Since reaching an historic agreement to scale back its nuclear program last summer, Iran, now liberated from some sanctions, has been actively courting old and new business partners in an effort to revitalize its economy. Among them is South Korea, an already active player in various Iranian sectors. In May, South Korean President Park Geun-hye paid a visit to Tehran, the first by a Korean head of state in 54 years. Accompanied by some 230 business executives, Park reached provisional, multi-billion-dollar deals with Iranian President Hassan Rouhani to boost cooperation in fields including information technology, science, education, and energy; she also met with supreme leader Ayatollah Ali Khamenei, the country's highest authority figure.

In addition to their established economic and business ties, Iran and South Korea are also beginning to explore potential cooperation in a formerly off-limits sector: nuclear energy. Following the 2015 nuclear deal (the Joint Comprehensive Plan of Action, or JCPOA), Iran is now seeking to expand its peaceful nuclear energy ties with other countries. Meanwhile, advances made by the South Korean nuclear industry, which makes both small modular reactors

and large nuclear power plants, have made it an attractive supplier in recent years.

From a nuclear nonproliferation, security, or geopolitical perspective, news about Tehran's interest in South Korean nuclear reactors may raise eyebrows, eliciting serious concern or objections. This is because, JCPOA notwithstanding, the international community still deems Iran an outlier and a rogue state. And while South Korea is a key US ally in East Asia—one that developed its nuclear energy program thanks to civil nuclear cooperation agreements with Washington—Tehran has a record of noncompliance with its international obligations under the Nuclear Nonproliferation Treaty, and its relations with the United States are characterized by hostility, miscommunication, and distrust. Moreover, Iran has cooperated on missiles and possibly even nuclear projects with North Korea, a country Seoul considers a vital threat to its security. Nonetheless, if we set aside these concerns for a moment, what at first might seem like a ludicrous idea is worth examination and analysis for longer-term policy considerations.

To be sure, there are potential geopolitical and economic challenges and concerns ahead for Iran and South Korea if they choose to become nuclear business partners, and possible downsides to such a relationship. But there are likely upsides, too: Iran—now liberated to build up its nuclear energy industry provided it abides by restrictions in the JCPOA and refrains from weapons development—is going to pursue nuclear power one way or the other. It will have a choice of suppliers, and among them, South Korea has a particularly good track record for high-quality construction, operation, and maintenance. In other words, encouraging Tehran to buy from South Korea—rather than, say, Russia or China—could help establish a strong culture of nuclear safety, nuclear security, and nonproliferation in Iran. If done well, such cooperation may not simply benefit the two countries, but could also help sustain the JCPOA and encourage Iranian compliance with its nuclear commitments even after some of the key elements of the deal conclude in 10 to 15 years.

The competition

It is no surprise that Iran and South Korea would want to rekindle their overall business partnership now that the nuclear deal is being implemented. The two countries have enjoyed a long history of amicable relations since establishing diplomatic ties in 1962. South Korean steel and construction firms were among the first outsiders to help build Iran's infrastructure in the 1970s. Leaders from South Korea's emerging industries, in particular the automobile sector, traveled to Tehran in the same time period to exchange ideas with fast-developing Iranian businesses. Hyundai executives would fly to Tehran to meet with Iran's Paykan, a leading car producer in the Middle East. The South Korean tech and auto sectors have since boomed, while Iran's collapsed under the weight of mismanagement and sanctions, but the relationship has remained strong. Korean giants like Samsung, LG, Hyundai, and Kia all have a large presence in the Iranian market. A "Tehran Street" exists in Seoul's business district, while a "Seoul Street" and "Seoul Park" exist in Iran. The fact that South Korea has large investments in Iran may put it in a better position to sell nuclear goods and services to Iran than would-be competitors with little experience in the country. The competition is significant, though. Russia has had a quasi-monopoly over the Iranian nuclear sector for more than two decades. It is an attractive nuclear supplier for several reasons: It offers a financing package that makes Russian reactors the cheapest in the global market; it is the only country that takes back spent fuel; and it employs a model under which it builds, owns, and operates nuclear plants in the host country—which many would-be buyers deem appealing.

It's not certain, however, that Moscow's extremely advantageous marketing strategy is sustainable. This uncertainty is partly due to Russia's political and economic isolation stemming from its aggressive foreign policy, which has made it the target of sanctions, as well as to its own domestic economic challenges. (Moscow recently announced plans to sell part of its investment in Turkey's Akkuyu nuclear power plant due to domestic economic difficulties.) While Russia presumably abides by the Nuclear Suppliers Group guidelines when supplying nuclear power reactors, its lack of transparency when it comes to requirements for civil nuclear cooperation projects has led to credibility and confidence questions from many in the international community. Iran also distrusts Russia, which has a history of long construction delays and

using energy as a bargaining chip—for example, by threatening to pull the plug on joint projects or withhold equipment and fuel to further its own political goals.

Meanwhile China and Japan, and perhaps even France, are all hoping to gain ground in selling nuclear energy infrastructure to Iran following the JCPOA. China, in particular, is well-positioned to make such gains, as it has a large presence in various sectors of the Iranian economy. However, Tehran does not trust Beijing to use high-quality materials and equipment, and has indicated it is willing to work with other partners. Thus, Iran may see South Korea as the most economical and reliable seller.

Challenges and concerns

In forging a nuclear business relationship with Iran, South Korea would face challenges that go beyond the immediate concerned reaction of nonproliferation and security experts.

First, Seoul would need to consult with Washington prior to moving forward with discussing any commercial nuclear deals with Tehran, since the United States may have political, strategic, and legal objections.

Seoul would also have to consider the political implications of engaging in peaceful nuclear trade with a country that is an intimate business partner with North Korea on ballistic missiles. A concern here would be the possibility of nuclear information and technology clandestinely flowing from Iran into North Korea, despite on-going sanctions, or vice-versa.

But this proliferation risk also shows how important it is—not just for Tehran, but for the rest of the world—for Iran to be able to engage in constructive, civilian nuclear cooperation. New ventures could show Tehran that it is benefiting, not suffering, from the JCPOA, and pinpoint the advantages of remaining in compliance with international obligations. But preventing potential cooperation between Iran and South Korea—or any trusted nuclear exporter—could give Tehran the incentive to turn to suppliers that do not require the same high standards in nuclear safety and security and nonproliferation. Worse yet, Iran could return to noncompliance if it cannot fulfill its nuclear energy needs within the JCPOA framework.

Second, if the notion of South Korea and Iran engaging in peaceful nuclear trade does, in fact, become a reality, Seoul will have to confront the question of whether this commerce is legal. South Korea would not be allowed to sell large nuclear power plants to Tehran without Washington's approval if they were based on American technology. If South Korea were to sell reactors containing American equipment or technology to Iran, Tehran would have to conclude a nuclear cooperation agreement with the United States, which is unlikely to happen. Seoul would have no legal barriers, however, to selling its small modular reactors—called System-integrated Modular Advanced Reactors—because Seoul claims they do not contain American technology or components. One caveat here is that some have argued otherwise, saying US federal law does not clearly define what constitutes American technology in a nuclear reactor. The broader consideration for Washington would be whether it is more comfortable with Iran pursuing small modular reactors as opposed to conventional, large reactors.

Seoul might also face another roadblock selling its small modular reactors to Iran. South Korea has already agreed to sell them to Saudi Arabia, a much larger market for nuclear energy and Iran's adversary. Seoul would not want to jeopardize its relationship with Riyadh simply for the sake of diversifying its customer base. Another problem could be a possible mismatch in technical configurations—some industry insiders say South Korea's small modular reactors do not meet the electricity generation capacity desired by Iran. For these two reasons, the South Korean nuclear industry is said to be discussing the potential sale of large nuclear power plants to Tehran, but this would require US approval. Another consideration may be that while Iran's nuclear energy market might not be as promising as Saudi Arabia's, the wider Iranian market could prove to be an important and enticing one for Seoul decision-makers.

Who gains?

Should Seoul strategically seize this opportunity to position itself as Tehran's top nuclear business partner, before China and Russia extend their tentacles deeper into the Iranian market? For some, associating with Iran is simply too taboo. But for anyone whose top priority is to ensure high standards in nuclear safety, nuclear

security, and nonproliferation, the answer may be "yes." This is because South Korea, more than its two most likely competitors, is recognized for its secure procurement channels, for observing strict requirements in the sale of nuclear technology and material, and for safely constructing, operating, and eventually decommissioning reactors.

If Seoul or any trusted nuclear exporter is deemed the supplier of choice, it will be in everyone's interest—and would calm certain anxieties—for Iran to adopt the highest nuclear safety and security standards. Iran has a long way to go in terms of nuclear safety and security, and working with the world's best experts would be a step in the right direction. This presents an opportunity to provide educational programs and assistance in these areas. South Korea's quality manufacturing skills and good track record in construction, operation, and maintenance could promote nuclear safety, security, and nonproliferation. Although the United States is unlikely to enter into a civil nuclear cooperation agreement with Tehran anytime soon, it can indirectly influence Iran through South Korea should plans for cooperation between the two go forward. South Korean efforts to prevent global nuclear terrorism could also open avenues to establish an effective nuclear security culture in Iran.

The United States will view the Iranian nuclear program through the prism of compliance with the JCPOA for the foreseeable future. But while Iran tries to comply, it will also seek to expand its nuclear program. To ensure that the JCPOA is implemented and sustained, it is critical to accommodate both sets of interests. To that end, Iran's future nuclear partners must bewilling and able to maintain high nuclear nonproliferation, safety, and security standards. The US will have to consider whether raising objections to nuclear cooperation with a reliable and responsible provider like South Korea will push Tehran toward less desirable partners. If Tehran does turn to a less trustworthy source, it might help achieve Iranian objectives, but it would not be optimal for the United States or the rest of the global community, which has an interest in sustaining the JCPOA and securing compliance from Tehran in the future.

The JCPOA presents a broad window of opportunity. It affords the international community a chance to monitor and control the way the Iranian nuclear program develops for 10 to 15 years. What happens during this time period will determine whether Tehran continues to comply with its international obligations afterwards. If the nuclear deal is implemented properly, Tehran will be much less likely to go back to its previous history of nuclear noncompliance. If the stakeholders miss this chance, all the advantages that stem from the nuclear agreement will be lost. This is why it is worth further studying whether South Korea-Iran civil nuclear cooperation is a step in the right direction for the two countries and global security at large.

Duyeon Kim *is a visiting senior fellow at the Korean Peninsula Future Forum, an independent think tank run by former South Korean National Security Advisor Chun Yung-woo. Her policy research focuses on nuclear, security, and geopolitical issues on the Korean Peninsula and in Northeast Asia. Kim was an associate in the nuclear policy and Asia programs at the Carnegie Endowment for International Peace, and a senior fellow and deputy director of nuclear nonproliferation at the Center for Arms Control and Non-Proliferation in Washington. Her work has appeared in outlets including the New York Times, World Politics Review, the Washington Post, the BBC, and CBS. She was formerly a correspondent based in Seoul for South Korea's Arirang TV, covering the country's Foreign Ministry and Unification Ministry.*

Ariane Tabatabai *is a visiting assistant professor in the Security Studies Program at the Georgetown University School of Foreign Service, and a former associate in the Belfer Center's International Security Program and Project on Managing the Atom at Harvard University. Previously, she was a nonresident research associate with the James Martin Center for Nonproliferation Studies. She was a Stanton Nuclear Security Fellow at the Belfer Center in 2013 and 2014, and received her PhD in War Studies from the Department of War Studies, King's College London in 2015. Her work has appeared in the Financial Times, the Boston Globe, the National Interest, Haaretz, and Al-Monitor, among*

other publications. She is a frequent media commentator on nuclear issues in English, French, and Persian, on such outlets as NPR, the BBC, Al-Jazeera, and France24.

Nuclear emergencies and the masters of improvisation

By Sonja Schmid

Source: http://thebulletin.org/chernobyl-fukushima-and-preparedness-next-one

April 26 marks the 30th anniversary of the Chernobyl disaster, and those old enough to remember the event can recall the explosion, the evacuation, and the dread. But they rarely remember an immense milestone in the *response* to the disaster: the completion in November 1986 of a concrete encasement of Chernobyl's reactor number four. Workers drawn from all across the Soviet Union built this "sarcophagus" under extreme radiological conditions, on the ruins of the destroyed reactor. They used unimaginable amounts of concrete—and a great deal of imagination. This concrete mausoleum has held up, with some assistance, for 30 years now. (A larger containment structure that will fit over the existing sarcophagus is now being built.)

Over the years, as the ranks of those who *responded* to Chernobyl have thinned, new generations of nuclear professionals have been trained to *prevent* another disaster. Their training has emphasized "safety culture." This, along with "inherently safe designs," was going to guarantee an accident-free nuclear future. For a while, it seemed as if the world was on the verge of forgetting forever what responding to a nuclear emergency really required. Then, in March 2011, multiple reactors at one of the world's largest nuclear power plants melted down as a consequence of a massive earthquake, a tsunami, and a sustained power outage.

As a student of the Soviet nuclear power program and the Chernobyl disaster, it was painful for me to watch the blame game that played out immediately after Fukushima. Almost to the letter, the Chernobyl "script" was followed. First, the plant's operators were blamed. Then the reactor design was at fault. Finally, it was the turn of the national nuclear regulatory structure. "Culture," of course, received a great deal of blame as well.

But while Chernobyl could ultimately be dismissed as a Soviet-made disaster that "could never happen here"—wherever "here" happened to be—Fukushima has not allowed such steadfast denial. Indeed, Fukushima has proved the death knell for a nuclear safety philosophy that focused exclusively on *preventing* accidents. Disaster preparedness and response were given scant attention in the years between Chernobyl and Fukushima, but now they have been added to the vocabulary of the world's nuclear industries. Curiously, however, this shift is only partial. Disaster prevention retains the greatest emphasis; preparedness is sometimes treated adequately; but resources (and imagination) devoted to actual *response* strategies remain limited.

The "lessons learned" from Fukushima—and new reports on these lessons continue to be published—focus predominantly on technical and legal fixes, organizational reform, and liability concerns. In the United States, the Nuclear Regulatory Commission responded to Fukushima by overhauling its rules and guidelines for accident prevention, preparedness, and response. **The US nuclear industry, meanwhile, implemented "FLEX," a program designed to provide nuclear reactors in distress with hardware such as extra pumps and generators, both on site and stored at regional centers.** In Europe, power reactors were subjected to "stress tests" after Fukushima, and these tests sparked conversation among nations hosting nuclear power reactors about harmonizing, if only loosely, national regulations concerning natural (and other) hazards to nuclear power plants.

Steps such as these go in the right direction. But emphasizing prevention and preparedness over response ignores a simple fact: Nuclear disasters tend to exceed people's worst expectations. There is a good reason that the nuclear industry refers to disasters as "beyond design-basis accidents"—only a limited number of scenarios can be anticipated and prepared for. Disasters, therefore, require the development of creative, skill-based, and team-based response strategies (along with strenuous efforts to avoid disasters entirely).

Training for emergency responders in general tends to emphasize flexibility and imagination, with a premium placed on performing quick assessments and triage in unprecedented situations. But in nuclear emergency response training, the situation is different. The nuclear industry seems deeply troubled by using human imagination to address situations that go "beyond the checklist." In Europe and the United States, at least—I can't speak for the entire world—the nuclear industry seems hung up on the idea of control. There is a plan for every conceivable situation. Should plans fail, there are more plans. Staff are trained to follow procedures and execute instructions. If they don't, that's always bad.

Such an approach, as documented by the anthropologist Constance Perin, fundamentally fails to acknowledge the messiness of operating imperfect, real-world technologies (and *all* technologies are imperfect). Worse yet, it incapacitates an aspect of creativity that, though it's more often associated with jazz, can be tremendously important in nuclear emergencies: improvisation. In music, improvisation calls to mind wild, random, and perhaps solitary acts. But if emphasized in training for nuclear emergencies, the metaphor of improvisation can help prepare responders to pursue skill-based, team-oriented, and highly organized actions under challenging conditions.

In any disaster, improvisation occurs. It happened at Chernobyl, even if creative imagination was thoroughly expunged from all written reports. Improvisation happened at Fukushima, and in fact a lot more improvisation will be necessary if the Fukushima disaster is ever to "end." It is tempting to remember creative action only when it fails. Making this mistake locks in a mindset of control and controllability. Any such mindset will be exploded—yet again—by the next nuclear emergency.

***Sonja Schmid** is an associate professor in Science and Technology Studies at Virginia Tech. Her expertise is in the history of technology, science and technology policy, and social studies of risk. Fluent in Russian, she investigates the history and organization of nuclear industries in the former Soviet Union and Eastern Europe and studies the way national energy policies, technological choices, and nonproliferation concerns shape each other. In a current project funded by a National Science Foundation CAREER Award, she is investigating the challenges of globalizing nuclear emergency response. She is the author of* Producing Power: The Pre-Chernobyl History of the Soviet Nuclear Industry.

Delivering the nuclear promise: TVA's sale of the Bellefonte nuclear power plant site

By Peter A. Bradford

Source: http://thebulletin.org/delivering-nuclear-promise-tvas-sale-bellefonte-nuclear-power-plant-site9524

Even as Energy Secretary Ernest Moniz convened a "summit" to discuss more governmental assistance to the nation's

troubled nuclear power plants, the recent announcement by the Tennessee Valley Authority (TVA) that it is selling its northern Alabama site containing the unbuilt Bellefonte reactors should have sobered the summiteers. Even if the site's appraised value of $36 million is realized, TVA customers will get back less than a 2016 penny for each of the $6 billion they have spent on the site over 46 years.

Two nuclear reactors were ordered for Bellefonte in 1970. When construction commenced in 1974, the TVA had almost no experience in actually operating a nuclear unit, but the TVA program had 16 reactors under construction in addition to one that had operated for a few months. All were at least four times larger than the largest plant that had operated for any length of time anywhere in the United States. All were intended to be completed in the

1970s. They were the TVA's initial share of the Atomic Energy Commission's 1972 forecast of 1000 reactors needed by the year 2000, plus reprocessing plants to supply the many breeders among the 1000 reactors. As it turns out, with Watts Bar 2 coming on line this year, seven TVA reactors will have been completed. The other ten—plus two announced in 2007—are cancelled, with at least $10 billion in customers' money spent on them in addition to some sweeteners from US taxpayers.

Bellefonte has a prominent place in this waxworks of miscalculation and waste. The two original Bellefonte reactors were the last ordered from Babcock & Wilcox, the designers of the plant that melted half its core at Three Mile Island (TMI) in 1979. They therefore received special scrutiny following the TMI accident. Even before TMI though, all of the TVA units under construction had been greatly delayed. By 1984 eight units—ranging from 44 percent to 3 percent complete—were canceled. Construction of the four reactors at Bellefonte and Watts Bar continued, albeit at a pace slowed greatly by construction problems, inflation, the accident at TMI, falling demand, falling fossil fuel costs and rising reactor costs. In 1988, the TVA decided to mothball the Bellefonte reactors as well as Watts Bar 2. Bellefonte Unit 1 was said to be 88 percent complete while Unit 2 was 58 percent done. Construction resumed in 1993 with completion eventually set for 2011 and 2014 respectively. By 2006, when construction was halted again and the Nuclear Regulatory Commission's (NRC) construction permits were terminated, these completion percentages had been revised to 55 and 35.

Two years later, in 2008, at the height of nuclear renaissance fervor, the TVA reconsidered and persuaded the NRC to reinstate the permits. Completion of the two units—said as always to be vital to meet rising demand and maintain the economic health of the Tennessee Valley—was then projected for 2017 and 2021. Unit 2 was canceled for the third and apparently final time in 2009.

In 2011, the TVA announced the selection of the French vendor Areva to complete the bulk of the nuclear portion of Unit 1. By 2013, with Areva in grave financial straits requiring a bailout from the French government, the then-TVA chair announced a search for a private developer to finish Unit 1. By 2015, however: the TVA resource plan showed no need for baseload capacity beyond what could be supplied by Watts Bar 2 for at least 20 years. Hence the decision to terminate Unit 1 and sell the site.

Meanwhile, renaissance fervor had swept over Bellefonte in another form. In 2002, the Bush Administration announced its Nuclear 2010 program, designed to produce at least two new plants by 2010 and to demonstrate that the new licensing process and advanced designs would bring an end to the cost overruns and delays that had plagued US nuclear power since the mid-1970s. Nuclear 2010 included a commitment to have taxpayers pay half of the engineering and application costs of the new reactors. Congress passed a 2005 subsidy package containing everything the industry was then asking for.

In 2007 NuStart Energy Development, a consortium of utilities and reactor vendors, announced the selection of Bellefonte as the site of the reference plant for the flock of Westinghouse reactors that would follow. NuStart's October 2007 NRC application for Units 3 and 4 was the start of the two-year-long US renaissance stampede in which applications for 31 new reactors were filed at the NRC. But as Bellefonte 3

and 4 fell behind the pace of construction at the Southern Company's Vogtle project in Georgia, NuStart transferred the reference reactor designation and the accompanying subsidies to the Vogtle units, which are now at least three years behind schedule and $3.5 billion above the original estimates.

Bellefonte 3 and 4 were canceled in 2011 in favor of completing Watts Bar 2 and Bellefonte 1. NuStart was disbanded in 2012. Nearly all of the 31 renaissance reactors have been canceled. Four are under construction.

The TVA reunited with Babcock & Wilcox to pursue yet another new nuclear idea in a 2011 letter of intent with Generation mPower, a joint venture of B&W and Bechtel, to build six small modular reactors at Clinch River, the site of TVA's multibillion dollar failed effort to build a breeder reactor opposed by President Carter and terminated as unnecessary and wasteful by Congress in 1983. The Clinch River breeder's cost estimate rose from $500 million in 1972 to $4 billion ten years later. Because the industry consortium declined to raise its contribution above its 1972 commitment of $250 million, US taxpayers were exposed to the entire overrun.

The Energy Department awarded Generation mPower $79 million toward completion of its small modular reactor design. In 2014 Babcock & Wilcox announced that it had lost interest in proceeding with the project on anything like the original schedule due to a lack of investors or customers.

Continuing its expensive half-century role as the leading enabler of Washington's nuclear innovation pork barrel, the TVA has applied for an early site permit (but not a construction license) for up to 800 megawatts worth of small modular reactors at Clinch River. At his May 19 nuclear "summit," Energy Secretary Moniz pledged his department's continuing support—meaning that US taxpayers will pick up a substantial share of the TVA small modular reactors' permitting costs. Congress is seeking to add additional support.

At the same "summit" many in the nuclear industry complained that renewable energy enjoys disproportionate federal support and dysfunctional markets. Secretary Moniz promised that his fellow longtime MIT nuclear cavalryman John Deutch would soon produce a report on how best to "incentivize continued operation" of endangered reactors because they are essential to low carbon electric reliability. The role will be familiar to Deutch, a Carter Administration Undersecretary of Energy who has presided over his share of meetings at which dozens of subsequently canceled reactors were wrongly forecast to be essential to freeing the electric sector from oil dependence, to keeping the nation's lights on and to lowering electric rates.

Closing reactors abruptly with no measures in place to assure that their replacements will be within acceptable CO2 limits is indeed no way to protect against climate change, but Secretary Moniz isn't holding summits to figure out the best ways to choose among available electric resources. Instead he has aligned himself with the political pulltoys whom the forlornly named industry front "Nuclear Matters" parades through state capitals—demanding fresh nuclear support and determined to avoid competing head-to-head with other low-carbon alternatives for that support.

While these road shows roll on, actual experience suggests the wisdom of a more competitive path. Other power supply options are rapidly falling in cost, and large scale power storage projects are underway in many states.. Even new combinations of existing resources are proving competitive in low carbon contexts. In New York State, competition from a transmission alternative dramatically cut the need to support the Ginna nuclear power plant near Rochester. Another transmission expansion proposes to use the site of the closing Pilgrim reactor in Massachusetts to import more low carbon electricity than Pilgrim generates. In Nebraska, the board of the Omaha Public Power District announced that it would replace the Fort Calhoun reactor at substantially lower cost through demand reductions and wind energy.

Doug Koplow, whose Earth Track website has for years been the best source of energy subsidy analysis, has chronicled and classified the subsidies received by nuclear power, an amount that far exceeds the totals made available to renewable energy: "Since its inception more than 50 years ago, the nuclear power industry has benefited—and continues to benefit—from a vast array of preferential government subsidies….Subsidies to the nuclear fuel cycle have often exceeded the value of the power produced". Koplow's subsidies do not count most of the costs of the nation's 120-plus canceled nuclear plants, or the cost

overruns at the operating reactors.

The power market operators are themselves concerned that the ongoing efforts of nuclear plant operators to obtain special support will undermine the efficiency of the markets. The most outspoken expression of this concern comes from the PJM ISO—one of the largest wholesale electricity markets in the world. In a recent study, it bluntly concluded:

The PJM markets show no signs of inadequately compensating legacy units and forcing a premature retirement of economically viable generators….the simple fact that a generating facility cannot earn sufficient market revenue to cover its going-forward costs does not reasonably lead to the conclusion that wholesale markets are flawed. More likely, it demonstrates that the generating facility is uneconomic.

PJM vice-president Craig Glazer was even blunter. According to *Nucleonics Week*, he admonished the Moniz "summit" that "the regional transmission organization's policies are intended to reward performance, not just nuclear plant performance.' If the question is 'just save nuclear,' that's a different policy goal than to increase the efficiency and reliability of the entire electricity system."

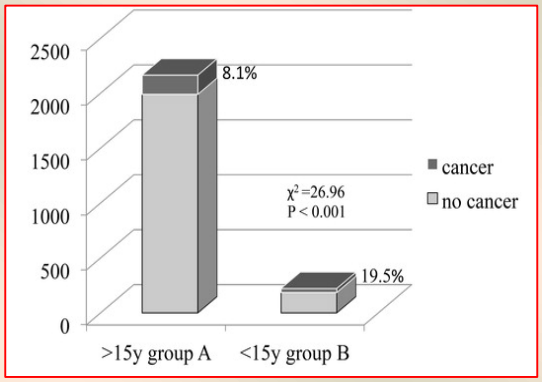
The Nuclear Energy Institute's chief executive officer, Marvin Fertel is flexing his substantial political muscle to deal with market operator skepticism toward nuclear bailouts. Fertel rode into office on the nuclear energy renaissance. Riding out on a wave of reactor closures, he expressed to the summiteers his industry's exasperation with the dawdling and dysfunctionality of its would-be rescuers. He called on Congress to "exercise its oversight responsibilities on FERC [the Federal Energy Regulatory Commission]" to "enforce some semblance of discipline," said the May 26 edition of *Nucleonics Week*. Foreseeing the closure of another dozen or so reactors, with their attendant job losses, community impoverishment, and carbon increases, Fertel took slight consolation from the forthcoming Deutch report: "We know you like nuclear, but all we hear about is renewables…..A report doesn't do anything unless the RTOs [regional transmission organizations] and FERC do something with it. So you need to get it to them, they need to do something about it, and they need to do it sooner rather than later," he said.

One cannot open the trade press without seeing Fertel's blandishments echoed and amplified by industry leaders, by their allies, and by journalists unfamiliar with nuclear history. But how much should these plaints and prophesies weigh beside the For Sale sign on the Bellefonte lawn?

***Peter A. Bradford** is an adjunct professor at Vermont Law School, where he has taught "Nuclear Power and Public Policy." From 1977 to 1982, he served on the US Nuclear Regulatory Commission, and he has chaired the utility regulatory commissions in Maine and New York. He advises and testifies on utility regulation and nuclear issues in the United States and elsewhere. He is vice chair of the board of the Union of Concerned Scientists.*

Number of thyroid cancers in Belgian children rises post-Chernobyl

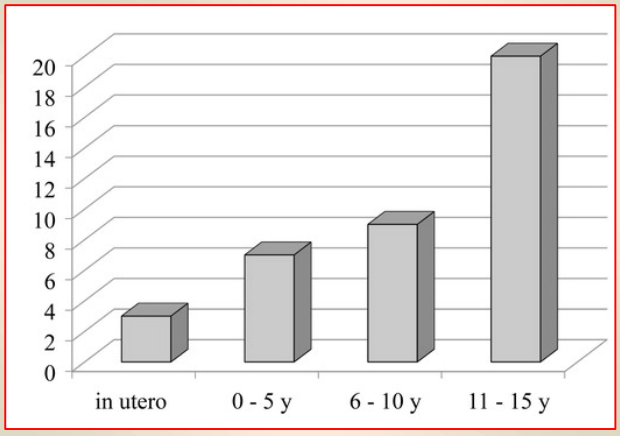
Source: http://www.homelandsecuritynewswire.com/dr20160608-number-of-thyroid-cancers-in-belgian-children-rises-postchernobyl



June 08 – Exposure in Belgium to radioactive fallout from the April 1986 Chernobyl nuclear accident may have increased the incidence of thyroid cancer in those exposed as children, according to new research published in the journal *Acta Chirurgica Belgica.*

About 2349 thyroidectomies: 175 PTC (8.1%) in patients aged >15 years (*group A*) and 36 (19.5%) in patients aged <15 years (*group B*) at the time of Chernobyl.

Thyroid cancer is usually rare among children, with less than one new case per million diagnosed each year. Taylor & Francis notes, however, that after the Chernobyl accident a striking increase in the disease was reported in children and teenagers in the most contaminated areas of Belarus and Ukraine.



Now, this new research from Belgium suggests countries further afield were also affected.

Age of the 36 youngsters at the time of the Chernobyl accident (plus three in utero) who developed PTC 8–27 years later.

Prior to April 1986, surgeons at Mont-Godinne University Hospital, Yvoir, Belgium had seen no cases of thyroid cancer in children. But in 1995, surgeon Luc Michel and colleagues treated four cases of papillary thyroid cancer in patients who were younger than 9 years old at the time of Chernobyl and operated on a further five patients between 2000 and 2002 aged under 12 at the time of the accident.

To examine whether this disturbing trend could be due to exposure to radioactive fallout from Chernobyl, the surgical team collected information on the number of new cases of papillary thyroid cancer in all patients born before April 1986 who were operated on at the hospital for any type of thyroid lesion between April 1986 and April 2015. They also obtained data from a classified Belgian Royal Institute of Meteorology (BRIM) report which revealed that in early May 1986 the average level of atmospheric radioactivity in Belgium rose to twenty times higher than normal, from 3.2 Bq.m-3 to over 70 Bq.m-3 .

36 new cases (19.5 percent) of papillary thyroid cancer were found among 185 Belgian children aged under 15 at the time of the accident, compared with just 175 cases (8.1 percent) in 2164 patients aged older than 15 years.

Numerous studies have shown that exposure to certain types of radiation increase the incidence of thyroid cancer in children and adolescents. The authors conclude that it is likely that radiation exposure from Chernobyl has affected residents of countries much further afield than Belarus and Ukraine including Belgium, potentially increasing the incidence of thyroid cancer in those exposed as children over the last 30 years. However, they caution that it is not clear whether these cases reflect an increased incidence in the Belgian population as a whole.

— Read more in Luc A. Michel et al., "Post-Chernobyl incidence of papillary thyroid cancer among Belgian children less than 15 years of age in April 1986: a 30-year surgical experience," Acta Chirurgica Belgica (20 April 2016).

Poor U.S.-Russia relations increase risk of dirty bomb in Europe - experts

Source: http://uk.reuters.com/article/uk-islamic-state-nuclear-idUKKCN0YT1PU

June 07 – **Tension between Russia and the West may be distracting them from cooperating to prevent an accidental nuclear confrontation or a dirty bomb attack by militants,** nuclear policy experts said on Tuesday.

Former U.S. Secretary of Defence William Perry said he regretted the current lack of communication between the United States and Russia, which went into a deep freeze after Russia's 2014 annexation of Crimea.

"We are about to recreate the conditions that nearly brought us to the brink of nuclear war" during the Cold War, Perry said.

Anatoly Adamishin, a former Russian Deputy Foreign Minister, argued that the U.S. has focused on a policy of "strangling Russia" and hoping for the departure

of Russian President Vladimir Putin, which has the effect of putting Russia at the forefront of a list of U.S. enemies.

"The U.S. simply has to rethink its own policy: what should be in focus is nuclear reductions," he said. "Russia and the U.S. are not inherent enemies."

They made their comments at a conference organised by the the Luxembourg Forum on Preventing Nuclear Catastrophe.

The forum's head, Moshe Kantor, said the threat of a 'dirty bomb' attack on a European city was at its highest level since the end of the Cold War.

Security experts have raised concerns since the attacks in Paris and Brussels by Islamist militants that poorly guarded European nuclear facilities pose a risk.

Kantor cited chemical weapons attacks carried out by Islamic State in Iraq, their stated desire to carry out more attacks in Europe, and evidence militants linked to the attacks in Paris had also been studying a Belgian nuclear power plant.

"This, combined with poor levels of security at a host of nuclear research centres in the former Soviet Union mean the threat of a possible 'dirty-bomb' attack on a Western capital is high," Kantor said.

He urged the United States and Russia, both nuclear powers, to cooperate on using their technological resources to monitor the illegal transportation of radioactive materials.

Gorbachev, appearing by satellite link, said he was alarmed by the increasing readiness of many nations to use military force to resolve conflict rather than negotiation.

"I note that these have not solved the problems, but they have served to undermine international law and weaken international relations," he said.

White House: Uranium discovered by IAEA likely tied to Iran's nuclear weapons program

Source: http://www.homelandsecuritynewswire.com/dr20160621-white-house-uranium-discovered-by-iaea-likely-tied-to-iran-s-nuclear-weapons-program

June 21 – Obama administration officials concluded that particles of uranium found at Iran's Parchin military base and revealed in the International Atomic Energy Agency's final report on the

country's past nuclear activities were likely tied to the regime's nuclear weapons program, the *Wall Street Journal* reported Sunday. The admission further underscores concerns that the IAEA's investigation into Iran's nuclear activities at Parchin should not have been closed following the report's publication.

"The man-made uranium found at **Parchin** (photo), which has only low-levels of fissionable isotopes, can be used as a substitute for weapons-grade materials in developing atomic bombs, according to nuclear experts," the *Journal* noted. "It can also be used as component in a neutron initiator, a triggering device for a nuclear weapon."

"The existence of two particles of uranium there would be consistent with our understanding of the involvement of Parchin in a past weapons program, but by themselves don't definitively prove anything," a senior Obama administration official told the paper.

"The assumption in the [U.S.] government is that these were nuclear weapons-related experiments," explained Robert Einhorn, a former Obama administration nuclear negotiator. "The evidence is, technically, inconclusive. But the administration believes it has other information that confirms there was weapons-related activity there."

Other explanations for the presence of the uranium — including that one of the inspectors may have inadvertently brought it in or that it came from depleted uranium, which is used in some conventional weapons — were considered "plausible but unlikely." Iran's explanation that the uranium was linked to the storage of chemicals used for the development of conventional weapons was not supported by either aerial photography or testing.

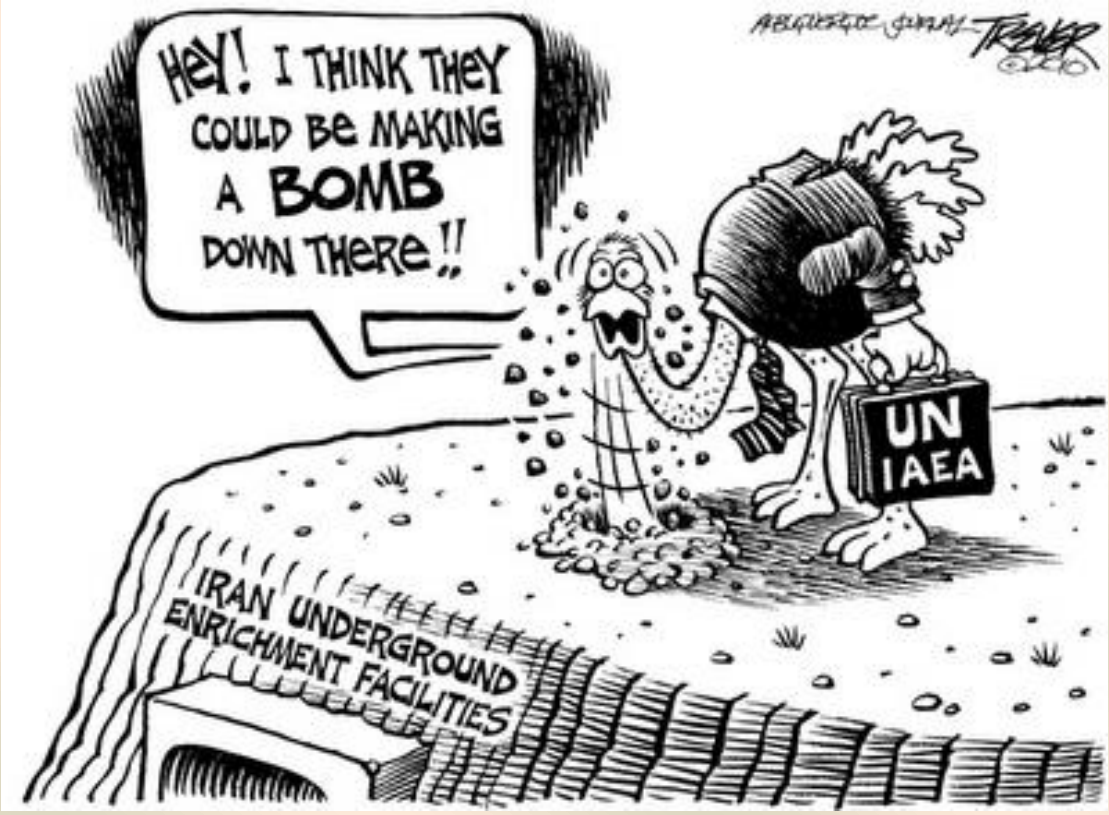
Critics of the nuclear deal with Iran have asserted that the uranium found at Parchin showed that the "Obama administration didn't go far enough in demanding Iran answer all questions concerning its past nuclear work before lifting international sanctions in January," the *Journal* wrote. They also questioned whether the IAEA can effectively monitor Iran without fully understanding the country's past nuclear work.

Independent experts argued when the IAEA report was released last December that the agency should not close its investigation of Iran's past nuclear work in light of the discovery of uranium particles at Parchin. The report also found that Iran was developing a nuclear weapon until 2009, contradicting U.S. estimates that Iran halted its efforts to develop a nuclear bomb by 2003.

Olli Heinonen, the former deputy director general of the IAEA, wrote shortly after the report was released that the IAEA required more complete information from Iran, or in the future "effective verification [of Iran's nuclear program] will be compromised." David Albright, a former weapons inspector and currently president of the Institute for Science and International Security, argued at the time that the presence of the

uranium particles meant that "the Parchin file can in no way be considered closed. It should remain open and the IAEA should continue its investigation into the activities that took place at the site. It is time that Iran starts to admit what really happened at Parchin."

Determining what research Iran carried out at Parchin is complicated by a controversial provision in the nuclear deal that allowed Iran to self-inspect the facility. Iran has also carried out significant construction at the facility, compromising evidence of past work there.



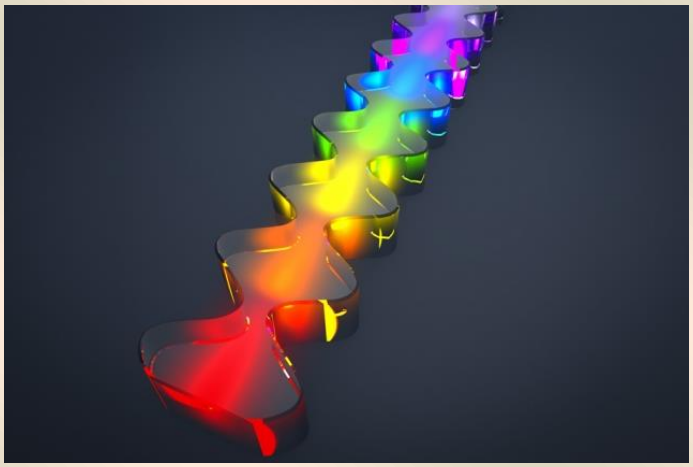
Speedy terahertz-based system could detect explosives

Source: http://www.homelandsecuritynewswire.com/dr20160524-speedy-terahertzbased-system-could-detect-explosives

May 24 – **Terahertz spectroscopy, which uses the band of electromagnetic radiation between microwaves and infrared light, is a promising security technology because it can extract the spectroscopic "fingerprints" of a wide range of materials, including chemicals used in explosives.**

But traditional terahertz spectroscopy requires a radiation source that is heavy and about the size of a large suitcase, and it takes 15 to 30 minutes to analyze a single sample, rendering it impractical for most applications.

In the latest issue of the journal *Optica*, researchers from MIT's Research Laboratory of Electronics and their colleagues present **a new terahertz spectroscopy system that uses a quantum cascade laser, a source of terahertz radiation that's the size of a computer chip. The system can extract a material's spectroscopic signature in just 100 microseconds.**



An artist's embellishment of an image of the "gain medium" used to produce terahertz frequency combs. The different colors indicate that different wavelengths of oscillating terahertz radiation travel different distances through the medium, which has a different refractive index for each of them.

The device is so efficient because it emits terahertz radiation in what is known as a "frequency comb," meaning a range of frequencies that are perfectly evenly spaced.

"With this work, we answer the question, 'What is the real application of quantum-cascade laser frequency combs?'" says Yang Yang, a graduate student in electrical engineering and computer science and first author on the new paper. "Terahertz is such a unique region that spectroscopy is probably the best application. And QCL-based frequency combs are a great candidate for spectroscopy."

Different materials absorb different frequencies of terahertz radiation to different degrees, giving each of them a unique terahertz-absorption profile. Traditionally, however, terahertz spectroscopy has required measuring a material's response to each frequency separately, a process that involves mechanically readjusting the spectroscopic apparatus. That's why the method has been so time consuming.

Because the frequencies in a frequency comb are evenly spaced, however, it's possible to mathematically reconstruct a material's absorption fingerprint from just a few measurements, without any mechanical adjustments.

Getting even

The trick is evening out the spacing in the comb. Quantum cascade lasers, like all electrically powered lasers, bounce electromagnetic radiation back and forth through a "gain medium" until the radiation has enough energy to escape. **They emit radiation at multiple frequencies that are determined by the length of the gain medium.**

But those frequencies are also dependent on the medium's refractive index, which describes the speed at which electromagnetic radiation passes through it. And the refractive index varies for different frequencies, so the gaps between frequencies in the comb vary, too.

To even out their lasers' frequencies, the MIT researchers and their colleagues use an oddly shaped gain medium, with regular, symmetrical indentations in its sides that alter the medium's refractive index and restore uniformity to the distribution of the emitted frequencies.

Yang; his advisor, Qing Hu, the Distinguished Professor in Electrical Engineering and Computer Science; and first author David Burghoff, who received his Ph.D. in electrical engineering and computer science from MIT in 2014 and is now a research scientist in Hu's group, reported this design in *Nature Photonics* in 2014. **But while their first prototype demonstrated the design's feasibility, it in fact emitted two frequency combs, clustered around two different central frequencies, with a gap between them, which made it less than ideal for spectroscopy.**

In the new work, Yang and Burghoff, who are joint first authors; Hu; Darren Hayton and Jian-Rong Gao of the Netherlands Institute for Space Research; and John Reno of Sandia National Laboratories developed a new gain medium that produces a single, unbroken frequency comb. **Like the previous gain medium, the new one consists of hundreds of alternating layers of gallium arsenide and aluminum gallium arsenide, with different but precisely calibrated thicknesses.**

Getting practical

As a proof of concept, the researchers used their system to measure the spectral signature of not a chemical sample but an optical device called an etalon, made from a wafer of gallium arsenide, whose spectral properties could be calculated theoretically in advance, providing a clear standard of comparison. The new system's measurements were a very good fit for the etalon's terahertz-transmission profile, suggesting that it could be useful for detecting chemicals.

Although terahertz quantum cascade lasers are of chip scale, they need to be cooled to very low temperatures, so they require refrigerated housings that can be inconveniently bulky. Hu's group continues to work on the design of increasingly high-temperature quantum cascade lasers, but in the new paper, Yang and his colleagues demonstrated that they could extract a reliable spectroscopic signature from a target using only very short bursts of terahertz radiation. That could make terahertz spectroscopy practical even at low temperatures.

"We used to consume 10 watts, but my laser turns on only 1 percent of the time, which significantly reduces the refrigeration constraints," Yang explains. "So we can use compact-sized cooling."

"This paper is a breakthrough, because these kinds of sources were not available in terahertz," says Gerard Wysocki, an assistant professor of electrical engineering at Princeton University. "Qing Hu is the first to actually present terahertz frequency combs that are semiconductor devices, all integrated, which promise very compact broadband terahertz spectrometers."

"Because they used these very inventive phase correction techniques, they have demonstrated that even with pulsed sources you can extract data that is reasonably high resolution already," Wysocki continues. "That's a technique that they are pioneering, and this is a great first step toward chemical sensing in the terahertz region."

— Read more in Yang Yang et al., "Terahertz multiheterodyne spectroscopy using laser frequency combs," Optica 3, no. 5 (2016): 499-502.

Terrorists "stockpiling explosives in Europe": EU security official

Source: http://www.homelandsecuritynewswire.com/dr20160525-terrorists-stockpiling-explosives-in-europe-eu-security-official

May 25 – **Manuel Navarrete Paniagua, the Head of the European Counter Terrorism Center at Europol, said that terrorist cells in the EU are probably stockpiling explosives for future attacks.**

Europol said it had foiled 211 terror plots in the last year, but that the threat of similar attacks on the scale of November 2015 Paris attacks and the March 2016 attacks in Brussels in March remained a concern.

Paniagua warned on Monday that "large clandestine stockpiles of explosives" are likely being set up

by terrorist groups, *EUObserver* reports.

Speaking at a briefing of Europol's EU Terrorism Situation & Trend Report, due to be released next month, Paniagua told members of the EU Parliament: "We have some information reported by the member states that terrorists groups are trying to establish large clandestine stockpiles of explosives in the European Union to be used eventually in large scale home attacks."

More than 4,000 foreign fighters have been identified in the EU and entered into a Europol database.

Paniagua said: "Using the terrorist financial tracking program, we provided last year more than 2,700 leads regarding foreign terrorist fighters to the member states."

The *EUObserver* notes that a key conclusion of the report suggests that "jihadist terrorism" remains the top threat to security in the EU, with recent attacks suggesting better coordination among terrorists than previously believed.

Paniagua said terror groups' use of explosives and firearms suggests they pose a rapidly evolving threat.

Paniagua also addressed the concern of jihadists using refugee flows to enter Europe in order to carry out attacks against Western targets.

"We found no evidence of the systematic use of this flow to infiltrate terrorists into the European Union. But they do, they use it, we have some cases, some of the people that perpetrated the Paris attacks were eventually disguised in this immigration flow," said Paniagua.

Europol said in May that it will deploy around 200 counter-extremism officers and investigators at refugee arrival centers in Europe, especially those with large numbers of arrivals such as in Italy and Greece.

Iaq – ISIS suicide vehicle (VBIED)

MoI release photos of suicide bomber, VBIED seized near the ministry compound

Source: http://www.khaama.com/moi-release-photos-of-suicide-bomber-vbied-seized-near-the-ministry-compound-0973

May 17 – The Afghani Ministry of Interior (MoI) released the photos of the would-be suicide bomber and the Vehicle-borne Improvised Explosive Device which the bomber wanted to use in targeting the Ministry of Interior compound.

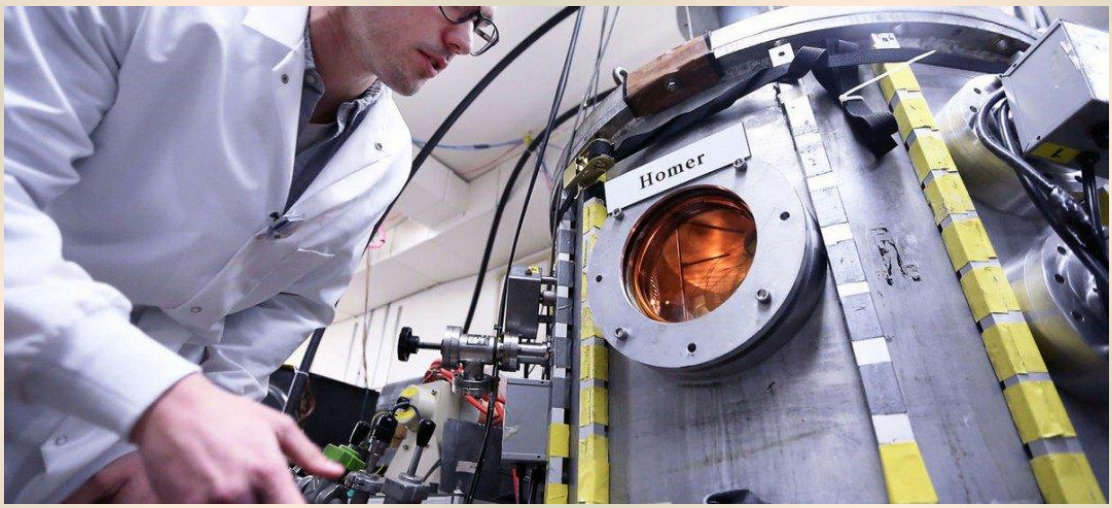
According to MoI, the suicide bomber was arrested from Jamhuriat Hospital road located which goes towards the Ministry of Interior compound.

The photos show the would-be suicide bomber with bruises on his face and blood stains covered his clothes as the security forces are taking him away from the site where he was arrested.
Other photographs show large amount of explosives recovered from the hatchback vehicle which was in custody of the suicide bomber as he was attempting to target the ministry.

Earlier, reports emerged that the suicide bomber managed to breach a number of the security posts located on the road towards the ministry compound.
Meanwhile, the Taliban group rejected that the group's suicide bomber was arrested by the security forces in Kabul today.
The latest attack attempt by the militant groups comes almost a month after a deadly attack rocked capital Kabul which left at least 64 people dead and 347 others wounded.
The Afghan national security forces managed to thwart at least five major attacks in capital Kabul plotted by the notorious Haqqani terrorist network during the past one month.
Meanwhile, the Resolute Support mission in a statement said Monday that a major rocket attack plot on Kabul city was foiled as the Afghan security personnel seized three 122 mm rockets before the militants manage to fire them on the city.
"Resolute Support Mission-trained Ministry of Interior #MOI Major Crimes Task Force (MCTF) Corruption Investigation Unit personnel thwarted a major rocket attack on Kabul on Friday, May 13," a statement by the alliance said.

Drones Can Now Sniff Out Bombs

Source: http://i-hls.com/2016/05/drones-can-now-sniff-out-bombs/



May 25 – Researchers at the University of Wisconsin-Madison have brought out a new tool in the fight against terrorism: **bomb sniffing drones**. The team took existing technology used to detect drugs and chemical and nuclear weapons and minituarised it so can be fitted on drones.
The technology should be familiar to all but the most casual observer. You see it in many airports at security checkpoint to scan luggage. In essence, arrays of sensors look for particle traces and gamma rays that reveal the presence of bomb making materials. What's new here is that now this technology is mobile.
Uses and applications for this could be far ranging, from detecting roadside bombs in combat zones in countries like Iraq and Syria to ensuring Iran complies with its

commitment to not manufacture nuclear weapons. It could also be used domestically, to quickly respond to bomb and terror threats.
But the technology's uses are not limited to the homeland security and defence fields. It could be used to map deposits of valuable minerals or help rescue survivors of natural disasters such as earthquakes.
"From what I've read, its applications are only limited by the imagination of the user," said John Weidner of the the US Department of Energy's National Nuclear Security Administration. "I think this can be a tremendous tool."
The technology should hit the market in a year or two, and it has already generated a lot of interest. Japan is reportedly looking to buy this technology to secure the 2020 Summer Olympic Games in Tokyo.

T.S.A. Trains Dogs to Stay One Sniff Ahead of Bomb Makers

Source: http://www.nytimes.com/2016/06/01/us/tsa-trains-dogs-to-stay-one-sniff-ahead-of-bomb-makers.html

May 31 – Just after dawn on a recent May morning, Ajax, a 2-year-old black Labrador retriever, eagerly worked his way through a sparsely furnished room sniffing for explosives. On his third try, he picked up a scent behind a piece of furniture near the front of the room.
"Good dog, good dog," said Andrew Baxter, his trainer, who reached into a pouch and threw Ajax a squeaky toy, much to the dog's delight.
Ajax is one of 230 dogs at the Transportation Security Administration's facility here on Lackland Air Force Base training to become bomb-sniffing canines. Dogs that pass the course will be deployed to the nation's airports, a first line of defense against terrorist bomb attacks.
The assignment is becoming increasingly difficult as terrorists adopt techniques using household chemicals to construct bombs that make it hard even for a dog's sensitive nose to discern.
"So we're now asking dogs not just to find a needle in a haystack — now we're also saying to the dog, 'We need you to find any sharp object in the haystack,'" said Clive Wynne, a professor at Arizona State University. He is leading a study funded by the Office of Naval Research to develop methods to train dogs to identify a wide variety of common ingredients that could be used to make bombs.

A Transportation Security Administration agent, Jason Berlfein, rewarded Hector, a chocolate Labrador, for detecting explosives at the training center. Credit Ilana Panich-Linsman for The New York Times

Since the Sept. 11, 2001, terrorist attacks, the federal government has spent billions on technologies to emulate the nose and brain of a trained bomb dog, which can detect minute traces of explosives. And while researchers have made progress, when it comes to accuracy, nothing quite beats the nose of a dog.
"Dogs can detect a teaspoon of chemical in a million gallons of water — nearly enough to fill two Olympic-size swimming pools," said Craig Angle, a professor in Auburn University's Canine Performance Sciences program. "They perform at a really high level. They're like the Peyton Mannings or Brett Favres of canines."
But the increase in explosive devices using common household chemicals has put that ability to the test, particularly in detection of the compound TATP, a favorite of terrorist groups.
Ibrahim Hassan al-Asiri, the Saudi who designed the device used by the so-called underwear bomber on a 2009 flight to Detroit, is believed to be at the forefront of these new terrorist bomb makers. Intelligence officials say Mr. Asiri built sophisticated devices by

using new types of explosives that intelligence officials had not seen previously and enclosed them in caulk to prevent leakage of the vapors that dogs could detect.

Mr. Wynne and other researchers are teaching dogs not only how to detect explosive ingredients but also to determine if what they smell could combine to form an explosive mixture. In other words, the dogs are being asked to identify a bomb before it becomes a bomb.

"There are more than 240 different types of smokeless powders alone," said Danny Diller, the training supervisor at the canine training center here at Lackland. "We can't train them on all explosives."

John Maccarone training Ali, a German shorthair pointer, at an airport mock-up at Lackland Air Force Base in San Antonio in May. Credit Ilana Panich-Linsman for The New York Times

And, he said, the agency is adjusting its training in response to events like the London subway bombings in 2005 and the attempt by Umar Farouk Abdulmutallab, the underwear bomber, to bring down an airliner, which led to training dogs for mass transit, and passenger screenings.

"We are hoping through all the variety, they will be able to generalize across the spectrum," Mr. Diller said.

The Department of Homeland Security, the parent agency of the T.S.A., has expanded its use of dogs to help screen passengers in airport security lines. Jeh Johnson, the secretary of Homeland Security, recently announced the deployment of bomb-sniffing dogs to larger airports where long security lines had not only increased the wait but provided a vulnerable target for an attack like the one in March at Brussels Airport.

Almost all of the dogs at Lackland, purchased mainly in Eastern Europe through a Defense Department program, arrived when they were a year to a year and a half old. The best breeds for training to find bombs, according to the T.S.A., are Belgian Malinoises, Labrador retrievers and German shorthair pointers.

Dogs like Ajax are trained to detect explosives in a variety of environments. Some dogs undergo 15 weeks of training to sniff out explosives, while others train for 25 weeks specifically to detect chemicals among passengers. Seventeen warehouses here contain mock airport settings, including cargo bays and even a room with a replica of the interior of a 747 aircraft. Dogs are also trained to operate on trains and aircraft.

T.S.A. trainers began the dogs' instruction by teaching them to recognize the scent of various chemicals that are commonly used in explosives such as TNT, C4, commercial dynamite and Semtex. The exact chemical combinations that the T.S.A. dogs can detect are closely guarded.

Buster, a black Labrador, sat to indicate to his handler that he had detected explosives. Credit Ilana Panich-Linsman for The New York Times

Once the dogs learn to recognize the odors, they are given a toy as a

reward. They are then put through a variety of training settings, like detecting explosives in a sparsely furnished room and finding odors in an area set up to look like a crowded airport boarding area.
"We keep throwing different situations at them until it doesn't matter," said Jerry Wilson, a training instructor at the center. "We want them to be comfortable in any environment."
Despite the intense training, the instructors here say that instances in which dogs find an actual bomb are rare. But they are not worried. The dogs are doing exactly what they are supposed to do. More important, the instructors say, a major part of a bomb-sniffing dog's mission is deterrence.
"But we still need to do constant training and practicing for that one time that they are needed," said Robert Gravel, a training instructor.
It is an expensive proposition. The T.S.A. has invested heavily in its canine detection program, recently building a new $12 million training center here that employs about 93 people. The center also trains dogs and handlers for state and local law enforcement agencies.

More than 900 canine teams are deployed across the country, at a cost last year of about $121.7 million.

Bobby, a wire-haired vizsla, was introduced to airplane seats at the training center. Credit Ilana Panich-Linsman for The New York Times

Not every dog makes it through the course, and some have to return for additional training for a variety of reasons, like aggression issues.
Even dogs that pass their training can make mistakes. Instructors here say dogs have been known to sit down next to a police officer, indicating the presence of explosives. But the officer had only recently fired a handgun at a firing range or handled bomb-making material.
"They are great tools," said Lawrence Myers, a former professor at Auburn's canine training center. "But do they lie and get things wrong? Yes, they do. Sometimes it's as simple as 'I want my reward, so what do I have to do for it?'"
A 2011 study by researchers at the University of California, Davis, found that handlers could influence the behavior of dogs, getting them to indicate the presence of explosives or drugs even when none were present.
Despite these issues, dogs remain the best method of detecting bombs. T.S.A. and other counterintelligence officials are hoping that the Arizona State University research by Professor Wynne can help provide better training for dogs to detect homemade bombs.
"It is essential we engage the dog's brain in considering the whole complexion of what they smell and making smart decisions about whether this can be a bomb or not," Professor Wynne said.

T-REX: A Portable Device for Explosives Vapors

By R. Rousier, S. Bouat, T. Bordy et al.
Source: http://www.sciencedirect.com/science/article/pii/S1877705812042208

Abstract
A portable device is reported to detect and identify in real time explosive vapors usually used by the terrorists. This device is composed of the multi-sensors chamber with three technologies of explosive vapors sensors: Quartz Crystal Microbalance (QCM), Surface Acoustic Wave (SAW) and fluorescence. The multi-sensors chamber was designed and optimized to guaranty an efficient fluidic repartition on each sensor to

assure the suitable responses of sensors. A laptop controls the device. An algorithm has been specifically developed to detect and identify gas nature. On 33 experimentations with various explosives or interferents, the preliminaries results have shown the detection and the identification in about 1 min.

(Photos from: CBNW Journal 2016 Vol2; p.89)

▶ **Full paper is available at source's URL.**

New Device Will Blow Cover Off Suicide Bombers

Source: http://i-hls.com/2016/06/watch-new-device-will-blow-cover-off-suicide-bombers/

June 06 – New Mexico engineers are working on a new device that could save scores of lives. Scientists from Sandia National Laboratories in cooperation with R3 Technologies are trying to develop a game-changing radar system that could detect suicide bombers.

"There is no technology in the market anywhere that will scan and look for a suicide bomber, and find them," said R3 Technologies Manager, Robby Roberson. "It doesn't exist."

The idea isn't new. In fact, Roberson's dad, Coda Roberson, started working on such a system years ago. Sadly, he died before his work bore fruit. "He felt he owed his country something," said Roberson.

But Roberson the son, along with the Sandia team, are now close to making it work.

JR Russell, Sandia Labs scientist, explained that suicide bombers frequently use materials like nails, ceramic balls, and even small rocks as shrapnel in their improvised explosive devices. **Roberson and Co's concealed bomb detector, CBD-1000, uses radar to find these materials that a metal detector simply cannot.**

If the device doesn't detect a threat, the operator will see a return signal that is vertically polarised. If there is a threat, then a horizontally polarised signal will also return, alerting the operator to the danger.

The device could have applications everywhere, Russell said, from airports, to concerts, to political rallies – any large gathering of people could be protected. As we have seen from the Paris and Brussels attacks, and from our own explosive history in Israel, there is a real need for such a device.

"If we're successful we'll be saving lives," said Russell.

▶ **You can watch it work in the video at source's URL.**

New guidance notes following Didcot explosion

Source: http://www.shponline.co.uk/new-guidance-notes-following-didcot-explosion/

June 07 – Following the Didcot Power Station incident in February, the National Federation of Demolition Contractors (NFDC) has confirmed that it will lead a project to write and publish industry guidance about the planning, preparation and use of explosives in demolition.

One person died and three further bodies have not yet been found following the collapse at the Oxfordshire power station, on 23 February. Five more people were injured in the blast.

Demolition was taking place at the time of the collapse and recent reports state that work to clear the debris from the site has been halted because contractors have reached a 50m (164 ft) "exclusion zone".

Along with the Institute of Demolition Engineers and the Institute of Explosives Engineers, the new NFDC guidance "will draw together and update existing material from a wide variety of sources."

Speaking to SHP, the NFDC said: "The National Federation of Demolition Contractors are delighted to have been asked by the HSE to prepare the Explosive Demolition Guidance Notes. The committee, formed by the NFDC is chaired by William Sinclair a very experienced explosives engineer, and backed by the IDE and IEE.

"This important document is a high priority for the industry, and will be ready for publication later in the year."

In a statement the HSE said: "The Didcot incident on 23rd February 2016 has highlighted a demand from clients and contractors outside the highly specialised but small explosives

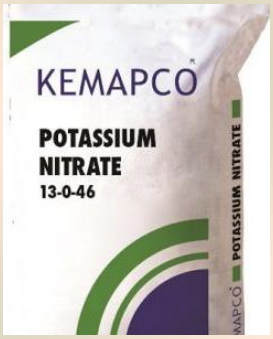
engineering community for information about the planning, preparation and use of explosives in demolition.
"The NFDC has kindly volunteered to lead a project, assisted by specialists from the Institute of Demolition Engineers and the Institute of Explosives Engineers, to write and publish guidance on this subject. This will draw together and update existing material from a wide variety of sources."
The HSE has confirmed that it is currently investigating two cases of failed implosions in April. One involved the failed blow-down of two 14-storey blocks of flats in Seaforth, Liverpool, and the other involved the failure to demolish a disused pit-tower at a former mine in Harworth, Nottinghamshire.

Turkey suspends sale of fertilizers containing nitrate in wake of car bombings

Source: http://www.homelandsecuritynewswire.com/dr20160609-turkey-suspends-sale-of-fertilizers-containing-nitrate-in-wake-of-car-bombings

June 09 – **In the wake of two car bombings which killed seventeen people, Turkey announced it was temporarily suspending the sale of fertilizers containing nitrate.**
The terrorists in the two bombings used fertilizers to make the explosives – as did Timothy McVeigh twenty years ago.
Cyprus Mail reports that Turkey has experienced a surge of violence since last summer, when the peace negotiations between the Turkish government and Kurdish rebels collapsed. At the same time, ISIS militants launched their own campaign inside Turkish territory.
The government says that Kurdish separatists were behind Tuesday's car bomb in Istanbul. The car exploded when a bus carrying police officers passed by. On Wednesday, a suicide car bombing targeted a police station in the town of Midyat, near the border with Syria, killing three police officers and three civilians.

The Turkish Interior Ministry official said the security services have evidence that both attacks were carried out by the Kurdistan Workers' party, or PKK. Explosive experts said the attackers had used half a ton of explosives in the attack against the police headquarters in Midyat.



"As of now, the sale of fertilizers containing nitrate that are used for explosives has been frozen in Turkey," the agriculture minister, Faruk Çelik, said on state television.
Security experts note that Turkey had already taken steps to control and monitor the sale of fertilizers but Çelik said these measures had proved inadequate. **He said security agencies have temporarily seized 64,000 tons of fertilizers containing nitrate from retailers.**

Smiths Detection Extends IONSCAN 600 Capability to Detect Narcotics

Source: http://www.hstoday.us/single-article/smiths-detection-extends-ionscan-600-capability-to-detect-narcotics/935b4707a35fc7e9535e8f388aa4914c.html

June 13 – **Smiths Detection's IONSCAN 600 trace detector has been enhanced to detect and identify narcotics, in addition to its existing capabilities for explosives**. Extending the library of threats to include narcotics will provide customers in the aviation,

ports and borders or critical infrastructure markets with a more comprehensive solution to their detection needs.

The portable desktop IONSCAN 600 will be able to detect a range of narcotics such as amphetamine, cocaine, heroin, ketamine, MDA, MDMA and others. This capability will be important to front-line organizations including customs authorities, prisons and other secure facilities, which have a growing requirement to detect and identify illegal narcotics and other controlled substances.

The new version of IONSCAN 600, available from June 2016, will offer the option to identify both narcotics and explosives, either separately, or both simultaneously. From October 2016, the IONSCAN 600 will also offer an optional built-in compact thermal printer to enable analysis results and logs to be documented on the spot.

Head of Sensor Products, Ken Fredeen, said, "IONSCAN 600 has established itself as a market leading product over the past two years, with certification by ECAC, the major European aviation authority and adoption by airports throughout the EU and Middle East. The additional narcotics library will provide customers with extended detection capabilities to better meet their ever-evolving, mission-critical detection needs."

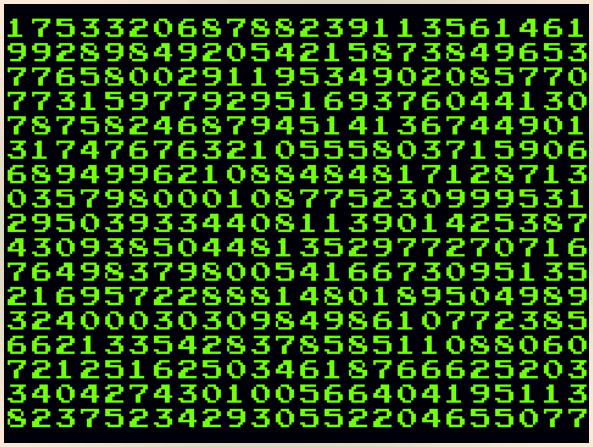
The IONSCAN 600 improves screening capabilities by delivering ease-of-use, flexibility and cost advantages for trace detection applications. It is augmented by ReachBack, 24/7/365 service and support to ensure optimum product performance, and delivers reliable performance consistent with Smiths Detection's range of high quality solutions.

The IONSCAN 600 narcotics version will be on display and available for demonstration to the general public for the first time in the United States at the American Correctional Association Congress of Correction, August 7-9, 2016 at the John B. Hynes Veterans Memorial Convention Center in Boston, MA.

New method of producing random numbers could improve cybersecurity

Source: http://www.cybersecurity-review.com/new-method-of-producing-random-numbers-could-improve-cybersecurity

May 16 – With an advance that one cryptography expert called a "masterpiece," University of Texas at Austin computer scientists have developed a new method for producing truly random numbers, a breakthrough that could be used to encrypt data, make electronic voting more secure, conduct statistically significant polls and more accurately simulate complex systems such as Earth's climate.



The new method creates truly random numbers with less computational effort than other methods, which could facilitate significantly higher levels of security for everything from consumer credit card transactions to military communications.

Computer science professor David Zuckerman and graduate student Eshan Chattopadhyay will present research about their method in June at the annual Symposium on Theory of Computing (STOC), the Association for Computing Machinery's premier theoretical computer science conference. An invitation to present at the conference is based on a rigorous peer review process to evaluate the work's correctness and significance. Their paper will be one of three receiving the STOC Best Paper Award.

"This is a problem I've come back to over and over again for more than 20 years," says Zuckerman. "I'm thrilled to have solved it."

Another Day, Another Hack: 117 Million LinkedIn Emails And Passwords

Source: http://www.cybersecurity-review.com/another-day-another-hack-117-million-linkedin-emails-and-passwords

May 18 – A hacker is trying to sell the account information, including emails and passwords, of 117 million LinkedIn users.

The hacker, who goes by the name "Peace," told Motherboard that the data was stolen during the LinkedIn breach of 2012. At the time, only around 6.5 million encrypted passwords were posted online, and LinkedIn never clarified how many users were affected by that breach.

Turns out it was much worse than anybody thought.

Peace is selling the data on the dark web illegal marketplace The Real Deal for 5 bitcoin (around $2,200). The paid hacked data search engine LeakedSource also claims to have obtained the data. Both Peace and the one of the people behind LeakedSource said that there are 167 million accounts in the hacked database. Of those, around 117 million have both emails and encrypted passwords.

Security risks in the age of smart homes

By Earlence Fernandes

Source: http://www.homelandsecuritynewswire.com/dr20160531-security-risks-in-the-age-of-smart-homes

May 31 – Smart homes, an aspect of the Internet of Things, offer the promise of improved energy efficiency and control over home security. Integrating various devices together can offer users easy programming of many

devices around the home, including appliances, cameras and alarm sensors. Several systems can handle this type of task, such as Samsung SmartThings, Google

Brillo/Weave, Apple HomeKit, Allseen Alljoyn and Amazon Alexa.

But there are also security risks. Smart home systems can leave owners vulnerable to serious threats, such as arson, blackmail, theft and extortion. Current security research has focused on individual devices, and how they communicate with each other. For example, the MyQ garage system can be turned into a surveillance tool, alerting would-be thieves when a garage door opened and then closed, and allowing them to remotely open it again after the residents had left. The popular ZigBee communication protocol can allow attackers to join the secure home network.

Little research has focused on what happens when these devices are integrated into a coordinated system. We set out to determine exactly what these risks might be, in the hope of showing platform designers areas in which they should improve their software to better protect users' security in future smart home systems.

Evaluating the security of smart home platforms

First, we surveyed most of the above platforms to understand the landscape of smart home programming frameworks. We looked at what systems existed, and what features they offered. We also looked at what devices they could interact with, whether they supported third-party apps, and how many apps were in their app stores. And, importantly, we looked at their security features.

We decided to focus deeper inquiry on SmartThings because it is a relatively mature system, with 521 apps in its app store, supporting 132 types of IoT devices for the home. In addition, SmartThings has a number of conceptual similarities to other, newer systems that make our insights potentially relevant more broadly. For example, SmartThings and other systems offer trigger-action programming, which lets you connect sensors and events to automate aspects of your home. That is the sort of capability that can turn your walkway lights on when a driveway motion detector senses a car driving up, or can make sure your garage door is closed when you turn your bedroom light out at night.

We tested for potential security holes in the system and 499 SmartThings apps (also called SmartApps) from the SmartThings app store, seeking to understand how prevalent these security flaws were.

Finding and attacking main weaknesses

We found two major categories of vulnerability: excessive privileges and insecure messaging.

Overprivileged SmartApps: SmartApps have privileges to perform specific operations on a device, such as turning an oven on and off or locking and unlocking a door. This idea is similar to smartphone apps asking for different permissions, such as to use the camera or get the phone's current location. These privileges are grouped together; rather than getting separate permission for locking a door and unlocking it, an app would be allowed to do both – even if it didn't need to.

For example, imagine an app that can automatically lock a specific door after 9 p.m. The SmartThings system would also grant that app the ability to *unlock* the door. An app's developer cannot ask only for permission to lock the door.

More than half – 55 percent – of 499 SmartApps we studied had access to more functions than they needed.

Insecure messaging system: SmartApps can communicate with physical devices by exchanging messages, which can be envisioned as analogous to instant messages exchanged between people. SmartThings devices send messages that can contain sensitive data, such as a PIN code to open a particular lock.

We found that as long as a SmartApp has even the most basic level of access to a device (such as permission to show how much battery life is left), it can receive all the messages the physical device generates – not just those messages about functions it has privileges to. So an app intended only to read a door lock's battery level could also listen to messages that contain a door lock's PIN code.

In addition, we found that SmartApps can "impersonate" smart-home equipment, sending out their own messages that look like messages generated by real physical devices. The malicious SmartApp can read the network's ID for the physical device, and create a message with that stolen ID. That battery-level app could even covertly send a message as if it were the door lock, falsely reporting it had been opened, for example.

SmartThings does not ensure that only physical devices can create messages with a certain ID.

Attacking the design flaws

To move beyond the potential weaknesses into actual security breaches, we built four proof-of-concept attacks to demonstrate how attackers can combine and exploit the design flaws we found in SmartThings.

In our first attack, we built an app that promised to monitor the battery levels of various wireless devices around the home, such as motion sensors, leak detectors, and door locks. However, once installed by an unsuspecting user, this seemingly benign app was programmed to snoop on the other messages sent by those devices, opening a key vulnerability.

When the authorized user creates a new PIN code for a door lock, the lock itself will acknowledge the changed code by sending a confirmation message to the network. That message contains the new code, which could then be read by the malicious battery-monitoring app. The app can then send the code to its designer by SMS text message – effectively sending a house key directly to a prospective intruder.

In our second attack, we were able to snoop on the supposedly secure communications between a SmartApp and its companion Android mobile app. This allowed us to impersonate the Android app and send commands to the SmartApp – such as to create a new PIN code that would let us into the home.

Our third and fourth attacks involved writing malicious SmartApps that were able to take advantage of other security flaws. One custom SmartApp could disable "vacation mode," a popular occupancy-simulation feature; we stopped a smart home system from turning lights on and off and otherwise behaving as if the home were occupied. Another custom SmartApp was able to falsely trigger a fire alarm by pretending to be a carbon monoxide sensor.

Room for improvement

Taking a step back, what does this mean for smart homes in general? Are these results indicative of the industry as a whole? Can smart homes ever be safe?

There are great benefits to gain from smart homes, and the Internet of Things in general, that ultimately lead to an improved quality of living. However, given the security weaknesses in today's systems, caution is appropriate.

These are new technologies in nascent stages, and users should think about whether they are comfortable with giving third parties (e.g., apps or smart home platforms) remote access to their devices. For example, personally, I wouldn't mind giving smart home technologies remote access to my window shades or desk lamps. But I would be wary of staking my safety on remotely controlled door locks, fire alarms, and ovens, as these are security- and safety-critical devices. If misused, those systems could allow – or even cause – physical harm.

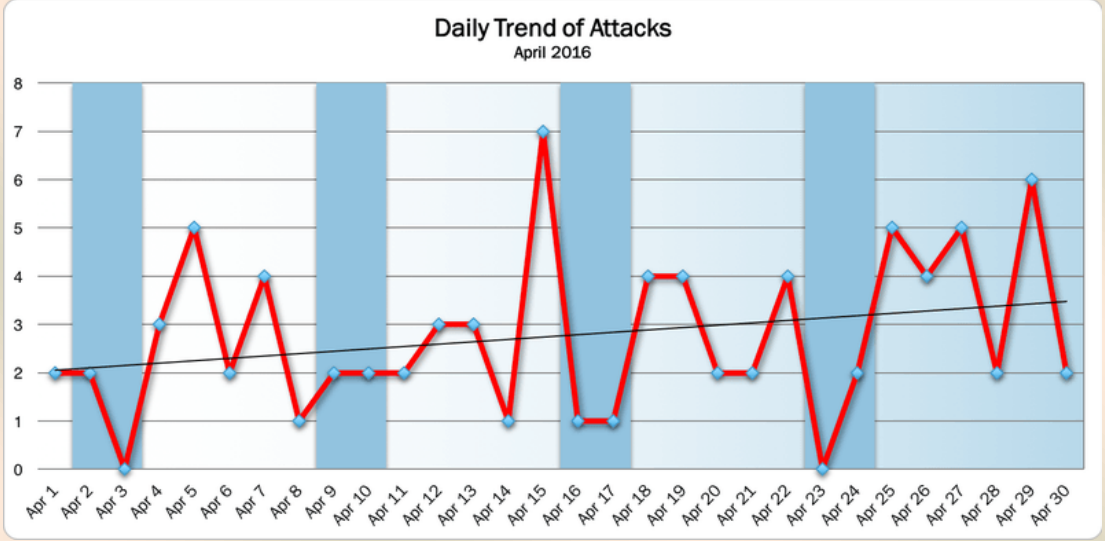
However, I might change that assessment if systems were better designed to reduce the risks of failure or compromise, and to better protect users' security.

Earlence Fernandes *is Ph.D. student, Systems and Security, University of Michigan. This research is the result of a collaboration with Jaeyeon Jung and Atul Prakash.*

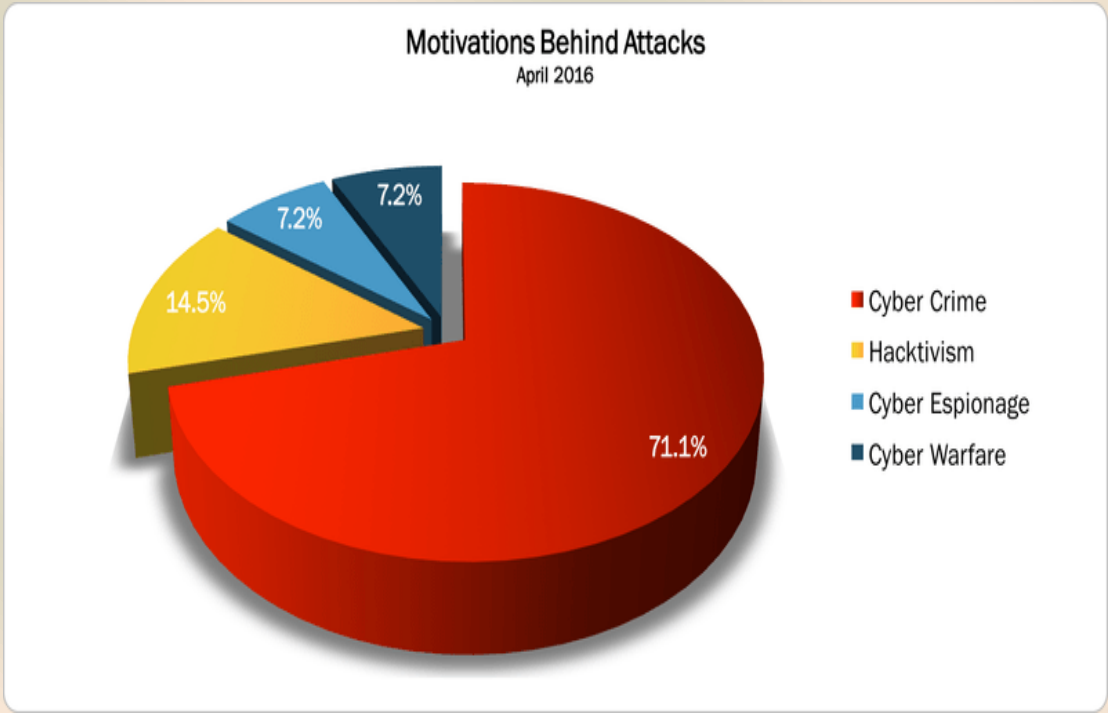
April 2016 Cyber Attacks Statistics

Source: http://opensources.info/april-2016-cyber-attacks-statistics-2/

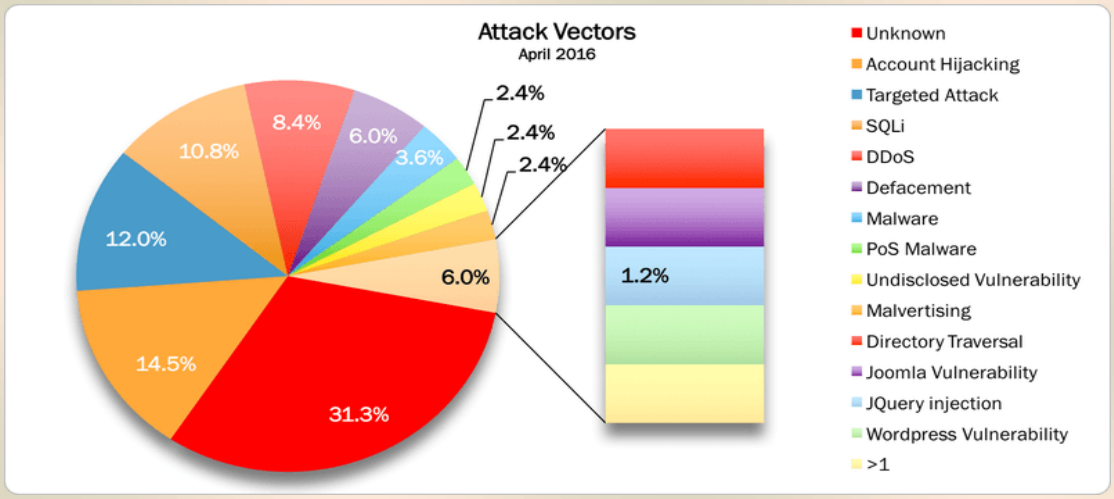
It's time to publish the statistics related to the two cyber attacks timeline of April (Part I and Part II).
As usual let's start from the **Daily Trend of Attacks**, which shows a trend progressively growing towards the end of the month, and is characterized by a peak in the middle.



Unsurprisingly, cyber crime ranks on top of the **Motivations Behind Attacks** chart with 71.1% (close to 73.9% of March). Hacktivism is essentially stable at 14.5% (a slight increase compared to 12% of March). Cyber Espionage and Cyber Warfare report the same 7.2%, against respectively 10.9% and 3.3% in March.

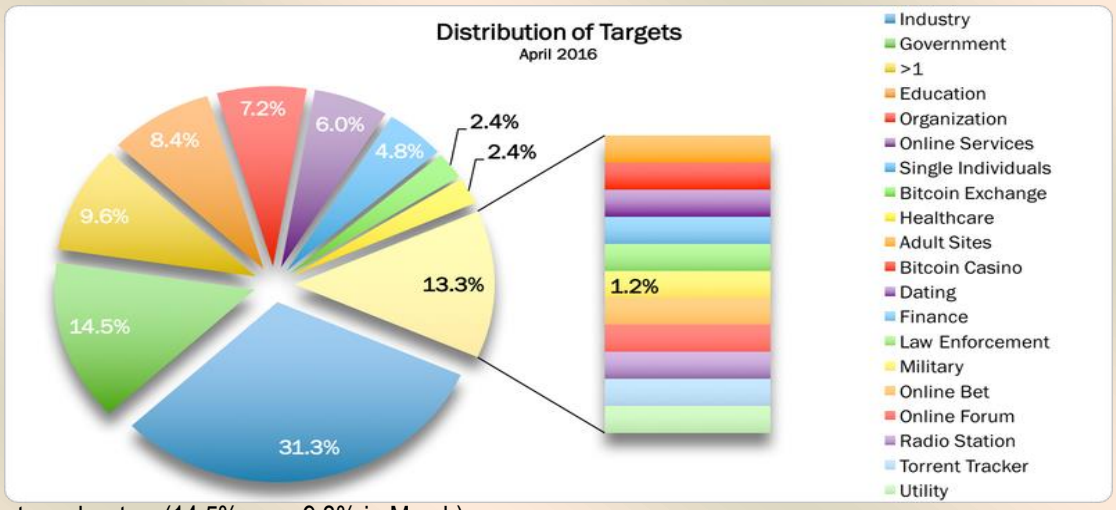


31.3% of the **Attack Vectors** are unknown. Analyzing the known vectors, account hijackings rank at number one among the known with 14.5% (in March they were at number one with 20.7%). Targeted attacks rank at number two with 12% (were 9.8% in March). SQLi is immediately behind with 10.8%



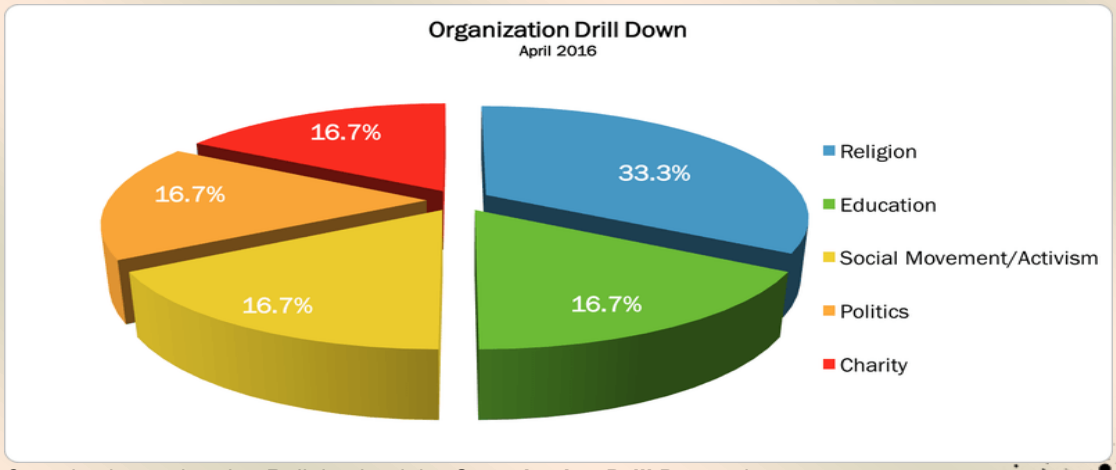
(9.8% in March).

Industries lead the **Distribution of Targets** chart with 31.3% (was 33.7% in March). Governments rank

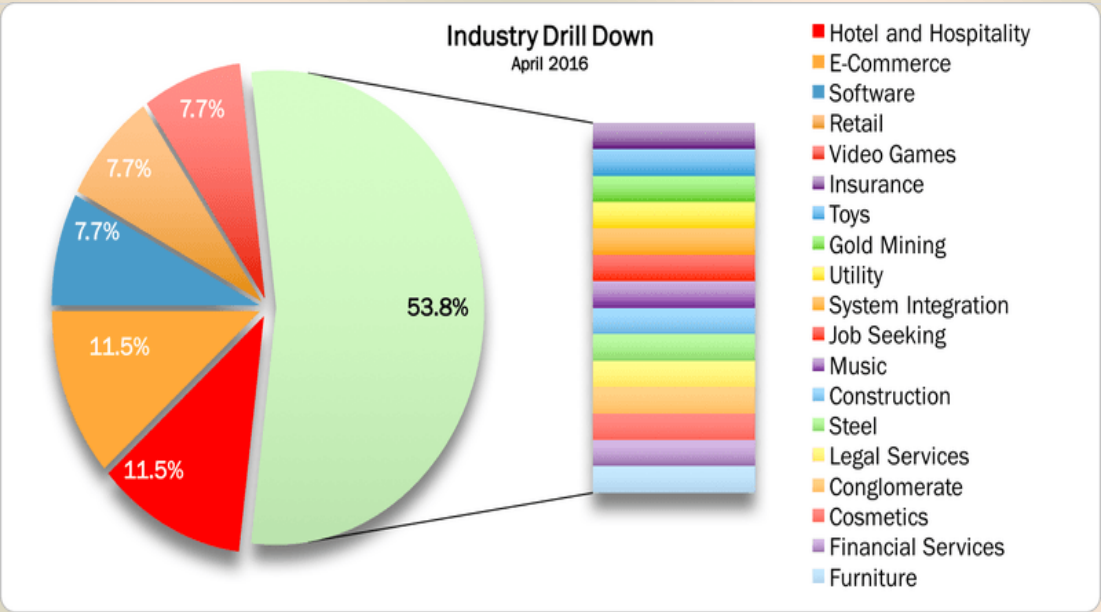


at number two (14.5%, was 9.8% in March).

The **Industry Drill Down** see Hotel and Hospitality and E-Commerce on-top with 11.5%. Software, retail and video games follow with 7.7% and emerge over the rest of the verticals.



Organizations related to Religion lead the **Organization Drill Down** chart.



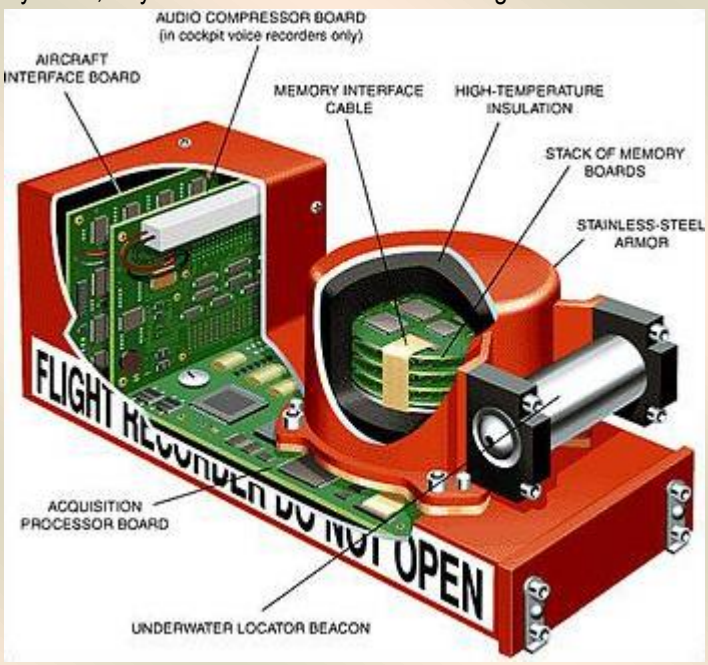
As usual, the sample must be taken very carefully since it refers only to discovered attacks included in my timelines, aiming to provide an high level overview of the "cyber landscape".

If you want to have an idea of how fragile our data are inside the cyberspace, have a look at the timelines of the main Cyber Attacks in 2011, 2012, 2013, 2014 and now 2015 (regularly updated). You may also want to have a look at the Cyber Attack Statistics.

Data contained in the black boxes should be stored in the cloud: Expert

Source: http://www.homelandsecuritynewswire.com/dr20160607-data-contained-in-the-black-boxes-should-be-stored-in-the-cloud-expert

June 07 – Professor David Stupples, City University of London's Professor of Electronic and Radio Systems, says the time has come for the flight data recorder (FDR) and the cockpit data recorder (CDR) — the black box found on aircraft — to be stored in the cloud.



The usually orange-colored flight recorder is an electronic recording device used in the event of an aviation accident (or incident) investigation.

CUL notes that Professor Stupples' recommendation comes in the wake of recent commercial airline accidents at sea where the recovery of the aircraft's black box from considerable sea depths is frequently long and arduous.

He suggests that following the disappearances of Air France 447 over the South Atlantic, Malaysian MH370 over the Southern Indian Ocean, and recently EgyptAir MS804 over

the Mediterranean, the aviation industry should reconsider the safe recording of flight data and flight-deck voice communications (the so-called black boxes) on a cloud facility, remote from the aircraft where it is instantaneously accessible:

"In the Air France incident it took two years to recover the flight data recorder and cockpit voice recorder in order to discover the cause of the crash leading to better training for pilots. With Malaysian MH370, it has been over two years since the disappearance with search teams no closer to finding the black boxes. Relatives of the lost crew and passengers are still awaiting closure and the world still needs knowledge of the cause of the loss."

Professor Stupples says the solution to black box storage "is very simple" and all that is needed is for the "required monitoring data to be streamed via satellite — Inmarsat for example — to a safe cloud storage facility."

He believes that due to the cost of implementing this solution and airline pilots not wanting their casual conversations recorded for extended periods of time, the aviation industry may be slow to respond:

"The cost factor comes down to retrofitting airliners with the required communications equipment and charges for using satellite communications to stream the required data. The technology could be prepared for very little additional cost."

Professor Stupples adds: "Perhaps some arrangement should be negotiated with airline pilots whereby their conversations would remain confidential and only stored for a limited period of time to maintain personal privacy. This is not 'rocket science' and the authorities should begin considering public safety rather that constantly considering the 'purse strings'."

New EU Cybersecurity Requirements Soon to Fall on "Essential Services" Operators

By Aline Doussin

Source: http://www.natlawreview.com/article/new-eu-cybersecurity-requirements-soon-to-fall-essential-services-operators

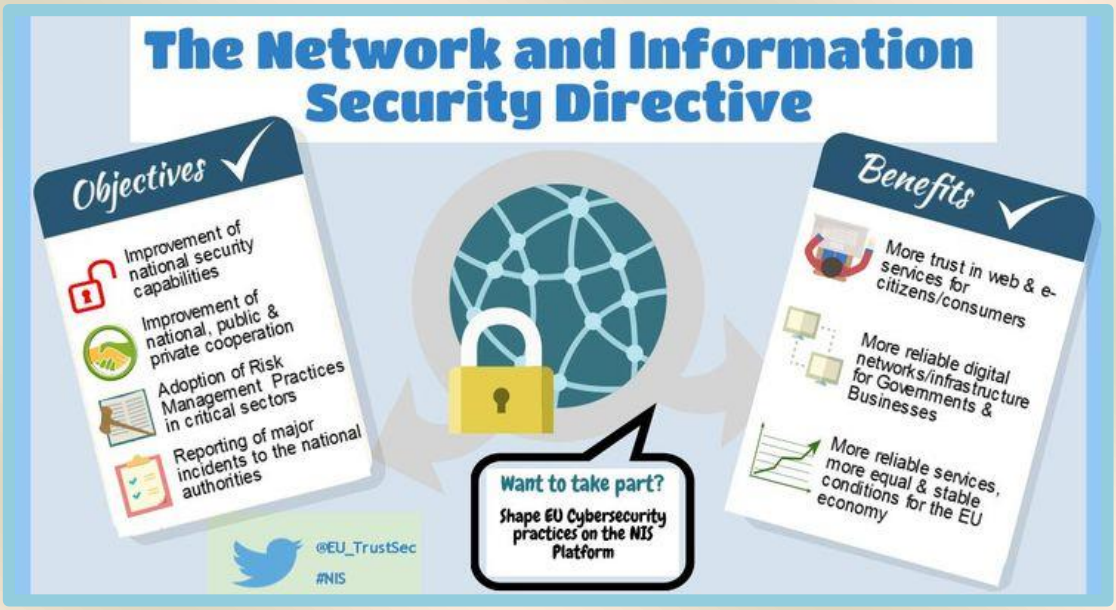
May 29 – On 17 May 2016, the Council of the European Union formally adopted the Network and Information Security (NIS) Directive at first reading, paving the way for its final adoption and entry into force in August 2016.

What is the NIS Directive?

The Directive aims to step up the security of network and information systems across the EU. Initially proposed in 2013, it has been progressing through the EU legislative procedure for some time. The Directive aims to:

- Improve the cybersecurity capabilities of Member States;
- Improve cooperation between Member States on the issue of cybersecurity;
- Ensure that operators of essential services in "critical sectors", such as banking, health, energy and transport and key digital service providers, such as online marketplaces, search engines and cloud services, take appropriate security measures and report cybersecurity incidents to the relevant national authorities;
- Ensure that each EU country designates one or more national authorities to implement and enforce the Directive and create Computer Security Incident Response Teams (CSIRTs) responsible for monitoring and responding to security incidents at national level; and

- Establish an EU-wide strategy for dealing with cyber threats.



Who is subject to the NIS Directive?

The NIS Directive applies to two categories of service providers: operators of essential services and digital service providers.

(i) *Operators of essential services*

A company is an operator of essential services if:

- It provides a service which is essential for the maintenance of critical societal and/or economic activities;
- The provision of that service depends on network and information systems; and
- An incident affecting the network and information systems of that service would have significant disruptive effect on its provision or on public safety.

The NIS Directive will require operators of essential services in the energy (electricity, oil and gas), transport (air, rail and roads), banking and healthcare sectors to take security measures and report cyberattack incidents to national authorities.

(ii) *Digital service providers*

The NIS Directive applies to three main categories of digital service providers: online marketplaces, online search engines and cloud computing services. Whether or not to include digital service providers within the scope of the Directive was one of the most contentious issues during the two years of negotiations around the Directive. Following lengthy negotiations, social networks and payment service providers were excluded.

- An "online marketplace" is defined as "a digital service that allows consumers and/or traders…to conclude online sales and service contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace." This broad definition includes marketplaces that engage in B2C as well as B2B transactions. Whilst app stores are deemed to be in scope, price-comparison websites are not.
- An online search engine is defined as "a digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query or any subject in the form of a keyword, phrase or other input; and returns links in which information related to the requested content can be found." However, the NIS Directive does clarify that search engines within a particular site will not be subject to the Directive.
- A "cloud computing service" is widely defined as a "digital service that enables access to a scalable and elastic pool of sharable computing resources." This could catch companies providing public, private and hybrid cloud services.

What are the sanctions for non-compliance with the NIS Directive?

Failure to comply with the NIS Directive will trigger substantial penalties for the most serious infringements: up to 2% of a company's global turnover. Businesses within the scope of the Directive must conduct internal audits to ensure that their network and information security practices are compliant with the new requirements, well documented and effective.

What are the next steps?

The NIS Directive must now be approved by the European Parliament. It is expected to come into force in August 2016. Thereafter, Member States will have 21 months to transpose the Directive into national law, and six months after that to identify operators of essential services.

***Aline Doussin** is a senior associate in the firm's Regulated Industries department specialising in International Trade (including export control and sanctions), EU Regulatory and Public Policy. Aline's experience is derived from her similar previous position in a major international law firm, and from her former roles at the World Trade Organization (WTO) in Geneva and as an in-house lawyer in Japan Tobacco International (JTI).*

Hackers could easily cause drones to ignore human controllers, or crash

Source: http://www.homelandsecuritynewswire.com/dr20160609-hackers-could-easily-cause-drones-to-ignore-human-controllers-or-crash

June 09 – Sales of drones — small flying machines equipped with cameras — are soaring. But new research by a Johns Hopkins computer security team has raised concerns about how easily hackers could cause these robotic devices to ignore their human controllers and land or, more drastically, crash.

Five security informatics graduate students and their professor discovered three different ways to send rogue commands from a computer laptop to interfere with an airborne hobby drone's normal operation and land it or send it plummeting.

Johns Hopkins reports that the finding is important because drones, also called unmanned aerial vehicles, have become so popular that they are, pardon the expression, flying off the shelves. A recent article in *Fortune*, referring to the 12-month period ending in April, trumpeted that "Drone Sales Have Tripled in the Last Year." And the devices are not cheap. The article stated that the average cost of a drone was more than $550, though prices vary widely depending on the sophistication of the device. A recent Federal Aviation Administration (FAA) report predicted that 2.5 million hobby-type and commercial drones would be sold in 2016.

Hobby drones are flown largely for recreation and aerial photography or videography. But more advanced commercial drones can handle more demanding tasks. Farmers have begun using drones with specialized cameras to survey their fields and help determine when and where water and fertilizer should be applied. Advanced commercial drones can also help in search and rescue missions located in challenging terrain. Some businesses, such as Amazon, are exploring the use of drones to deliver merchandise to their customers.

Johns Hopkins security informatics grad students and their professor discovered three security flaws in a popular hobby drone, all of which can cause the small aircraft to make an "uncontrolled landing." (Credit: Will Kirk/Johns Hopkins University)

But in their haste to satisfy consumer demands, drone makers may have left a few digital doors unlocked. "You see it with a lot of new technology," said. Lanier A. Watkins, who supervised the recent drone research at Johns Hopkins' Homewood campus. "Security is often an afterthought. The value of our work is in showing that the technology in these drones is highly vulnerable to hackers."

Watkins is a senior cybersecurity research scientist in the university's Whiting School of Engineering, Department of Computer Science. He also holds appointments with the Johns Hopkins Applied Physics Laboratory and the Johns Hopkins Information Security Institute.

During the past school year, Watkins's security informatics master's degree students were required to apply what they had learned about information security by completing a capstone project. Watkins suggested they do wireless network penetration testing on a popular hobby drone and develop "exploits" from the vulnerabilities found to disrupt the process that enables a drone's operator on the ground to manage its flight.

An "exploit," explained Michael Hooper, one of the student researchers, "is a piece of software typically directed at a computer program or device to take advantage of a programming error or flaw in that device."

In the team's first successful exploit, the students bombarded a drone with about 1,000 wireless connection requests in rapid succession, each asking for control of the airborne device. This digital deluge overloaded the aircraft's central processing unit, causing it to shut down. That sent the drone into what the team referred to as "an uncontrolled landing."

In the second successful hack, the team sent the drone an exceptionally large data packet, exceeding the capacity of a buffer in the aircraft's flight application. Again, this caused the drone to crash.

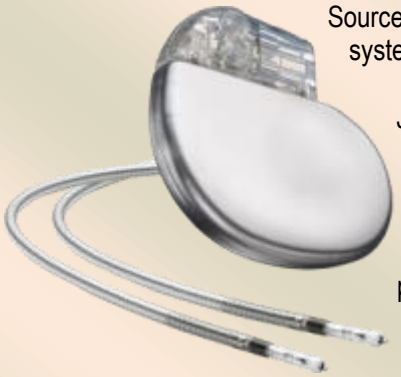
For the third exploit, the researchers repeatedly sent a fake digital packet from their laptop to the drone's controller, telling it that the packet's sender was the drone itself. Eventually, the researchers said, the drone's controller started to "believe" that the packet sender was indeed the aircraft itself. It severed its own contact with the drone, which eventually led to the drone making an emergency landing.

"We found three points that were actually vulnerable, and they were vulnerable in a way that we could actually build exploits for," Watkins said. "We demonstrated here that not only could someone remotely force the drone to land, but they could also remotely crash it in their yard and just take it."

JH notes that in accordance with university policy, the researchers described their drone exploit findings in a Vulnerability Disclosure Package and sent it early this year to the maker of the drone that was tested. By the end of May, the company had not responded to the findings. More recently, the researchers have begun testing higher-priced drone models to see if these devices are similarly vulnerable to hacking.

Watkins said he hopes the studies serve as a wake-up call so that future drones for recreation, aerial photography, package deliveries and other commercial and public safety tasks will leave the factories with enhanced security features already on board, instead of relying on later "bug fix" updates, when it may be too late.

Electronic anti-theft systems pose a threat to cardiac device patients



Source: http://www.homelandsecuritynewswire.com/dr20160609-electronic-antitheft-systems-pose-a-threat-to-cardiac-device-patients

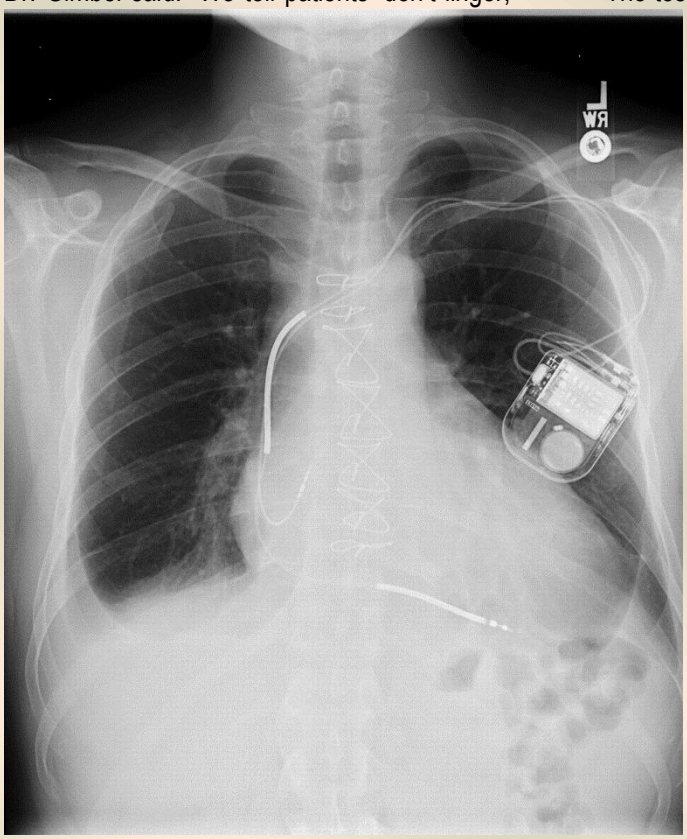
June 09 – Electronic anti-theft systems still post a threat to cardiac device patients, according to research presented the other day at CARDIOSTIM – EHRA EUROPACE 2016 by Professor Robert Stevenson, senior scientist at Greatbatch Medical in Santa Clarita, California.

"Cardiac implantable electronic devices (CIEDs) are critical to patients' health," said paper co-author Dr. Rod Gimbel, an electrophysiologist at Case Western Reserve University. "Pacemakers provide pacing support, without which there

would be no heart beat at all for a pacemaker dependent patient. Implantable cardioverter defibrillators (ICDs) deliver pacing or shocks to rescue patients from potentially life threatening arrhythmias."

The European Society of Cardiology reports that even though reported events are rare, prolonged exposure to electronic anti-theft systems, also called electronic article surveillance (EAS) systems, can cause pacing therapy to drop beats or in the worst case leave pacemaker dependent patients with no heartbeat, and cause ICDs to deliver inappropriate shocks. In 2000 the Food and Drug Administration (FDA) advised CIED patients not to linger or lean next to EAS systems. But since then manufacturers have created sleeves for retailers to cover traditional pedestal systems with advertising and new systems are hidden under floors, in walls and in doors.

Dr. Gimbel said: "We tell patients 'don't linger,



don't lean' but that advice is hard to follow when systems are invisible. To make matters worse, advertising draws patients closer to the pedestals. Some shops have placed camouflaged pedestals next to a chair or in a checkout line, so patients may be next to them for some time, and sofas are put on top of under floor systems, encouraging patients to sit for long periods."

The current study was conducted at Georgia Tech Research Institute (GTRI) in Atlanta and assessed the safety of modern EAS systems. The investigators tested pacemakers and ICDs with up to five CIED manufacturers against the three types of EAS systems currently in use: pedestals (five manufacturers), doorframes/in wall (two manufacturers) and under floor (two manufacturers). The under floor system was tested flat and at a 30 degree angle to mimic slouching in a chair. The results were recorded in four categories: no interference, prolonged pacemaker inhibition, inappropriate shocks, and other inappropriate tachycardia therapy such as anti-tachycardia pacing or subclinical shocks.

The tests were conducted with the pacemakers and ICDs in a tank filled with a type of saline that mimics the electric properties of body tissue. Cardiac device leads were placed in the same loop shape as they would be in a patient and the devices were tested in unipolar and bipolar settings. The distance between devices and the floor was set for average height patient. Devices were tested in static positions and using a robot to simulate a patient walking through the EAS systems, leaning towards them, and facing them.

The investigators found that the pedestal systems interfered with cardiac device functioning particularly when the devices were in close proximity and lingered. Devices programmed for unipolar sensing had the most interactions which included prolonged inhibition of pacing and inappropriate ICD therapy. Devices programmed with bipolar sensing showed fewer interactions but unintentional shocks and other inappropriate tachycardia therapy was observed.

Professor Stevenson said: "Significant interactions occurred with nearly all the pacemakers and ICDs when the robot closely faced the EAS system and the device lead loop was parallel to the EAS system loop. Facing or having your back to an EAS pedestal or a toddler with a pacemaker crawling over a

subfloor system is of particular concern."
Wall (doorframe) systems did not interfere. Preliminary tests of under floor systems (only two CIED manufacturers), which are completely hidden, did not interfere when flat or at a 30 degree angle from vertical. Professor Stevenson said: "We know from the physics that at 90 degrees (this is when the patient's chest is close and parallel to the floor) we would likely have serious interactions. Further testing is needed to find out when the angle becomes dangerous. I suspect it will be about 45 degrees. This angle could occur with a patient really slouching in a chair for example."
He continued: "Unipolar sensing is sometimes required but otherwise I would urge doctors to use bipolar sensing since the lead loop area is smaller, lowering the chance of interference. Doctors must educate patients about the potential dangers of EAS systems as many have never been warned not to lean or linger in retail store entrances. It is particularly important that patients do not sit or slouch in a chair or couch in store entry areas."
Professor Stevenson concluded: "Electronic anti-theft systems are a part of everyday life, with more than 800 000 pedestals alone installed worldwide. Patients are safe if they walk at a constant pace through the system. EAS gates that are obscured with advertising or goods for sale, or hidden in the floor with couches or chairs adjacent, are a serious concern and EAS manufacturers have a responsibility to ensure that retailers install them in such a way that they are visible and well marked."

ISIS kill list names '39 Brits' as terror targets its supporters should 'follow' and 'avenge for Muslims'

Source: http://www.mirror.co.uk/news/world-news/isis-kill-list-names-39-8145792

A pro- ISIS hacking group have published a list of names - including 39 Brits - as fresh terror targets on a chilling 'kill list'.
The United Cyber Caliphate (UCC) shared the full list of 8,318 people including their addresses and email contact details on a secretive messaging app service.
It urged its supporters to "follow" those listed - and "kill them strongly to take revenge for Muslims".
An image it attached to the posts declared: "All world can't stop Islamic State" - and talked of 'Ghosts' and a 'Caliphate Cyber Army' - together with a picture of a lone, masked and armed soldier wandering a battlefield.

It is one of the longest kill lists any ISIS-affiliated group has distributed to date - but the believed to be the first the group has issued to contain details of non-US citizens.

It is not known if the 39 Brits named are military or government workers - or people in the public eye like royalty or celebrities.

The list - written in both English and Arabic - was uncovered by the media group Vocativ which specialises in investigating the hidden side of the web. It discovered it on a messaging app service called Telegram on Monday night.

It said most of the names and the accompanying addresses listed "appear to belong to people in the United States, Australia, and Canada".

The numbers of people listed in each country were:

- **USA – 7,848**
- **Canada – 312**
- **Australia – 69**
- **UK – 39**

The rest of the people listed are reported to be from a variety of nations including: Belgium, Brazil, China, Estonia, France, Germany, Greece, Guatemala, Indonesia, Ireland, Israel, Italy, Jamaica, New Zealand, Trinidad and Tobago, South Korea and Sweden.

Vocativ last night refused to share further details of those named on the list.

Searches on the Telegram service on Wednesday failed to uncover any list - suggesting it had since been removed.

It is not clear if any of the information published was already available in the public domain or if it had been passed on to relevant authorities.

UCC has previously been criticised for 'taking credit for others' work' in a recent study by data and intelligence specialists Flashpoint.

An article in The Wall Street Journal last month claimed authorities were at odds over whether the lists pose an actual threat or are merely scare tactics. Mirror Online has contacted the Home Office for comment.

Terrorist groups working to paralyse cities with just one click, warns head of British intelligence

Source:http://www.christiantoday.com/article/terrorist.groups.working.to.paralyse.cities.with.just.one.click.warns.head.of.british.intelligence/88263.htm

June 14 – **What does it take to shut down an entire city? A nuclear bomb? Thousands of heavily armed troops? Or an epidemic?**

All these are possible, but there is another way. For the head of the British security and intelligence organisation, just one click of a button could be enough to shut down cities.

Robert Hannigan, the United Kingdom's Government Communications Headquarters (GCHQ) chief, warned that terrorists and rogue states are building up their technical capabilities to paralyse urban areas in an instant.

In a rare public appearance at the Cheltenham Science festival, the British intelligence chief said terror groups are planning to shut down big cities like London using the so-called "Internet of things"—the increasing

online connectivity of common things like cars and household appliances.

"There are certainly states and groups with the intent to do it, terrorist groups, for example, who have no threshold when it comes to the loss of life," Hannigan told participants of the festival, as quoted by The Telegraph.

"We're not quite there yet, but as the world becomes ever more connected that will become a greater risk," he added.

The head of the GCHQ further said that rogue states are actually developing the kind of cyber programmes that can be used to attack major cities. Terrorist groups, for their part, are looking at acquiring this technology.

"At some stage they will get the capability," he said.

With this in mind, Hannigan said intelligence services should step up surveillance of the Internet, saying that the U.K. has intercepted at least seven cyberattacks for the past 18 months.

In an opinion piece on Jihad Watch, columnist Christine Williams said the statements made by Hannigan do not bode well for the whole world in terms of security.

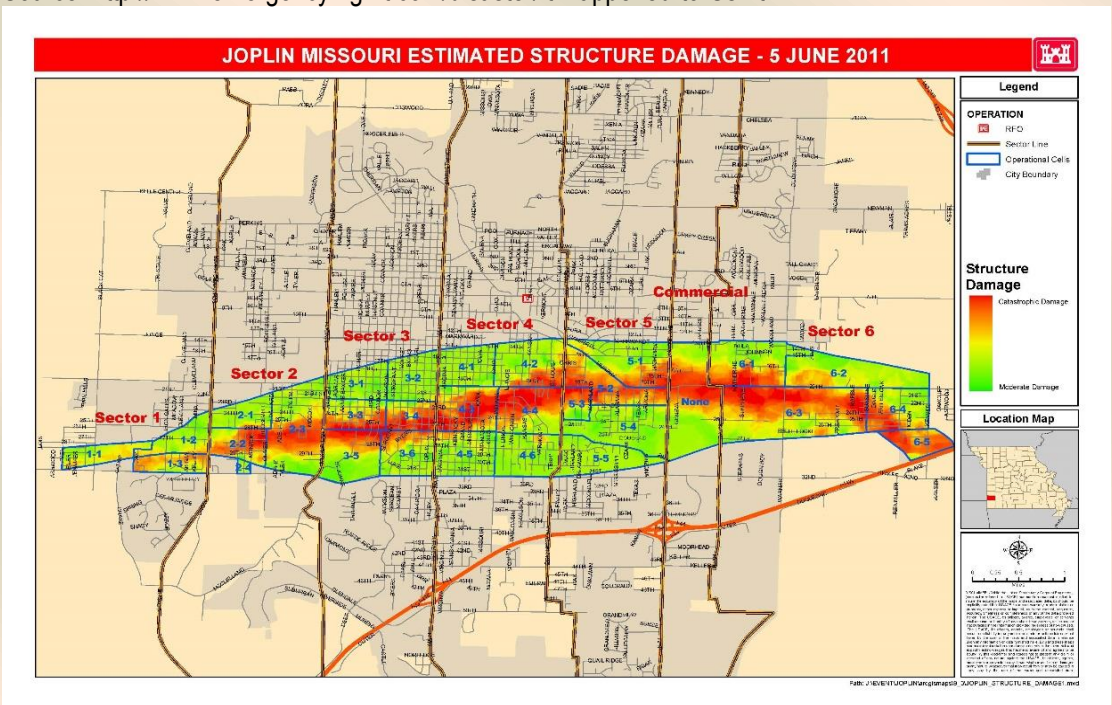
Williams said this means that terror groups like the Islamic State have already turned into "killing machines" that are "destructive without boundaries."

She further urged the United States to step up its vigilance against terrorism following the British intelligence chief's warning.

"In the words of al-Qaida leader Ayman al-Zawahiri: 'The first matter is striking the West and specifically America in its own home, and attacking their interests that are spread everywhere'," Williams said.

'It Happened to Us'

Source: http://www.emergencymgmt.com/disaster/It-Happened-to-Us.html



This spring will mark the fifth anniversary of the devastating tornado that struck Joplin, Mo., on Sunday, May 22, 2011. The tornado killed 161 people and caused nearly $3 billion in damage. Keith Stammer was the Joplin/Jasper County director of Emergency Management and is today. He talked recently about the recovery and lessons learned in Joplin.

This year marks the fifth anniversary of the 2011 tornado. How has the recovery gone?

Recovery is going pretty well; everything is cleaned up. We got that done in short order. The problem here is coming back with housing. Joplin has more rentals than it has homeownership, so we have a lot of low- and moderate-income people who need places to stay. If you've ever done that, particularly with state and federal tax credits, it takes a while.

We were warned that this would take some time, but I was hoping it wouldn't take as long as they thought. That being said, we've gained back what little of the population we lost. We actually have a few more residents than we had prior to the tornado, and unemployment is running under 5 percent. The other big thing that helped Joplin was that we basically live off sales tax and not off property tax, and the sales tax did not go down in terms of revenue. In fact, it went up because everyone wanted to rebuild. So that helped us from a financial standpoint in terms of not losing anything.

You have a long list of lessons learned from this event. Can you talk about a few of them?

For the first three years, you couldn't talk weather and not talk about the tornado. Most of what I have [learned] is from a response standpoint. There are also some lessons learned from a recovery standpoint this far down the road, as we're still in recovery mode.

One of the big things that helped us probably more than anything else is we had a standing COAD, Community Organizations Active in Disaster. We've had one since the tornadoes in 2003. We had two ice storms in 2007 and a Mother's Day tornado in 2008, so when the 2011 tornado came along, we had the COAD there that immediately formed a Long-Term

Recovery Committee, and they acted as the umbrella organization for all our different entities. We said, "If you're interested in rebuilding and recovery, we want to do this as a group." At the height of it we had 120 people representing 80 different organizations as members of our LTRC.
That has wound down and been dismantled and taken over by the COAD, which continues to meet every other month.

Emergency managers are traditionally more involved during response. What's been your role during the recovery?
If I have anything as far as my general role in this, it is to act as a resource to individuals and organizations. I have about 720 different contacts on my phone — companies, churches, clubs, nonprofits and whatever else. So when somebody wants to do something in terms of the recovery, I can step in and say, "Yes, I know who you need to talk to."
I participated in several group meetings on the recovery. One of the things the city did was form a Citizens Advisory Committee, whose job it was to go to the citizens and say basically, "We have this canvas that's been unpainted, if you will, that is three-quarters of a mile wide and six miles long. What do you want in here?"
It wasn't totally destroyed, but there were a lot of blocks after blocks of nothing. Do you want schools? What about zoning, churches, parks, running trails? All of a sudden businesses started saying, "We've always wanted to be located along 26th Street but there was never any property; now there is. Is that something the citizens are interested in?"

The hospital

And so [the advisory committee] produced a booklet with a lot of different ideas that was used as feedback to the city. Another thing we learned is that you can't depend on yourself in this kind of thing because who has this kind of experience, particularly on this scale?
People have asked me, "What's the dirt on this tornado? What really went wrong?" I've said, "We have experience in doing these things. The big thing that really grabbed us was the size of the event. We've had small tornadoes, ice storms and floods, comparatively — nothing of this size." We have had people from Springfield, Tulsa, Kansas City and other locations come in and work with our planning and zoning group, public works group and public information officer to help us, increase our staff load and also to gather information on experiences they've had.

What are a couple of major lessons that would have aided response?
First of all, let me emphasize that what we did in terms of response wasn't that much different from how we responded to other disasters that we've been through. It was just on

a larger scale. With that in mind, it's easy to get complacent when you're planning for an emergency response to whatever type of disaster you might have.

There are only two things you can do: run and hide. Running we call "evacuation," and hiding we call "shelter in place." We incorporate those in there, but if we had one failing prior to the tornado it was that we didn't think much beyond the past. We would have a tornado exercise or a hazardous release exercise, but it was based on what we had seen before.

I'm confident that if I walked into a disaster planning session with an EF5 tornado scenario in my back pocket that would have killed 161 and damaged 7,500 structures, I would have pretty much been told, "That's nice, but can we [work on] something that's actually going to happen?"

Another big thing that helped us is that relationships are key. In the first 72 hours after the tornado, there was nobody who came into my EOC in terms of agency head or department head who I did not already know. On a local, state and federal level, these were people we'd already worked with. One of the key elements that really helped with our communication among response personnel was the Incident Action Plan [IAP]. We ran 24/7 from Sunday through Friday night, then starting that Saturday, we ran 7 a.m. to 7 p.m. So we would have a meeting every day at 7 a.m., and our planning team had been working all night on the IAP so when people walked in, we had copies for them. "Here is today's weather, today's goals, etc."

I wished we had printed more so that the police officer standing on the corner for eight hours directing traffic could look through one and say, "I see what they're trying to do" and be able to point people in the right direction. We kind of assumed that would get pushed out to the individuals on the ground, but we could have done a better job of making sure that happened.

It's almost impossible to be totally prepared for something like that isn't it?

In emergency management, we participate in and we advocate for the all-hazards approach. In your standard National Incident Management System response and recovery, it's people first, scene second and property third. We felt like we were fairly well prepared. Confidence is that feeling you have just before you fully understand a situation. We had, like, nine different exercises in the 12 months before the tornado. In fact, the Wednesday prior to that Sunday we had a four-hour EOC ops tabletop exercise in conjunction with seven states for an earthquake along the New Madrid fault. That helped a lot as far as making sure everybody knew their role, how to respond to the EOC and how those things were going to work.

People used to say "that can't happen here," and now they don't say that anymore. I've had several emergency managers that have called me and said, "Can we have a map and outline or overlay of the path of the tornado?" And they've laid it over their own city because they know it happened in Joplin and it can happen there. They used that map for a tabletop exercise of how they would work things.

We continue to encourage builders and citizens that sheltering is a big deal. Many if not most of our schools, not just in Joplin but in surrounding areas, have applied for FEMA mitigation money on a 75/25 split that enables them to build storm shelters within their schools.

You have to adhere to certain building codes and standards, and most of this is low and moderate income. It's quite a labyrinth to work through state and federal regulations that touch on many of these things.

Now we're trying to raise the bar, but it's going to take some time — it's not something that's done overnight. The trick is to continue to not let the momentum sway you to the point where you get back into the old way of doing things, but continue to stand up and say, "Look, it happened to us. What are we trying to do to make things better?"

How do you continue to get that point across and not let momentum lag?

One of the things we use is the fifth anniversary, and we've used the other anniversaries. It's a chance for awareness. We do an annual weather education training within the city. Then I do about 20 different individual weather training sessions with churches, clubs, nonprofit organizations, governmental entities and such, and emphasize what happened and why.

Our planning and zoning departments continue to keep all this in mind and will for some time as they look at these new buildings that we want to put up, particularly for housing, and to say, "It happened to us and we've got to continue to hold tight and make sure we

don't go back to the way we were." It might be a bit easier for us having been bitten so hard as opposed to a community say 50 miles down the road that wasn't affected by it.

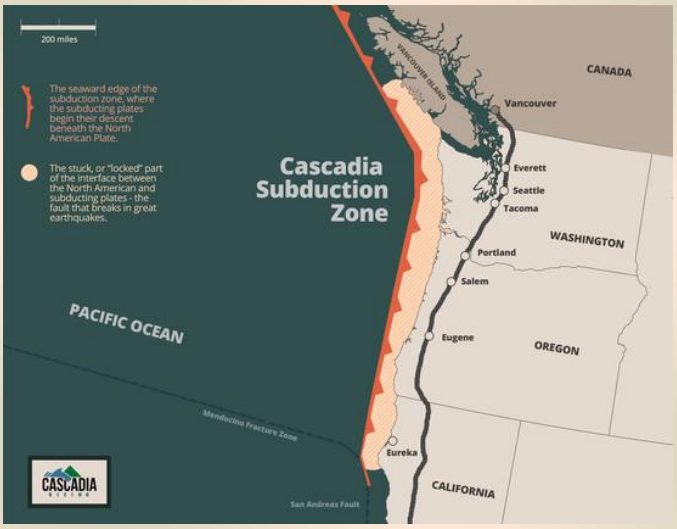
If Megaquake Destroys Docks, Navy Can Build its Own

Source: http://www.emergencymgmt.com/training/If-Megaquake-Destroys-Docks-Navy-Can-Build-its-Own.html

June 05 – **A Cascadia megaquake will devastate ports across the Northwest at a time when the region is in desperate need of supply shipments.**

Delivering cargo under difficult conditions is something the military knows how to do.

So that expertise is being tested this week, as Navy, Army, Marine and Coast Guard units from across the country participate in the biggest disaster drill in Northwest history.



The Cascadia Rising exercise is meant to simulate response to a monster earthquake and tsunami. With roads and airports heavily damaged, one of the best ways to deliver food, heavy equipment and other gear will be by water, Capt. Greg Vinci, of the U.S. Naval Construction Force, or Seabees, said Wednesday during a tour of several operations.

If ports, docks and piers are unusable, the Navy can make its own, Vinci explained.

"We provide that link from ship to shore."

At Naval Magazine Indian Island, a munitions storage depot near Port Townsend, the Navy has deployed several small landing craft and portable docks, called causeway ferries.

On Wednesday, crews loaded shipping containers on and off the vessels with fat-wheeled cranes designed to move cargo over rough terrain.

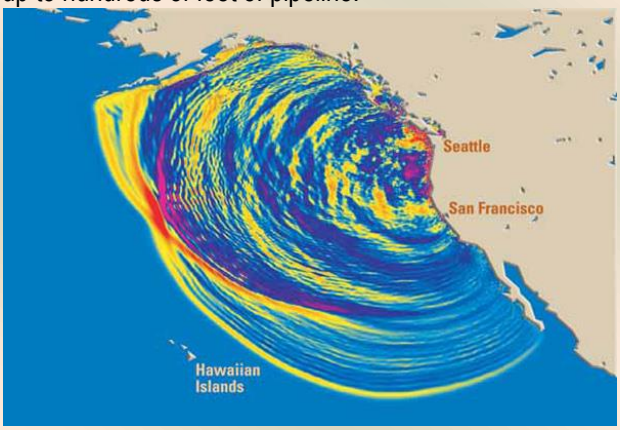
A 500-person encampment, with row upon row of green tents, supports the operation. The camp took about a week to set up, said Navy Lt. Andrew Anderson. The complex comes complete with portable showers, a kitchen, mess hall and diesel-powered generators to keep the lights and computers humming.

The vessels, camp gear and other equipment were shipped from Naval Base Coronado in San Diego on the **USNS Bob Hope**. The 1,000-foot-long ship is essentially a floating warehouse, with 380,000 square feet of storage space, Anderson said.

In war, the ship and others like it are used to deliver tanks, trucks and military supplies. In peacetime, the design is ideal for delivering humanitarian aid. Several similar ships, fully stocked with emergency supplies, are positioned around the globe, Anderson said.

Also being tested at Indian Island is a portable fuel-delivery system. The Inland Petroleum Distribution System provides bulk fuel storage and can serve as a kind of temporary gas station when fuel pipelines are severed — as expected in a Cascadia quake.

For the exercise, two 50,000-gallon bladders were laid out on the beach, filled with water, and hooked up to hundreds of feet of pipeline.



A full-scale system can cover 40 acres and has a capacity of 3.8 million gallons, said Army Staff Sgt. Christifer Graham. The pipeline can be extended up to 250 miles.

At the Port of Port Angeles, special teams from the Washington National Guard practiced the type of decontamination operations that will be needed after a major quake and tsunami.

Surges of 20 feet or more could hit the harbor on the Strait of Juan de Fuca, turning mills, factories, fuel tanks, cars and houses into a slurry of chemical-laden debris, officials explained. Much of the waterfront, which is built on fill, will also liquefy in the shaking. Fire and rescue crews and cleanup workers will all need to be decontaminated after being exposed to the mess.

A few hardy Guardsmen volunteered to be sluiced off Wednesday in a yellow shower tent erected on the muddy shore. Crews also practiced hosing down a firetruck.

Several Clallam County officials took a break from their own Cascadia Rising response drill to observe the operations.

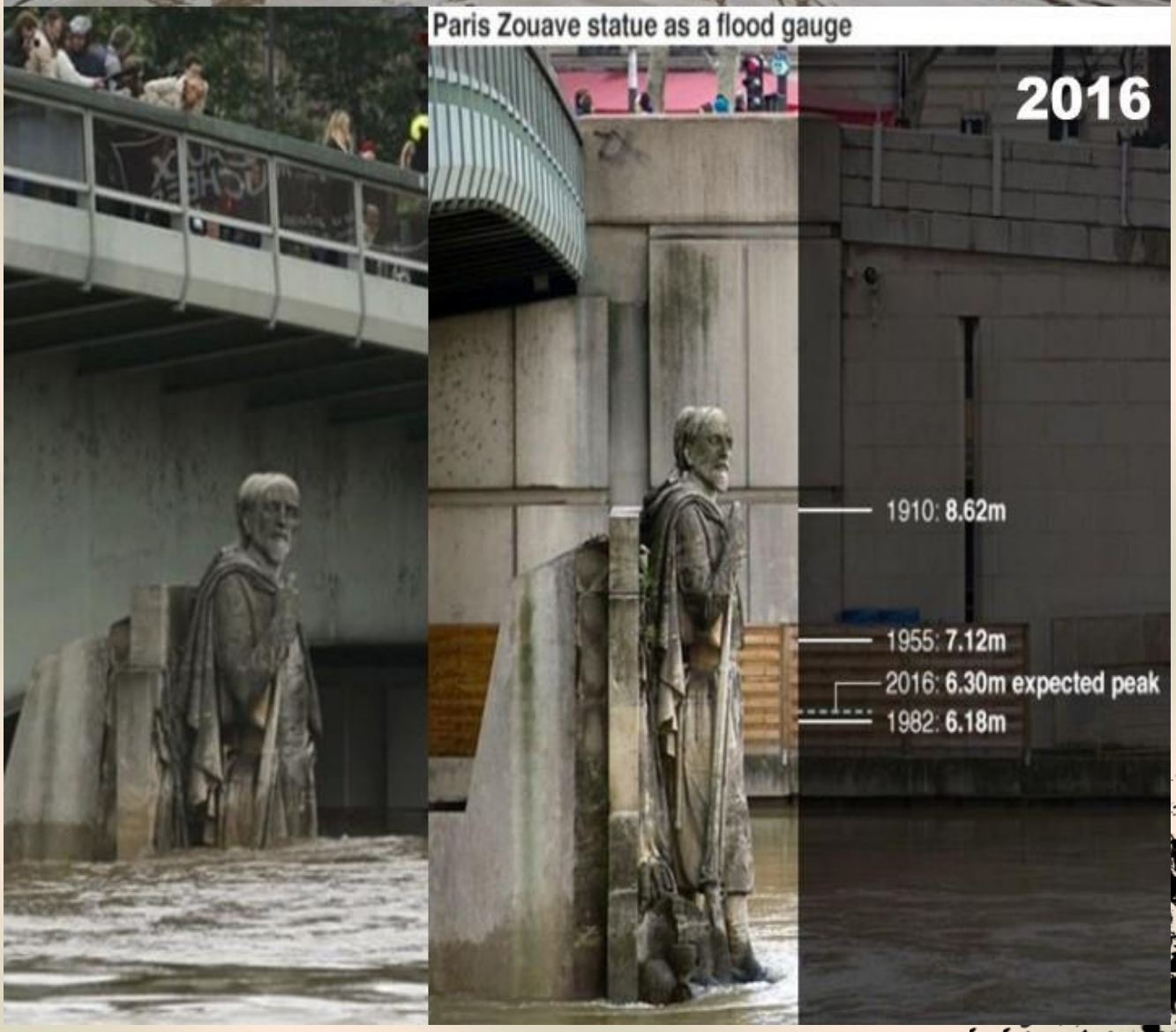
Penny Linterman, of Clallam County Emergency Management, said it will be great to have the military pitch in after a major disaster.

But even military resources will be spread thin after a Cascadia megaquake and tsunami, with devastation across Washington, Oregon and Northern California, she pointed out.

And military forces can be slow to mobilize. Setting up a full-scale network of temporary docks and vessels can take four to six weeks.

“The military can do amazing things,” Linterman said. “But it takes time.”


Because the unexpected always happens!


Paris Zouave statue as a flood gauge
2016
1910: 8.62m
1955: 7.12m
2016: 6.30m expected peak
1982: 6.18m

Working with Journalists During a Crisis

By Mark Hooper

Source: https://www.linkedin.com/groups/3798271/3798271-6141596144343531527

May 26 – During my years working in Corporate Communications at The Boeing Company, we had a number of high profile incidents and accidents that challenged the company and helped us understand ways to better manage our media relationships.

I always enjoyed the challenge of managing interactions between our corporate spokespeople and the media. Both sides have a job to do, and what we share is pressure, deadlines, and the delicate dance required to get a successful outcome, which I always enjoyed seeking to achieve.

During a crisis, journalists would prefer complete and total access to information, and media relations practitioners want to manage the information flow to get the story out while protecting the reputation of the company. Quite often, these respective positions are at odds. But, there are some "ins and outs" to develop effective working relationships with journalists in a crisis. Here they are:

In the midst of a crisis is not the time to get to know your key media. If you are meeting media contacts for the first time once a major incident is unfolding, you will struggle to align your mutual interests.The time to get to know your key media contacts is when you're in the midst of relative calm. Spend time understanding what your key media need, how they work, their personality quirks, and how to develop a working relationship that creates a sort of shorthand so that your respective expectations can be understood and managed.

Here's an example: At Boeing, if a journalist who worked the aviation beat called on a routine working day and asked for some information on how a thrust reverser works on an airplane, we would probably provide that information. However, if a Boeing airplane had just crashed, and there was speculation (for example) about the thrust reverser being the reason for the accident, then we would probably not provide that information. After all, why would we want to fuel the speculation that may have nothing to do with the accident? Obviously, that might confuse your media contact wanting to write that story. But, if you've already developed a good working relationship with the beat reporter, then having ground rules established in advance can help set expectations and lessen tense interactions.

Given the high stakes that emerge during a crisis, it is OK to not have "friendly" working relationships with key media contacts. Of course, having friendly relations is the goal, but that is not always possible. Some journalists/organizations prefer to cultivate "coolness" in the relationship so that it doesn't appear too cozy. Thus, they might strike a less than friendly pose day-in and day-out. That's OK. Your goal, and theirs, is to keep the relationship productive. Friendship is not required. I've found this type of relationship has limits, however, because caution built into the relationship precludes breakthrough communication. Some might refer to this as "trust." But, if that's how it is, then that's how it is.

Focused journalists are the norm during a crisis. Understand your own requirements thoroughly. Given their mission, journalists are trying to get a scoop, or story, first. Thus, they will do what is necessary to achieve their goals. As a BBC World News reporter said in a recent TV promo, "I will not take no for an answer." You should expect to feel pressured to provide information, context, data and insider company information so they can satisfy their objectives. Maintaining calm and understanding your own responsibilities will prevent possible mistakes. They have a job to do and so do you.

Ensure your spokespeople are familiar with the media, and have been properly trained. Again, preparing for a crisis in advance will allow you to effectively handle a crisis that is unfolding. Knowing your key media can help mitigate chaos. In day-to-day media relations, PR professionals are answering media queries and handling relationships and providing the "company story." But, during a crisis, it might require an executive spokesperson at the highest level of the company, who has little experience in dealing with the media during a crisis, to respond. Therefore, it is critical that the executive be trained and briefed properly in advance.

Here's an example: The British Petroleum (BP) oil spill in the Gulf of Mexico in 2010 is a classic example. The CEO, Tony Hayward, was ill-prepared to handle communications during a crisis and that was illustrated through the various wrong-footed statements made by Hayward. His classically inappropriate line, "There's no one who wants this thing over more than I do. You know, I'd like my life back", spoke volumes about his insensitivity towards stakeholders concerns. It also highlighted BP's misunderstanding about the stakes involved in engaging the media/public. Journalists love colorful speakers who create "news." Your job is to ensure the appropriate level of engagement is happening to protect the company.

Embrace the power of social media and media relations when working a crisis. Because social media is the fastest way to move, or to respond, to a story, then you must be prepared to anticipate how a story evolves and to use social media as a key communication channel.

Here's an example: It was a July 4, 2013 holiday weekend in America when an Asiana Airlines 777 crashed at San Francisco International Airport. We were amazed to learn a Samsung executive on board the flight from Seoul that crashed had sent a dramatic tweet after escaping the burning plane. His video went global in seconds/minutes. Media people began calling us at Boeing, and luckily, we were able to follow with a tweet confirming the event soon afterward, thereby providing our initial statement that media expected. Still,

because of the holiday weekend, and because of the speed of the passenger's tweet, our response only came about an hour after the crash happened, which wasn't bad considering our crisis communications team was on holiday.

Truly, the game has changed. Understanding social media, and using it to help you manage and anticipate events, and to respond to them quickly, is critical to telling your story. In our case, we had some "canned" social media holding statements ready to go and deployable as soon as practical. When dealing with social media, you need to imagine a story breaking, and going potentially viral, quickly. So, be prepared.

Over the past 25 years, CS&A International has been devoted to the mission of continuously enhancing our clients' crisis preparedness and resilience: we write crisis plans, conduct crisis leadership and crisis media communication training, coach senior executives and spokespersons and design crisis exercises. We can help your company and executives prepare, and manage your media relations and social media engagement optimally, to prevent a crisis from turning into a reputation train wreck.

Being prepared and having the knowledge that your organization's reputation is "in good hands" is a good place to be.

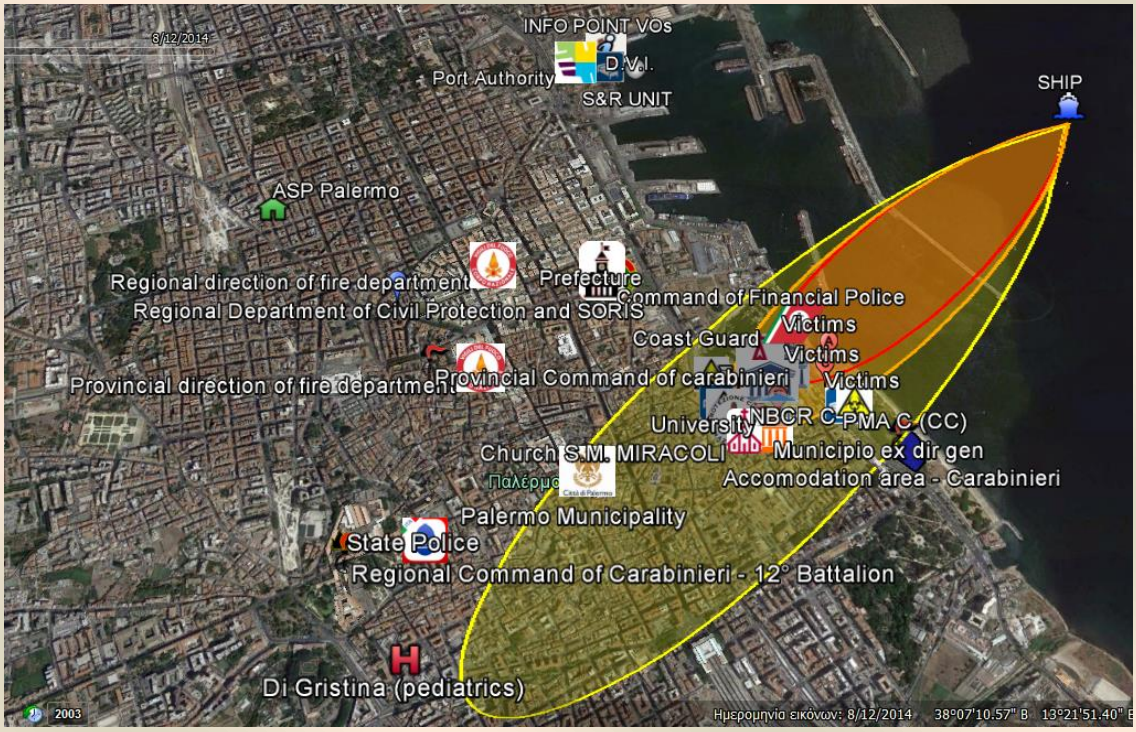
Mark Hooper *is an Associate with CS&A, based in Hong Kong. Mark most recently was Vice President – Communications & Marketing, Boeing Commercial Airplanes (BCA) for The Boeing Company, until October 2014, where he was heavily involved in corporate issues and crisis management.*

EU Project IMPRESS Palermo excercise

Source: http://fp7-impress.eu/index.php/news/37-impress-palermo-excercise

The **first IMPRESS DSS test and validation exercise, the "Palermo Demo",** took place in **Palermo**, **Italy** on 7 June 2016 under the auspices of the National Research Council of Italy in cooperation with the Civil Protection of Palermo.

The exercise scenario involved a fire on-board a cargo ship moored in front of the Palermo harbor, in the sea, right in front of the Palermo promenade. The fire was not able to be extinguished or placed under control and the captain and crew abandoned ship. Due to Northeasterly winds, there was a risk that the plume of toxic substances (burning plastics) released in the fire to affect the densely populated area of Kalsa District. Several victims were reported which need medical attention and transportation to nearby hospitals; essentially triggering a mass casualty emergency operation.



For the purposes of this exercise, installation, integration and testing procedures took place throughout the preceding week between 30 May to 5 June 2016. On May 31 2016 blended online and physical training of end users participating in the exercise took place at the premises of CNR with hands-on physical training taking place on June 6 2016 at the premises of the major Italian Agencies involved in the exercise.

For evaluation purposes, an Evaluation Committee has been established, and the participation of external observers has been confirmed. These teams include experts and representatives from the following organisations:

- Greek National Emergency Dispatch Centre (EKAB)
- Foundation for Interfacesof Engineering & Healthcare (WTTZ)
- IRCCS San Raffaele
- Bulgarian Ministry of Health
- SIMNOVA - Centro di Simulazione in Medicina e Professioni Sanitarie, Università del Piemonte Orientale
- Greek National Center of Health Emergency Operations (EKEPY)
- Greek General Secretariat for Civil Protection (GGPP)
- The postgraduate course on "Disaster Medicine and Health-Crisis Management" of the Athens University School of Medicine

IMPRESS

2016 Palermo Drill

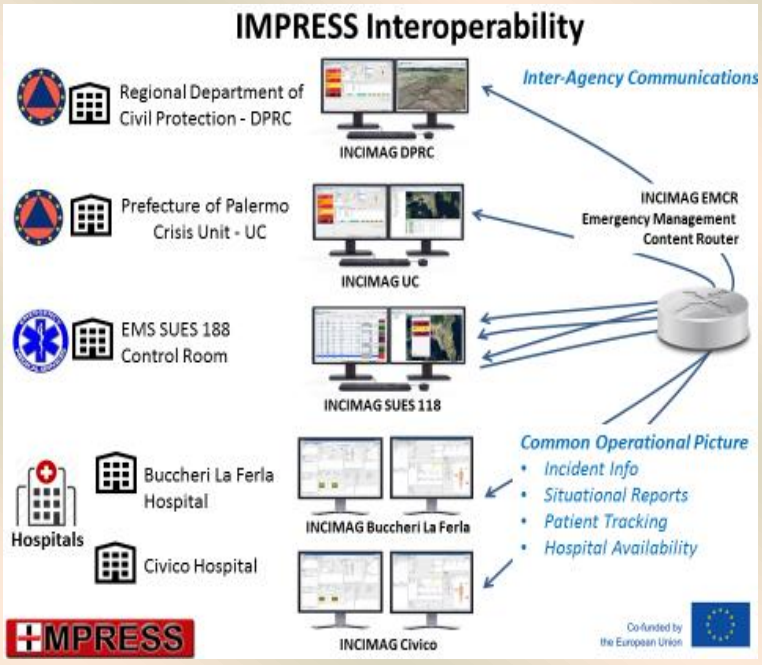
Editor of the Newsletter participated as Evaluator and member of the IMPRESS consortium (KEMEA)

The Italian Agencies involved in the exercise include:

- Regional Department for Civil Protection of Sicily
- Civil Protection Office of Palermo Municipality
- Civil Protection Office of Province of Palermo
- Palermo Municipality
- Prefecture of Palermo (local office of Ministry of the Interior)
- Coast Guard
- Command of Financial Police of Palermo
- State Police
- State Police, Section of Expert Crime Scene Investigation - DVI
- Regional Direction of Fire Department, Sicilia
- Provincial Direction of Fire Department, Palermo
- Provincial Command of Carabinieri
- 12° Carabinieri Battalion "*Sicilia*"
- 9° Helicopter Brigade Carabinieri
- Operational Air and Naval Command of Finance Guard
- Harbor Authority
- Corp of Forest Guards of Sicily
- Regional Agency for Environment Protection of Sicily
- Regional Department for Public Health (Body of Regional Government for public health)
- Health District of Palermo (ASP Palermo)
- Provincial Command of Italian Red Cross, Palermo
- Emergency Health Service (118)

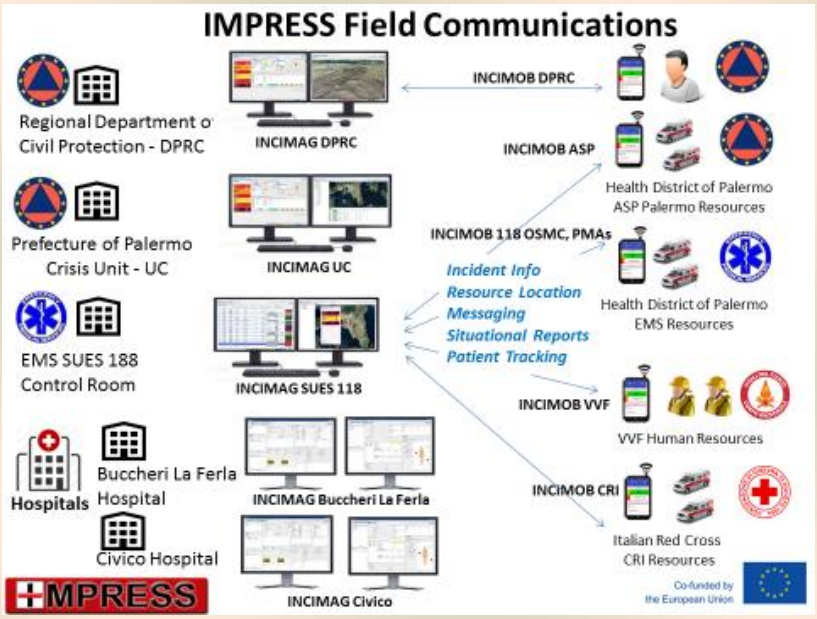
IMPRESS contribution to the trial

According to the planned tests the fire developing on-board the ship shall produce a toxic cloud which will spread over the Kalsa district due to the wind blowing from the North East. . IMPRESS modules will be activated at the Emergency Service, Emergency Department of local hospitals and at the National Health Service Operation center for managing the public health aspects of the incident. The Regional department of civil protection Agency (DRPC) coordinates the operations that will be supported by the various IMPRESS system modules as follows:



- WARSYS is accessed by authorized users of the involved authorities (NHS and EMS) to retrieve data concerning real time medical and logistics information.
- PATEVO shall provide a physiological forecast of patients' status evolution to the EMS and to the ED of relevant hospitals in order to support relevant decisions
- LOGEVO module will support at the NHS and EMS level the monitoring and logistics of health care resources

- Several independent INCIMAG installations will be used to manage the incident in a collaborative way, to produce a common situational picture and exchange it among the agencies involved. The INCIMAG installations shall be integrated with the mobile data terminals (INCMOBs) and the DSS tools in order to provide the correct information and support to the right people.

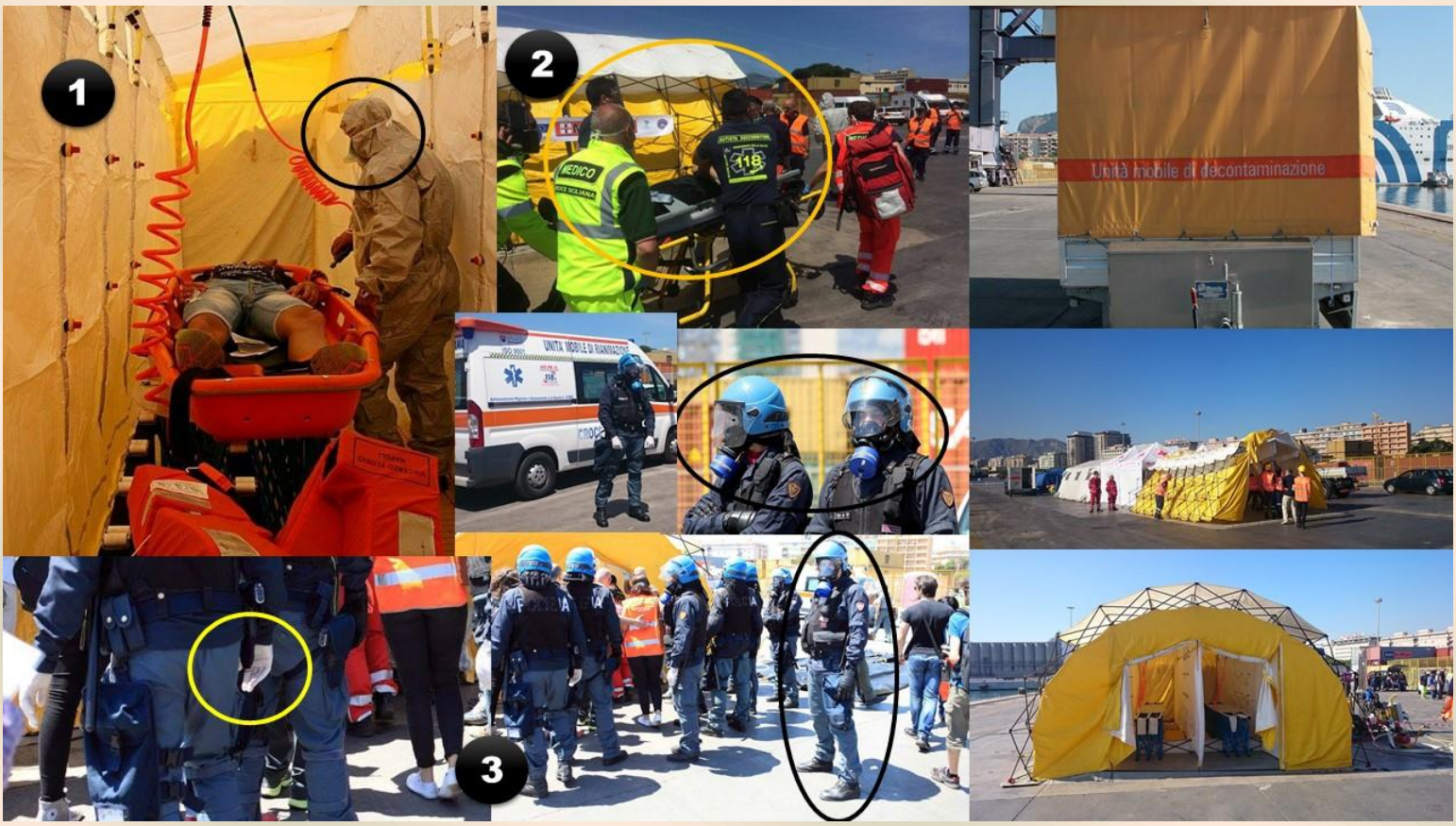


- INCIMOB mobile applications will provide field data collection and management support allowing the insertion of patient data, exchanging and recording of Triage data and displaying the actual situational picture

The Data Harmonization Component will provide harmonized data at the semantic level linking internal data with the necessary open web data (e.g. weather data or city block population data) to allow for enhanced situational awareness and decision support.

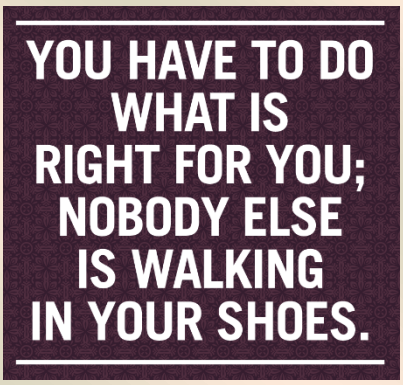
The decontamination component of Palermo Drill

Although the overall drill was successful, the chemical decontamination part was not as realistic as the overall multi-agency operation. Since the Editor was on a Coast Guard patrol boat and not on the dock where emergency response tents (including the "yellow" decon dacility) have been deployed, the study of related photos and videos revealed that there is a lot of work to be done in this specific sector of emergency response.Three examples below:



1. No gas mask by responder conducting wet decontamination;
2. Contaminated casualties were not received by first first responders dressed in PPEs – the photo reminds that outside St. Lukes hospital where doctors and nurses in plain clothing received the victims after the Tokyo subway sarin release (1995);
3. Wearing the ordinary police gear plus a gas mask with filter and some surgical gloves does not compose a PPE suitable to protect against chemicals (either CWAs or TICs).

It is crucial to remember that if we do not do things right during drill most certainly we will do it right in a real life emergency!



Balancing Risk – Understanding & Preparing for Catastrophes

By Catherine L. Feinman

Space weather, nuclear, and catastrophic natural disasters are just lying in wait for the right combination of conditions. Although it is not possible to plan specifically for every type of threat – imaginable and unimaginable – it is necessary to weigh the risks associated with various threats and take sufficient actions to mitigate the devastating effects.

On 27 April 2016, William (Bill) Murtagh, assistant director for space weather at the Office of Science and Technology Policy, Executive Office of the President, addressed leaders from government and industry to share updates on the National Space Weather Strategy and Action Plan and the related tasks and subtasks that are now being assigned to various federal agencies. The strategy urges all community stakeholders to plan and exercise for long-term regional and nationwide blackouts, which would have profound implications for business continuity and disaster planning. Successful mitigation requires a higher level of local community sustainability, especially in lifeline infrastructures such as power, communications, water and sewer, healthcare, emergency management, and law enforcement. High-impact incidents may make it unlikely for outside help to arrive within four days. Forty or 400 days may be more likely.

Source: http://www.domesticpreparedness.com/pub/docs/DPJJune16.pdf

Catherine Feinman *joined Team DomPrep in January 2010. As the editor-in-chief, she works with subject matter experts, advisors, and other contributors to build and create relevant content. With more than 25 years of experience in publishing, she heads the DomPrep Advisory Committee to facilitate new and unique content for today's emergency preparedness and resilience professionals. She also holds various volunteer positions, including emergency medical technician, firefighter, and member of the Media Advisory Panel of EMP SIG (InfraGard National Members Alliance).*