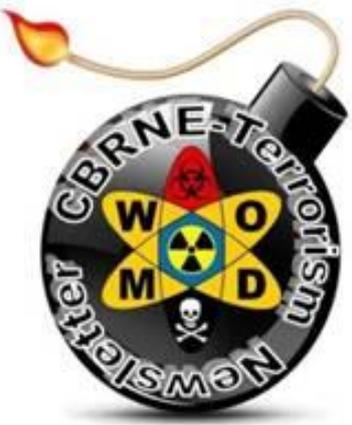


August 2014



CBRNE NEWSLETTER

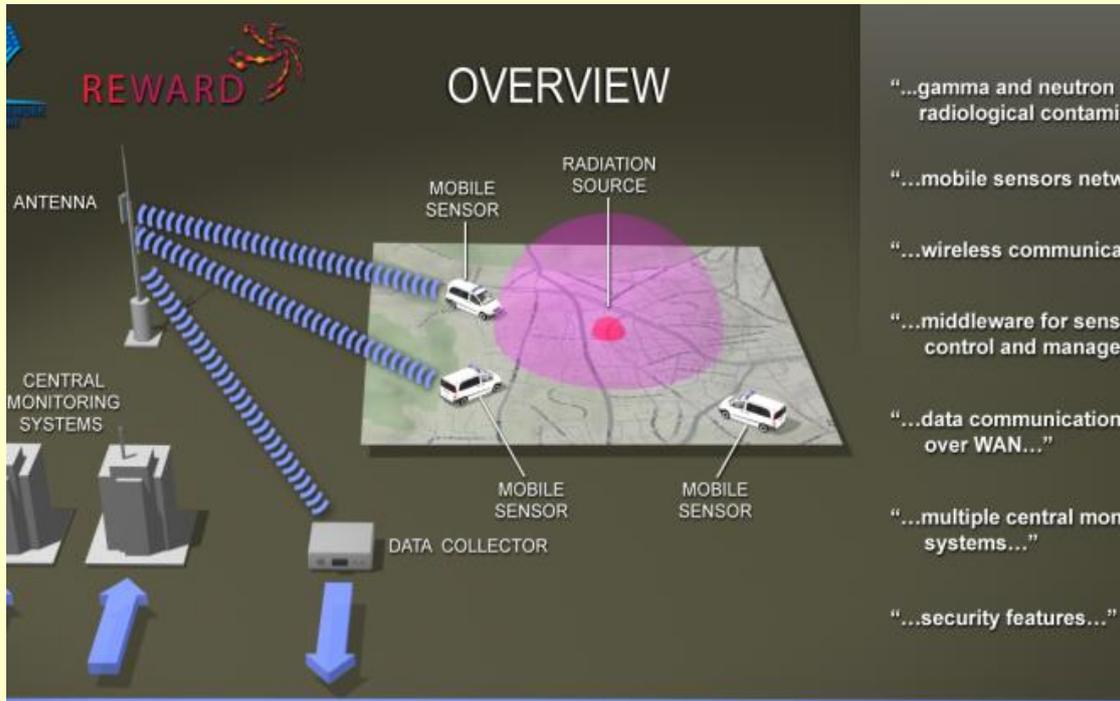
E-Journal for CBRNE & CT First Responders



REWARD Project: Security on the road

Source1: <http://www.cbrneportal.com/reward-project-security-on-the-road/>

Source2: <http://www.reward-project.eu>



Nowadays radioactive sources are widely used in medicine, industry and agriculture. Their security has become a growing concern, particularly the potential that such a source could be used as a radioactive dispersal device or "dirty bomb". The number of potentially dangerous nuclear transports is still high, as demonstrated by trucks containing radioactive material stopped on European roads (Austria, May 2013 – Italy, July 2013). Calls are so growing for more routine radioactive screening. Because of the high risk to citizens' health if these radiation sources are deliberately or accidentally manipulated (death is possible in less than one hour if the exposure is high), most Western Countries have deployed a set of detection systems and maintain communication networks in order to try to avoid their introduction and spread. However, these systems are mostly set-up at borders (roads, ports, airports and rail controls) and do not cover a large surveillance area but only zonal 'pinch point' sites. Moreover they are highly sensitive, expensive, of large dimensions and not at all portable. It is therefore imperative to explore alternative and complementary detection strategies to the systems already in place.

REWARD (Real Time Wide Area Radiation Surveillance System) is the name of a 3 years project, started in December 2011 and partially funded by the European Commission under the Seventh Framework Programme, developing novel mobile system for real-time, wide-area radiation detection and identification. The project brings together a consortium of eight institutions: three academic partners (Instituto Tecnológico e Nuclear, University of Freiburg and CSIC), two SMEs (Sensing and Control, XIE), two large companies (EDISOFT, Vitrociset) and one final user (Civil Protection Campania). Also three other final users (Spanish Guardia Civil, Civil Protection Catalonia and Italian Fire Brigades) are contributing as Advisory Board members. The final REWARD product will be a complete radiation monitoring system that can be installed to mobile transport (car, motorbike, trucks, trains, helicopter, etc.) or in buildings/infrastructures across a wide area. The scenarios range from nuclear terrorism threats, lost radioactive sources, radioactive contamination or nuclear accidents. The areas where the system has been deployed will be controlled in real time from a central remote control station. An expert

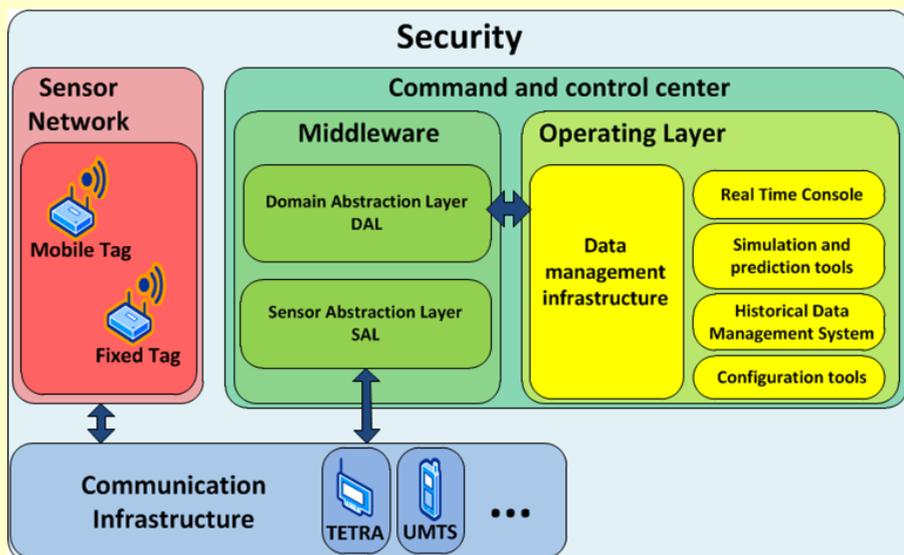


system will continuously analyze the sensor information received from the monitoring tags in order to detect risk situations not predictable through the analysis of data from isolated stations.

REWARD is based on the implementation of gamma radiation and neutrons detectors: one sensor is a CdZnTe detector for gamma radiation with precise energy measurement to identify the emitting isotope; the other sensor is a highly efficient neutron detector based on novel silicon technologies and a converter material. These detectors form the core of a sensing unit (or tag) which includes: a silicon-based neutron detector subsystem, a Cadmium-Zinc-Telluride gamma detector system, a processor to control the whole unit performance and link the data to the communications equipment, the battery system

REWARD's tags targets easy integration and deployment in emergency systems at different levels, self-adapting to in-vehicle communication systems (TETRA, GPRS, etc...) embedded in current emergency, fire or police vehicles. The communication systems will upload geo-referenced radiation information to a central server throughout its own middleware.

The REWARD system incorporates middleware and high-level software to provide web-service interfaces for the exchange of information and an expert system to continuously analyse the information from the radiation sensor and correlate it with historical data in order to generate an alarm when an abnormal situation is detected. Multiple sensing devices and the communication system are neatly coupled to a centralized processing module via a Sensor Abstraction Layer (SAL) component. Neutron and gamma count, collected by the sensors, are used to identify and to calculate the position of the radioactive source from the sensors' position, through algorithms based on geo-statistical techniques. The collected data are used to build a 2D/3D map of the radiations in the area of interest. A security framework is also developed to ensure protection against unauthorized access to the network and data, ensuring the privacy of the communications



and housing for the whole unit. A wireless communication interface is also integrated to send the data remotely to a monitoring base station as well as a GPS system to calculate the position of the tag.

REWARD tags are small, mobile, portable modular units in the sense that virtually any number of sensing modules in a network is feasible, allowing the flexible adaption of the system to the end user needs. They can be deployed in patrol vehicles, emergency units and in general in any type of mobile equipment. The first prototypes of REWARD sensing unit are now available for the testing campaign in a real environmental scenario (Naples, Italy) and the external communication unit based on GPRS technology is already implemented.

and contributing to the overall robustness and reliability of the REWARD system.

On 24th September 2013, REWARD project received a prize as the best Innovative project related to the Not Conventional Threat (NCT) Chemical Biological Radiological Nuclear explosives (CBRNe) products. A highly distinguished jury stated that "the developed detection and surveillance system offers a perfect solution for end-users to enhance crucial capabilities in RN analysis, risk communication and surveillance in case of a radiation incident". During a spectacular ceremony, hosted in Aloft Hotel grand ballroom in Kuala Lumpur (Malaysia), the winners of the first edition of the NCT CBRNe Awards were announced and REWARD project was granted the NCT CBRNe



Innovation Award for the most innovative product, service or research paper. During the first field tests for the monitoring of radiation, held in Naples on 12th 15th May 2014, the CBRN group of the Italian Fire Brigades deployed the REWARD mobile units inside the cars, provided by the Civil Protection of Campania Region, and two radioactive

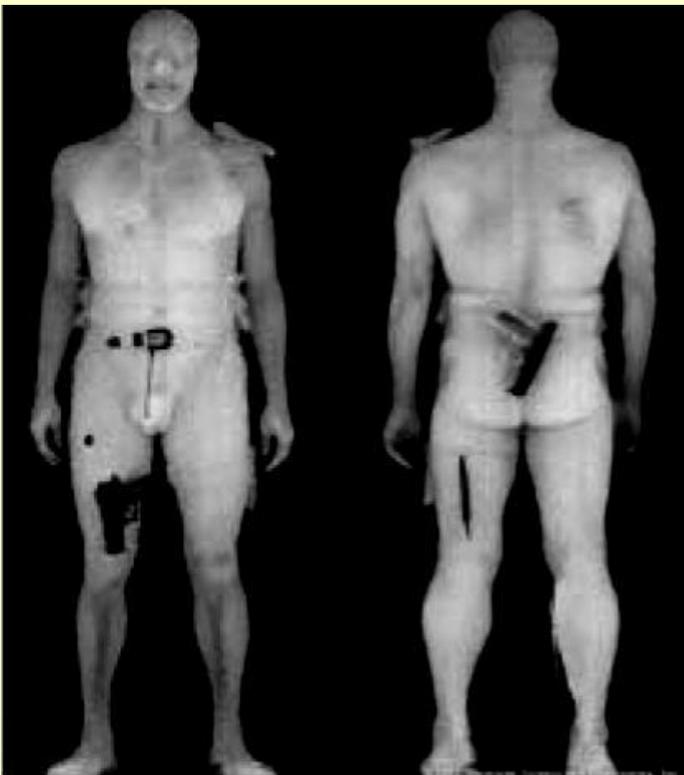
sources (60Co and 226Ra) were placed in a controlled environment inside the Fire Brigades Headquarter. During the field tests the radioactive background of the area was measured, the radioactive sources were detected and identified with their characteristic spectra and an alarm was forwarded and notified to the operator.

Backscatter body scanner making a comeback

Source: <http://www.homelandsecuritynewswire.com/dr20140729-backscatter-body-scanner-making-a-comeback>

Airline passengers have already said bon voyage to the controversial backscatter X-ray security scanners, pulled from U.S. airports in 2013 over concerns about privacy and potential

backscatter machines were in compliance with applicable national and international safety standards. A NIST release reports that to evaluate these results, as well as similar



radiation risks. The devices may, however, be reintroduced in the future, in part because they produce superior images of many concealed threats, and Congress still wants to know whether these systems — currently used in prisons, in diamond mines, and by the military — produce safe levels of radiation for screeners and the people they screen.

Two years ago, researchers from the National Institute of Standards and Technology (NIST) in Gaithersburg, Maryland, produced a report stating that the radiation exposure levels produced by one widely used class of

findings at other institutions, Congress ordered an independent third-party assessment of the backscatter systems to be carried out by a team selected by the National Academy of Sciences (NAS). Last week, NIST hosted the NAS study at the Gaithersburg campus, in a lab that contains a government-surplus backscatter machine that once screened passengers at LaGuardia Airport. Government agencies regularly ask the National Academies to conduct in-depth studies, says Erik Svedberg, senior program officer of the NAS National Materials and Manufacturing Board and study director for the NAS assessment of the scanner.

“As an independent not-for-profit organization, the National Academies can take a look at almost any issue within their purview without having a ‘stake in the game,’” Svedberg says.

The NAS group will be using the same model of scanner that NIST used to make its measurements — a Rapiscan Secure 1000 that was widely used to screen passengers at airports around the nation. NIST’s scanner is one of very few available machines in the country that is not either in storage or active use, says NIST researcher Lawrence Hudson, co-author of NIST’s original 2012 report.

Unlike the radiation used in the millimeter-wave whole-body scanners



currently used in airports, the radiation in backscatter X-ray scanners such as the Secure 1000 is ionizing.

Ionizing radiation can disrupt chemical bonds and, above certain exposure levels, has been shown to be associated with risks of cancer. However, “we live in a sea of radiation,” Hudson says, with natural sources of ionizing radiation including cosmic rays, bananas, and minerals that can appear in products such as cat litter. “So in order to assess relative risk, researchers need to accurately measure the exposures from such systems and compare those measurements to other exposures to ionizing radiation,” he continues.

For comparison, a person’s typical daily “effective whole-body dose” from natural sources is about 1,000 microrem (μrem) or, in SI units, 10 microSievert (μSv) — both units for measuring radiation absorbed dose. An airplane flight from New York to LA adds an extra 4,000 μrem (40 μSv) to a passenger’s daily dose. The 2012 NIST analysis indicated that the dosage from a single screening with the Secure 1000 scanner is 1.26 μrem plus or minus 0.08 μrem (12.6 nSv plus or minus 0.8 nSv).

All X-ray sources penetrate as well as scatter, or reflect, when they encounter tissue. Instead of collecting the transmitted X-rays as one would for a medical image, however, these scanners collect the X-rays that backscatter from the skin. Usually the machines collect two images, one from the front and one from behind.

The Rapiscan Secure 1000 is a single-pose system. To be scanned, a person stands between two units, each of which houses a moveable X-ray source that travels up or down inside the unit.

The X-rays from the source fly through a horizontal slit that produces a flat, fan-shaped beam, then encounter a spinning wheel with notched edges. The notches further reduce the output to a small, square beam of X-rays that scans the subject line by line like a fax machine. This “flying spot” of X-rays goes through clothing, bounces off skin, and is collected by a series of large-area X-ray detectors inside the scanner.

“It’s a really clever way to acquire a well-resolved image of an object or a person with very little exposure to radiation,” Hudson says. The X-ray “spot” spends only a few tens of microseconds on each part of the body. The

resolution of the resulting image is determined by the size of the small spot, not that of the detectors whose large size simply helps to increase the sensitivity.

In their 2012 report, the NIST team used radiation detectors to create a 3-D exposure map showing levels of radiation in the inspection zone, the space between the two scanning units where a person would stand. Hudson and colleagues then used this exposure map to estimate how much dose a person would get to their whole body as well as individual organs, particularly the skin and eyes.

Unsurprisingly, the skin gets a higher dose of X-rays than an organ inside the body. However, Hudson says, skin is one of the least radiosensitive organs. The calculation of “effective dose” takes that into consideration to produce a number used by regulators to determine compliance with safety standards. Using three different approaches to estimate effective dose to various organs, NIST scientists found that these numbers are well within the limits recommended by the National Council on Radiation Protection and Measurements (NCRP) and the International Commission on Radiological Protection (ICRP). For example, it would take 465,340 scans in a year to reach the annual recommended limit for the skin and 139,602 scans to reach the recommended limit for the eye.

The NAS report is scheduled to be ready by end of the year or the beginning of 2015, Svedberg says. Meanwhile, NIST has re-assessed the measurement techniques and tools that researchers have been using to measure a rastered source of X-rays like that used in the backscatter technique. It is tricky to extrapolate the dose levels as a function of distance produced by the various implementations of X-ray backscatter systems, Hudson explains, because the X-ray sources aren’t stationary; instead, they are spatially translating and in some cases also rotating throughout a scan.

“If you want to compare studies measuring the radiation levels of such machines, you need to be able to correctly extrapolate to different stand-off distances to see if results are consistent,” Hudson says. “This has not been widely appreciated in the studies published so far and has been one source of confusion.”



In a forthcoming article in the *Journal of Research* of NIST, Hudson and colleagues conclude that the tools commonly used in radiation dosimetry, if properly applied and interpreted, are entirely adequate to determine radiation levels and rates for security-screening systems that employ the backscatter method. He explains, however, that neither the measurements of NIST nor the NAS team are

intended to assess the safety of backscatter X-ray scanners directly.

“NIST is not in the business of declaring such systems safe or unsafe,” Hudson says. “Our role is to inform the public debate by measuring the exposure levels absolutely, validating the measurement tools and methods, and assessing the uncertainties.”

— Read more *J. L. Glover et al., Assessment of the Rapiscan Secure 1000 Single Pose (ATR version) for Conformance with National Radiological Safety Standards (NIST report for the TSA, inter-agency agreement HSHQDC-11-X-00585, 28 September 2012)*

Bulgaria Signs Deal With Westinghouse on Nuclear Power Plant

By Sean Carney

Source: <http://topics.wsj.com/person/A/biography/7734>

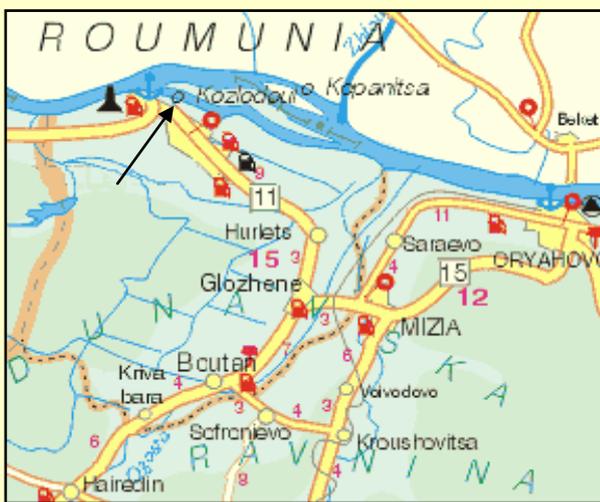
August 01 – An American nuclear engineering company and Bulgaria Friday reached a long-

The project will be a major employment booster in the EU's poorest member state by economic output per capita. The company said during the construction phase some 3,500 local workers will be employed on site with an additional 15,000 workers involved in the associated supply chain. Once the reactor is complete, it will employ up to 800 specialists. Within the next year, Westinghouse will issue a tender for the plant construction in line with EU and Bulgarian public procurement legislation, a process that is expected to involve Bulgarian and global construction companies.



sought deal paving the way for the European Union state to diversify its energy generation and nuclear fuel sources away from Russian to Western technologies while meeting the EU's strict carbon-emission reduction targets.

Pennsylvania-based Westinghouse Electric Co. Ltd. said after seven months of negotiations it signed an agreement with Bulgaria's state-owned nuclear power plant operator Kozloduy Nuclear Power Plant PLC giving the American company a 30% stake in a project company that aims to build a new 1,000 megawatt reactor worth over \$5 billion. Westinghouse will provide all of the plant equipment, design, engineering and fuel.



The deal comes amid a period of pronounced political turmoil in Bulgaria, where the cabinet resigned in July after being in office little more than one year. Next week a caretaker government will be appointed to lead the country to early parliamentary elections in October.

Michael Kirst, Westinghouse vice president for Central and Eastern Europe, said all major political parties were consulted on the deal, and additional agreements are subject to approval by the country's future governments. U.S. officials said the deal is an opportunity to expand economic and commercial ties between the U.S. and Bulgaria.

"Today's agreement between the Kozloduy Nuclear Power Plant and Westinghouse exemplifies international partnerships that advance important interests of both Bulgaria and the U.S.," U.S. Secretary of Energy Ernest Moniz said.

Bulgaria enjoys long cultural and economic ties with Russia and currently there are two Russian-designed reactors in operation at the Kozloduy facility in northern Bulgaria along the Danube River. The country is also reliant on Moscow for gas and oil supplies.

The European Union for several years has urged member states to diversify energy suppliers to reduce dependence on Moscow, a request that is finding new urgency amid the Ukraine crisis and increasing levels of Western sanctions on Russia.

In this light, both the previous right-leaning government and the current outgoing left-leaning cabinet have worked with Westinghouse, majority-owned by Japan's Toshiba Corp., to strike a deal for an alternative energy supplier.

Bulgarian Energy Minister Dragomir Stoynev Friday said developing the country's energy infrastructure is a long-term issue that requires sustained efforts of multiple governments.

Financing terms, design, licensing and construction details still need to be worked out and approved before construction can begin. The investors hope to bring the new reactor on line around 2022.

Westinghouse's stake in the project company during construction incentivizes it to build a plant that meets international and Bulgarian safety standards, is on schedule and within budget, the company said, adding that once construction is complete it will divest its stake so Bulgaria is sole owner of the asset.

Mr. Kirst said a full analysis of the competitiveness of the envisioned reactor, namely whether it is economically viable in future in a period when wholesale electricity prices are at historic lows, will be undertaken. All required preliminary work should be completed by next summer, at which point Bulgaria and Westinghouse together will be able to make the final decision whether to build, he said.

Financing for the planned reactor will probably come from export banks in the U.S., Japan and possibly the United Kingdom, Mr. Kirst said.

This agreement comes as EU state Hungary earlier this year made a deal with Russian nuclear company Rosatom in which the Russian side will fully finance the development and construction of two new reactors at the PAKS nuclear power plant in Hungary at a cost estimate to be in excess of €10 billion (\$13.39 billion).

Sean Carney is a reporter for The Wall Street Journal based in Prague. Sean is an avid skateboarder and a member of the Czech Volunteer Firefighters Association.

Complimentary Report Detailing the Consequences of a Radiological Dispersion Device Using Cobalt 60

Source:http://www.domesticpreparedness.com/Industry/Industry_Updates/Complimentary_Report_Detailing_the_Consequences_of_a_Radiological_Dispersion_Device_Using_Cobalt_60/

RDD's or 'dirty bombs' result when a terrorist uses an improvised explosive device (IED) to spread radiological material. The consequences of such a device are both the blast damage resulting from the explosive device itself as well as the distribution of

radiological material that could affect responders and the public. RDD's should not be mistaken with nuclear weapons. Nuclear weapons have greater explosive, radiation, and radiant heat destructive capability by orders of magnitude than





a 'dirty bomb', and they also spread radiological material referred to as 'fallout'. The brief entitled 'Radiological Dispersion Device using Cobalt 60' details the explosive effects of different IED's as well as the dispersion of radiological material based on wind direction using the 'RDD' and 'Explosives' modeling tools from their PEAC-WMD software.

Cobalt 60 was chosen as the topic substance for this brief due to the theft of a truck transporting the material from a Mexican medical facility in late 2013. It is thought that radiological isotopes used in medical applications would be the most likely target by terrorists when attempting to construct RDDs. The substance remained missing for several days, but was recovered along with the stolen truck when it was found abandoned in a Mexican field.

"Dirty bombs have been a topic of concern in the responder community for quite some time," stated Bruce King, CEO of Aristatek. "After the theft of the Cobalt 60 in Mexico, we had a lot of inquiries from our customers about how we could help them with planning for dirty bombs."

One of the scary revelations in the brief is the reminder that with a substance like Cobalt 60 having a half-life of 5.3 years, the area exposed to this exploded substance would have to remain uninhabitable for many years allowing sufficient time for radiation to reach suitable levels unless costly clean-up measures are employed. The brief also contains useful tables on gamma radiation exposure and radiation health damage that can be used by responders for planning a response to a similar incident.

"Hopefully this brief, and our 'RDD modeling' tool that is in a beta stage for our PEAC-WMD software are resources that can help responders prepare and train for an RDD incident," continued King.

This latest technical brief from AristaTek is a follow-up to their other popular briefs titled 'Ammonium Nitrate Estimated Blast Effects' released in September 2013, 'Toxic Consequences of Smoke Plumes from Crude Oil Fires' released in January 2014 and 'Acetyl Fentanyl – A Dangerous Street Drug' released in March 2014. These briefs can also be requested by visiting the company's web site.

▶ The document is available to those that request it at the Company's web site (<http://www.aristatek.com>). **The only problem is that it is available only (?) to US readers.**

New Handheld Radiation Detector Offers Enhanced Threat Detection, Identification

Source:http://www.domesticpreparedness.com/Industry/Industry_Updates/New_Handheld_Radiation_Detector_Offers_Enhanced_Threat_Detection,_Identification/



Security professionals who are responsible for ensuring public safety by detecting, locating and identifying radiological threats can now simplify and accelerate their work using a new handheld radiation detector with nuclide identification capabilities.

The instrument, the Thermo Scientific RadEye SPRD (Spectroscopic Personal Radiation Detector), builds on the success of previous generations of Thermo Scientific radiation detectors by adding a new operation mode for identifying nuclides. Equipped with a 1,024 channel analyzer, the RadEye SPRD gives non-expert users the ability to perform initial identification of radioactive materials found in the field. Thermo Fisher Scientific designed this next-generation handheld instrument to easily detect and identify common nuclides of



interest – including cesium-137, cobalt-60 and more.

“In security situations involving radioactive materials, quickly and accurately identifying the precise nature of the threat is mission critical,” said Bernd Friedrich, product line manager for radiation measurement and security instruments, Thermo Fisher Scientific. “The RadEye SPRD represents our continuing commitment to ensuring that the professionals responsible for keeping the public safe from radiological threats always have access to the best tools possible.”

In addition to its nuclide identification capabilities, the RadEye SPRD offers:

- An expansive library of nuclides of interest, which allows a security team leader to create custom alarm profiles for their team;
- The same easy-to-use, portable design common to the Thermo Scientific RadEye instrument platform, which has been trusted by security professionals for years; and
- Sophisticated software that allows the instrument to distinguish between background radiation and nuclides of interest automatically.

Y-12: Poster child for a dysfunctional nuclear weapons complex

By Robert Alvarez

Source: <http://thebulletin.org/y-12-poster-child-dysfunctional-nuclear-weapons-complex7361>

In early June 1995, while I visited the Y-12 nuclear weapons plant in Oak Ridge, Tennessee, a small aircraft flew over the site, dropping about 100 leaflets that local police described as “pornographic” and



“libelous.” Word had it that a spurned lover had decided to get even by depositing sexually explicit photos at a Y-12 employee’s workplace. Witnesses reported the plane dove to 150 feet above the weapons plant, in violation of federal aviation rules.

At the time, I was an advisor to Energy Secretary Hazel R. O’Leary, and it disturbed me that this stunt was treated merely as a racy instance of littering. I had just toured the site’s main storage facility for highly enriched uranium (HEU)—a 51 year-old wooden warehouse manifestly unsuited to store highly flammable fissile material. A fire at the warehouse, which contained one of the largest stores of weapons grade uranium in the world, could have meant a national radioactive disaster; the ability of a small

airplane to fly over Y-12 graphically illustrated how vulnerable the site was to aeronautical accident, or attack.

The United States halted production of new nuclear weapons in 1989, with the end of the Cold War. But the US nuclear weapons complex—composed of eight key facilities that have an annual budget exceeding \$8 billion—has stumbled on, in the form of a massive, decaying



empire that in many cases does its work poorly or dangerously, or both. The Y-12 National Security Complex is the poster child for much of what ails the weapons complex. Although Y-12 has not produced weapons for some 25 years, its annual budgets have increased by nearly 50 percent since 1997, to more than \$1 billion a year.

For decades, the Energy Department—which manages the weapons complex through the National Nuclear Security Agency (NNSA)—has not been able to reconcile competing objectives at the 811-acre Y-12 site, whether they involve storage areas for HEU and other fissile materials, the restarting of old weapons facilities, environmental cleanup, the building of new weapons facilities, or the downsizing of the site. As a result, costs have significantly increased, and long-standing problems have continued, unresolved, for years that have run into decades. For every dollar spent to maintain and modernize the US nuclear weapons stockpile, nearly three dollars is spent “to provide the underlying infrastructure” for maintenance and modernization at Y-12.

Long-term secrecy and isolation have created a dangerous form of hoarding at Y-12; a panoply of severe hazards continues to build up, constantly awaiting ever more costly mitigation in the future. But the stark reality is that there are no more cans to kick down the road. Y-12 has inexorably caught up with its future. Its environmental and security problems are too threatening to leave unaddressed, and questions about its mission will have to be answered definitively in an age of budgetary austerity and relatively little need for new nuclear weapons.

A historic mission, now history

Construction of the Y-12 complex began in 1942 in Bear Creek Valley, nestled between the Great Smoky Mountains and the Cumberland Mountains, about 18 miles from Knoxville, Tennessee. Its primary mission at the time was to produce sufficient quantities of uranium 235 for the Hiroshima atomic weapon. During this period, some 50,000 people were employed to operate electromagnetic separation facilities (calutrons) designed by nuclear physicist Ernest O. Lawrence and his research team at the University of California. “By any scale, the operation there was mammoth,” historian Gregg Herken wrote in his 2002 book, *Brotherhood of the Bomb*. Two 500-tank calutron “race tracks” were installed “each measuring four football fields long.” By 1946, the uranium-enrichment operation was shifted to the Oak Ridge K-25 Gaseous Diffusion Plant, sharply curtailing the calutron operations.

In 1949, the Y-12 plant began a significant transformation, becoming a major center for the processing of nuclear and other materials and the fabrication of nuclear weapons components during the Cold War. Over time, the plant acquired foundry operations for shaping highly enriched uranium and depleted uranium, production facilities for lithium used in nuclear weapons, weapon-component fabrication and dismantlement operations, and storage facilities for a variety of materials used in the manufacture of nuclear weapons. In addition to building several types of fission warheads, Y-12 produced the components for

the canned sub-assemblies (CSAs) used in US hydrogen bombs. CSAs contained the highly enriched uranium, lithium deuteride, depleted uranium and other materials that are squeezed to about one-thirtieth of their size and heated to the temperature of the sun’s surface by the fission detonation that triggers hydrogen bombs. More than 70,000 weapons components have been made at Y-12 since the late 1940s.

During its heyday, Y-12 produced some 1,000 CSAs per year. Now, its annual production capacity has dwindled to less than 100. Though the NNSA declares that Y-12 has multiple missions, including non-proliferation efforts that involve the downblending of HEU and the provision of fuel for the Navy’s nuclear-powered submarines, nearly 99 percent of its budget comes from funds dedicated to maintain the US nuclear weapons stockpile. More than anything, Y-12 serves to stockpile thousands of CSAs from discarded nuclear weapons, as well as depleted uranium, lithium, and other hazardous chemicals.

Because Y-12’s historical role—producing the components for vast numbers of thermonuclear warheads—has largely vanished, the NNSA has made a number of attempts to stretch the national security mission of the complex, and some of those attempts also stretch the boundaries of imagination. Meanwhile, the Government Accountability Office finds that “NNSA’s decision to retain many CSAs ... poses significant challenges to Y-12’s ability to plan its disassembly workload.” Although exact numbers



have been classified since the 1990s, there are likely several thousand excess CSAs, containing hundreds of tons of HEU, awaiting dismantlement at Y-12.

Problems, unaddressed for years and years

In the aftermath of my 1995 visit to Y-12, nuclear weapons officials in the Energy Department did their best to stall a planned vulnerability assessment of the department's highly enriched uranium storage operations, mainly because of the large potential cost of fixing problems at Y-12. Hundreds of tons of HEU were stored at Y-12 then. Just a year earlier, Building 9212, Y-12's main uranium processing facility, had been shut down as a result of serious safety violations uncovered by the Defense Nuclear Facility Safety Board (DNFSB). This setback renewed serious discussion in Energy Department headquarters of closing Y-12 altogether. The discussion proved to be idle chatter. The impacts of closing Y-12, which has dominated the wage and benefit structure for several generations in east Tennessee, was not lost on the White House, mindful of the 1996 elections.

Around New Year's Eve of 1996, a long-awaited vulnerability assessment of HEU storage at Energy Department sites was released. Y-12 had the most significant problems. Even though fires posed the greatest danger of radiation and chemical exposure to workers and the public, buildings, mostly constructed in the 1940's, had deteriorated and had insufficient or non-existent fire-protection systems, despite the very real possibility of a truly catastrophic fire and resulting release of radiation. It wasn't until 14 years later that a replacement facility for the aged wooden structure serving as the main HEU storage warehouse was opened; it cost five times the original construction estimate. That facility gained notoriety in August 2012, after nonviolent peace protestors, including an 84-year-old nun, penetrated its security barriers.

Making matters worse, there was a backlog of more than 100 tons of "combustible in process materials" that had accumulated in "virtually every building." Containers holding unstable and flammable forms of HEU sat for decades in hallways, narrow production aisles, and in process lines. Inspectors found that the site's overall safety plan "often does not contain such fundamental information as the physical forms, storage configurations, or inventories of HEU

assumed to be present in the facilities; and, therefore, were not evaluated for potential releases during major accident scenarios." And more than 60 percent of the many thousands of containers holding HEU had never been opened and lacked documentation as to what was inside.

To its credit, the Defense Nuclear Facility Safety Board has played an important role over the past 20 years in improving safety at Y-12 and continues to pressure the NNSA to come to terms with problems there. Several improvements have been made, particularly regarding the removal of unstable nuclear material from deteriorated structures, safer packaging of nuclear materials, upgrading fire protection, and establishing a formalized safety culture.

But these improvements haven't come close to eliminating Y-12's many security, environmental, and budgetary problems. Between 2006 and 2011, remote-controlled equipment meant to protect workers from inhaling uranium failed in Building 9212. For five years, kneeling workers had to load uranium oxide by hand into canisters, while wearing respirators.

From 1997 to 2006, there were 21 fires and explosions at Y-12 involving electrical equipment, glove boxes, pumps, waste containers, and nuclear and hazardous chemicals. Several resulted in worker injuries and destruction of property.

After the 1994 shutdown of Building 9212, it took 12 years for uranium processing operations to restart there. The cost of resuming operations was more than \$500 million—five times the original estimate. The facility has yet to achieve an adequate capacity to process the backlog of unstable materials and produce purified HEU.

An inability to downsize

Although the end of the Cold War has eliminated much of Y-12's bomb-manufacturing mission, attempts to downsize by eliminating ancient, excess infrastructure have largely been unsuccessful. More than half of the Y-12's structures were built in the 1940s. Several buildings have been shuttered for years and are seriously deteriorated. Years of leaking roofs have created chronic safety problems, including standing water in fissile material storage areas and water accumulation near electric control



panels. In March 2014, a large portion of a concrete ceiling collapsed in a building that was once part of the weapons operation. It was a near miss: Foot-long concrete pieces bounced onto walkways and an area where welders had been working just a day before.

Over the course of nearly 20 years, however, several plans to downsize the Y-12 complex have foundered. In 1989, the National Research Council noted that Y-12 buildings occupied approximately 5.5 million square feet. Eight years later, the Energy Department announced that “by about the year 2003, the Y-12 facility would be approximately 10 to 20 percent the size of the existing plan.” As of this year, the square footage had shrunk by only about 7 percent. Even with this modest space reduction, the total Y-12 footprint is comparable to the square footage of the Nissan car assembly plants in Tennessee, which produces more than 550,000 vehicles annually.

Other attempts to close facilities at Y-12 have also evaporated. These failures are mainly due to the large expense of downsizing, which would increase the NNSA’s budget and compete with funds for weapons modernization. Congress is less likely to approve large-scale spending for downsizing antiquated structures than for a mission of maintaining thousands of nuclear weapons for national defense. And so efforts to close or dramatically shrink Y-12 have gone nowhere.

In 2005 a Department of Energy Task Force on the Nuclear Weapons Complex Infrastructure, citing the lack of “modern-day production technology,” recommended the closure of the Y-12 complex and urged the Energy Department to “immediately begin site selection processes for building a modern set of production facilities with 21st century cutting-edge nuclear component production, manufacturing, and assembly technologies, all at one location.” After the Tennessee and other congressional delegations created a political uproar, the Energy Department decided to proceed with a policy of “modernization in-place.”

Modernizing by cost overrun

In 2007, the NNSA began to seek funds from Congress for the Uranium Processing Facility (UPF), which would replace several dilapidated plants at the aging Y-12 site. The UPF was to use new technologies, under development at Y-12 for more than a decade, to replace the

chemical conversion and foundry processes used to create HEU weapons components since the 1950s.

The projected total project cost was \$1 billion and operations were expected to begin as early as fiscal year 2013. As with nearly all other new high-hazard nuclear facilities promised by the Energy Department, however, costs for the UPF have soared and its schedule has slipped by several years. The price tag for the UPF, renamed the Uranium Capabilities Replacement Project, now ranges from \$6.5 billion to \$19 billion.

With a projected workload an order of magnitude less than during the period of peak weapons production, a major question remains: What should the capacity of the UPF be? The large stockpile of thermonuclear components sitting at Y-12, justified in large part for potential reuse in a dwindling nuclear arsenal, implies that a very modest production capacity is needed.

In April 2014, the NNSA released a “red team” report, led by the director of Oak Ridge National Laboratory, on the troubled UPF. The team’s most significant recommendation was to rethink a basic, “big-box” approach that would create a UPF to serve multiple functions in one structure. Instead, to hold the line at an estimated \$6.5 billion for design and construction costs, the team recommended going back to the drawing board to effectively reduce the size and scope of the project. Meanwhile, in recognition of the growing hazards associated with a deteriorating infrastructure for storing “materials at risk,” the team recommended that greater emphasis should be given to safe consolidated storage of materials, deferred maintenance, and safety upgrading.

Conspicuous by their absence were explicit references to downsizing Y-12 overall.

The mercury threat

Activities at Y-12 have produced multiple environmental challenges; perhaps the largest is mercury pollution.



During the crash program to build thermonuclear weapons in the 1950’s and early 1960’s, Y-12 purchased about 24 million pounds of mercury to purify lithium. Of that amount, about 10 percent (2.4 million pounds) was released into the environment or could not be



accounted for inside buildings. To put the problem in perspective, **Y-12 mercury losses are about eight times the annual mercury emissions estimated by the Environmental Protection Agency for the entire United States during the years 1994 and 1995.**

Despite the well-recognized hazards of mercury, a neurological poison, workers were not provided with adequate protection from it. People living nearby, including hundreds of school children, were exposed for years to an estimated 73,000 pounds of mercury released to the air. In 2012, the Agency for Toxic Substances and Disease Registry concluded that “elemental mercury carried from the Y-12 plant by workers into their homes could potentially have harmed their families (especially young children).” A rough measure of harm to workers can be found in compensation statistics maintained by the Department of Labor. Nearly 9,000 Y-12 workers have received some \$417 million for exposure to non-radioactive substances.

The Upper East Fork Poplar Creek and Bear Creek continuously transport about 500 pounds of mercury from heavily contaminated soil on the site to downstream areas. The contaminated creeks then feed into the lower Watts Bar reservoir of the Tennessee River and the Clinch River, where tens of tons of mercury have accumulated in sediments. In 2002, nearly 40 percent of the anglers using the Watts Bar Reservoir continued to eat mercury-contaminated fish, despite a public ban on consumption. African-Americans were the least aware of the ban and were the most vulnerable to potential harm.

After recognizing the magnitude of the mercury problem at least 35 years ago, the Energy Department is just beginning to construct a

water treatment plant to remove mercury from the contaminated creeks and to reduce offsite mercury run-off. The total cost of mercury cleanup at Y-12 has not been determined. However, it may rival the cleanup costs of profoundly contaminated areas such as the Hanford Site in southeastern Washington state.

Cosmic mission creep

The current national security mission at Y-12 is so ill-defined and expansive that it strains credulity. For instance, the Government Accountability Office recently reported that one of the primary justifications for stockpiling excess canned sub-assemblies at Y-12 is “for potential use in planetary defense against earthbound asteroids.” In 2013, the Obama administration convened a senior-level team and established a now-stalled joint project with Russia to try to fend off asteroids bound for Earth, using nuclear weapons.

Regardless of the wisdom of or need for an asteroid-protection program, the future of Y-12 should be focused on earthly realities: cleaning up the environment, decontamination and decommissioning of facilities, stabilizing nuclear and other hazardous materials, and the dismantlement of a large excess stockpile of weapons components. There is a very real need to replace the collapsing infrastructure at Y-12 with facilities that can accomplish these goals.

Protecting the planet from asteroids is a poor rationale for failing to deal with the environmental, safety, financial, and health challenges the Y-12 site poses to the people who live in the area, and to the country as a whole.

*A senior scholar at the Institute for Policy Studies, **Robert Alvarez** served as senior policy adviser to the Energy Department's secretary and deputy assistant secretary for national security and the environment from 1993 to 1999. During this tenure, he led teams in North Korea to establish control of nuclear weapons materials. He also coordinated the Energy Department's nuclear material strategic planning and established the department's first asset management program. Before joining the Energy Department, Alvarez served for five years as a senior investigator for the US Senate Committee on Governmental Affairs, chaired by Sen. John Glenn, and as one of the Senate's primary staff experts on the US nuclear weapons program. In 1975, Alvarez helped found and direct the Environmental Policy Institute, a respected national public interest organization. He also helped organize a successful lawsuit on behalf of the family of Karen Silkwood, a nuclear worker and active union member who was killed under mysterious circumstances in 1974. Alvarez has published articles in Science, the Bulletin of Atomic Scientists, Technology Review, and The Washington Post. He has been featured in television programs such as NOVA and 60 Minutes.*



How did we get from trade disputes in Ukraine to nuclear threats in Severodvinsk?

By Kennette Benedict

Source: <http://thebulletin.org/how-did-we-get-trade-disputes-ukraine-nuclear-threats-severodvinsk7363>

The downing of Malaysia Airlines Flight 17 over Ukraine, apparently by Russian-trained separatists using a Russian missile launcher. The US government's determination that Russia has violated the Intermediate-Range Nuclear Forces Treaty of 1987 by testing ground-launched cruise missiles. Increasingly stringent US and European economic sanctions against Russia's government and key areas of the country's economy. Troubles in and around Ukraine are straining relations between Russia and the United States and raising the prospect of a new Cold War. Fear is fueling actions on all sides, even leading Russian Deputy Prime Minister Dmitry Rogozin, in a speech on the country's July 27 Navy Day, to laud new nuclear submarines being built at Severodvinsk, saying they will be a reliable deterrent against any threat: "We see the presence of a nuclear potential can cool the fervor of any aggressor located at any point in the world."

How has the East-West relationship moved from a November 2013 dispute over economic trading partnerships to veiled threats of nuclear weapons use just nine months later? Many Western observers begin their analysis with Ukraine's internal problems, of which there are many. But the current tensions have their origins in the ending of the Cold War, as US Ambassador to the Soviet Union Jack Matlock and others have observed.

In the years after the Berlin Wall fell, and particularly now under President Vladimir Putin, Russia has come to feel—with some justification—that it offered peace and a new beginning in East-West relations but was marginalized and even taken advantage of when it came to economic dealings and diplomatic relations with the West, a process it is trying to reverse with its actions in Ukraine. The United States and its European allies, on the other hand, view the annexation of Crimea and other Russian responses to the Ukraine crisis as aggressive violations of international norms.

In other words, as the Ukrainian situation has played out, Russian, US, and European political leaders have continued to view international relations as a competitive, win-lose game. They would be better served to think about international relations as a system of continuous and dynamic change—more like the weather than a game of Go, and therefore more appropriately dealt with through careful adjustments based on common interests than haphazard confrontations that can send the system reeling in unpredictable and perhaps very dangerous directions.

The problem, before Ukraine

A longer view of the current crisis would focus on the history of US-Russia relations since the end of the Cold War and the underlying conditions contributing to Russian and US actions today. The United States government has failed to understand the profound sacrifices that Russia and its citizens made in the aftermath of the Cold War's end. The region underwent four simultaneous revolutions, beginning abruptly with the dissolution of the Soviet Union and the fall of Mikhail Gorbachev: in the economy, in the political system, in Russia's national identity, and in foreign policy. Indeed, as experts watched what was happening in the early 1990s, some feared that the turmoil might even lead to conflict among ethnic groups within Russia and the outbreak of civil war, accompanied by an internal struggle for possession of the country's vast nuclear arsenals.

Those were not easy times for Russia and former Soviet societies, and far from offering a helping hand to its erstwhile enemies, the US government turned away from the profound problems of the region to focus on the United States and its own economic problems. The most successful post-Cold War program was one that helped Russia dismantle its nuclear arsenals and secure fissile material; others supported scientific exchanges, joint research, and employment for nuclear scientists. Russian hardliners took a



message from this help: The United States was more worried about Russian nuclear warheads aimed at America than about the economic shambles and psychological trauma that Russians were living with. In fact, a triumphalist narrative emerged in the West, contending the United States had outspent the Soviets in an arms race that brought about the collapse of their economy and a cry of “uncle.”

Many Russians had a different view. Rather than losing the Cold War, they believed, they had stopped the nuclear madness, given up their claims to regional hegemony, and opened their borders. They had stepped back from the nuclear precipice and extended the hand of peace to Western powers. In doing so, they sacrificed economic security, military preeminence, and international standing as one of the two superpowers in the world. For giving up so much, many Russian leaders believed they should have been rewarded.

Instead, they were left to their own devices. Very little financial or technical aid was provided to make the transition to a market economy. Trading relations among Eastern European countries were dismantled, and the Warsaw Pact dissolved, while NATO remained in place and even expanded. Soldiers and workers went unpaid, the Russian gross domestic product fell by more than 40 percent from 1990 to 1999, and male life expectancy dropped from 64 to 58 years. Under such conditions, it was a minor miracle that civil war did not erupt and that Russia remained intact.

It was in Putin’s first term as president that the economy began to turn around. Profits from extractive industries were showing up on state-owned company ledgers, and ordinary people began to feel a bit more secure. From 2000 to 2008, GDP grew seven per cent each year, and the economy began to stabilize, producing a growing middle class and a slightly more predictable future. Russia does not see itself as a “developing country.” The land of Tolstoy, Tchaikovsky, Chekhov, and Pushkin, as well as home to some of the greatest mathematicians and scientists of the 20th century, has a right to play on the world stage as a nation to be taken seriously.

But even now, economic life in Russia feels tenuous, politics is dominated by cronies and money, and neighboring China is on the rise. Under these circumstances, any moves by erstwhile allies to initiate stronger relationships with the West can seem threatening.

It is little wonder, then, that when Ukraine sought closer economic links with the European Union rather than developing deeper ties in a Russia-led customs union, Russian leaders were not happy. Along with the loss of a trading partner, and a likely rise in prices for Ukrainian-made goods, came a political coup, supported by the West, that brought instability to Russia’s border. In the best of times, such developments would worry a country’s leaders. And these were not the best of times.

A needed change of mindset

None of the aforementioned post-Cold War circumstances excuse Russia’s seizure of Crimea or its support for separatist military forces that wish to secede from Ukraine. But if the United States were faced with similar circumstances on its own border, it would likely try to influence events and social forces in the neighboring country, as it has in Mexico’s “drug war.”

In Ukraine, the conditions were ripe for instability. A stumbling economy that served the few and political institutions that exacerbated social divisions created a potent formula for protest, violence, an unruly political transition, and fears that the country would be pulled apart. Where there is disorder, whether at a border or within a society, fear mounts and conflict can turn violent and escalate into civil war that too often spills over into other communities and countries.

This current crisis illustrates vividly the complexity of societies and international systems, and the inability of many leaders to grasp the interconnections between politics and economics, between governing institutions and market forces, and between domestic change and international relations. In complex systems, like weather systems, for example, perturbations in one part of the system can ripple with unexpected force to cause disruption in another. There are tipping points, surprises, time delays, and unpredictable events with long-lasting effects. As environmental sustainability expert David Orr puts it, “Wisdom begins with the awareness that we live amidst complexities that we can never fully comprehend let alone control.”

As long as leaders and analysts continue to think entirely in terms of national interest, of leaders driven only by their personal ambitions, of military force as a means to further those ambitions—as in



games like chess or Go—decisions will reflect very short-term time horizons and lead to poor outcomes. To avoid surprises and catastrophes like the current troubles in Ukraine, and the subsequent worsening of East-West tensions, requires a mindset rare among national it.

leaders. It is a mindset capable of seeing connections, patterns, and dynamic systems, one with a sightline extending into the future far beyond the next political election, and into the past, as well, as seen by others who experienced

Benedict Kennette came to the Bulletin from the John D. and Catherine T. MacArthur Foundation, where she directed the international peace and security program from 1992 to 2005. She also established and directed the foundation's initiative in the former Soviet Union from 1992 to 2002. Before joining the foundation in 1987, she taught at Rutgers University (1980-1981) and at the University of Illinois at Urbana-Champaign (1981-1985). Benedict received her A.B. from Oberlin College and a PhD in political science from Stanford University. Her media appearances include interviews on ABC's 20/20, CNN, CNN International, BBC, CBC, NPR, CTV, Voice of America, Fox News Channel, Agence Presse-France, and Al Jazeera. She has been quoted in USA Today, the Chicago Tribune, Village Voice, Los Angeles Times, and Congressional Quarterly, among others. She appears regularly on radio news and talk shows in the United States, Britain, and Australia.

Hiroshima and Nagasaki: The many retrospectives

By Dan Drollette Jr

Source: <http://thebulletin.org/hiroshima-and-nagasaki-many-retrospectives7366>

Sixty-nine years ago, at 8:15 in the morning on August 6, the first atomic bomb exploded over Hiroshima. Three days later, another bomb was dropped on Nagasaki. **Estimates vary as to the number of people who died in those blasts, but the figure of at least 130,000 deaths for Hiroshima seems to be generally accepted, with another 70,000 for Nagasaki as of surveys conducted in November 1945.**

With the anniversaries of those events have come many news and comment stories in the press. But how best to put the bombings into perspective, especially after so much time has passed? The problem—to loosely paraphrase Joseph Stalin, no stranger to death on an industrial scale—is that “one death is a tragedy, while a million deaths is a statistic.” (This is particularly true when dealing with dry analytical reports about security, which inevitably use phrases like “collateral damage,” “kilotons,” and “battlefield scenarios”—masking the fact that there are large numbers of very real human lives involved on the receiving end of a nuclear weapon.)

Consequently, some of the most powerful and compelling articles about the atomic bombing bring things back to the individual, dealing with just a single person and the most intimate, small details of his or her life at the moment of

the bombing, as shown in this BBC multimedia piece on Hiroshima survivor Shinji Mikamo. For example, after the blast, while looking through the ruins of his family home, Mikamo found his father's watch, which had stopped at precisely 8:15 am. In Mikamo's words: “The unimaginable intense heat that reached several thousand degrees Fahrenheit from the blast had fused the shadows of the hands into the face of the timepiece, slightly displaced, leaving distinct marks where the hands had been at the moment of the explosion. It was enough to clearly see the exact moment the watch stopped.”

Other articles, such as this one in the *Washington Post*, tried a different approach to bring home the horror of the blasts. It focuses on a large and well-known symbol of the bombing: the dome of a concrete-and-steel structure that was one of the few buildings to survive the atomic blast in 1945. Now known as the Hiroshima Peace Memorial, the building has become the epicenter of yearly memorials and services to remember the victims. Through the use of the article's slide show, readers can see the dome as it looked immediately after the blast, and again over the years, until today. The memorial itself contains a museum with artifacts, exhibitions, and first-



person survivor, or *hibakusha*, accounts. There is something about seeing or hearing something first-hand, on-site; it really makes an impression. Knowing this, the mayor of Hiroshima asked leaders of nuclear-armed nations to see for themselves atomic bomb-scarred cities. "If you do, you will be convinced that nuclear weapons are an absolute evil that must no longer be allowed to exist," Kazumi Matsui was quoted as saying by ABC News. Not that there is anything wrong with standing back and taking a look at the big picture. Some media outlets have used the anniversary as an occasion to pause and think about nuclear weapons, such as this *Time* magazine piece by Harvard's Elaine Scarry, which notes: "An appropriate way to reflect on these events might be to contemplate our current nuclear arsenal and ask why it is being kept in place. The U.S. has by far the most powerful arsenal on Earth. Our 14 Ohio-class submarines together carry the equivalent of at least 56,000 Hiroshima blasts. These ships are not a remnant of the Cold War. Eight were made after the opening of the Berlin Wall during the presidencies of George H.W. Bush and Bill Clinton."

Over the years, of course, the *Bulletin of Atomic Scientists* has published its own rich lode of material—from all viewpoints—on the bombings of Hiroshima and Nagasaki. Highlights include *The Sanctification of Hiroshima*, a 1985 piece in which a physicist affiliated with the Manhattan Project supports the Hiroshima but not the Nagasaki bombing.

Meanwhile, **John E. Coggle's 1982 review** of the 600-page book *Hiroshima and Nagasaki: the Physical, Medical, and Social Effects of the Atomic Bombings*, by The Committee for the Compilation of Materials on Damage Caused by the Atomic Bombs hews to a different perspective. Drawing on his background as a medical doctor, Coggle went over the informative, technical prose and the 200 statistical tables, diagrams, maps, and photographs that graphically depict the effects of thermal radiation, the shock wave and ionizing radiation, short-term and long-term biological effects, and the

social and psychological impacts. Coggle used the phrase "encyclopedia of horror" to describe the book's un-nerving but necessary content, noting: "As a radiation biologist one sees the words 'Hiroshima and Nagasaki' quite frequently but only in the arid academic context of science..."

At the end of the day, it can be worthwhile on the Hiroshima and Nagasaki anniversaries to think about the personal and the emotional—while keeping such clinical data in mind and ready to hand when it is necessary to debate proponents of ideas such as "battlefield nuclear weapons," "limited nuclear war," and the use of select nuclear strikes as a form of "de-escalation."

Therefore, perhaps the most compelling of the stories in the *Bulletin* archive is a first-person recollection, *Hiroshima Memories*, by Hideko Tamura Friedman, who was just a young girl back on August 6, 1945. After moving to the United States and becoming a therapist in private practice and a part-time social worker in the Radiation Oncology Department at the University of Chicago Hospitals, Hideko excerpted this 1995 article from a longer, unpublished manuscript she was working on.

Hideko describes how she was reading a book when "a huge band of white light fell from the sky down to the trees." She jumped up and hid behind a large pillar as an explosion shook the

JOHN E. COGGLE reviews

Hiroshima and Nagasaki—the Physical, Medical, and Social Effects of the Atomic Bombings by The Committee for the Compilation of Materials on Damage Caused by the Atomic Bombs in Hiroshima and Nagasaki, translated by Eisei Ishikawa and David L. Swain Basic Books, Inc. 706 pages, \$37.50

This book is an encyclopedia of horror. It is also both a scientific text and a plea for sanity. Commissioned by the two devastated Japanese cities, it was written and compiled by 34 Japanese medical, physical and social scientists. It consists of over 600 pages of informative, technical prose and some 200 statistical tables, diagrams, maps and photographs. The photographs alone are a graphic reminder of the biological and physical destruction wrought in a few seconds by two tiny nuclear weapons.

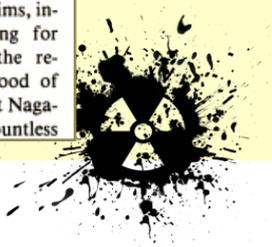
The opening sentence, "The names of Hiroshima and Nagasaki are known around the world—yet people remain ignorant of the reality and meaning of

of the A-bomb victims in the ensuing 35 years.

The two cities, dense with houses and people, were instantaneously destroyed. Over 90 percent of the buildings at Hiroshima within three kilometers of the hypocenter of the explosion were blasted, burned and demolished; over a third of all the buildings in Nagasaki were severely damaged. Of the estimated 300,000 people in Hiroshima on August 6, 1945, about 140,000 died either within hours of the attack or within the following few weeks. At Nagasaki on August 9, 1945, some 70,000 of the estimated 270,000 people present died.

The death and destruction were indiscriminate—babies, children, women, civilians, soldiers, residents, visitors, hospitals, schools—all blasted and irradiated into oblivion. About 90 percent of the deaths occurred immediately or within 14 days, and 90 percent of these were from blast, heat and radiation injury, and from the collapse of buildings.

Besides these primary victims there are the secondary A-bomb victims, including early entrants looking for friends and relatives, and the relief teams—in the neighborhood of 78,000 at Hiroshima, 11,000 at Nagasaki. And then there are the countless



earth and pieces of the roof fell about her. Hideko survived; some members of her family did not. "My father," she wrote in a heart-

rending statement of fact, "brought Mama's ashes home in his army handkerchief."

► **Read Coggle's review at:**

<http://books.google.ca/books?id=ggoAAAAMBAJ&pg=PA33&dq=hiroshima&hl=en&sa=X&ei=n6niU9nHN8PB8QHF54Eg&ved=0CCkQ6AEwAw#v=onepage&q=hiroshima&f=false>

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

Electromagnetic disaster could cost trillions and affect millions. We need to be prepared

By Anders Sandberg

Source: <http://www.homelandsecuritynewswire.com/dr20140812-electromagnetic-disaster-could-cost-trillions-and-affect-millions-we-need-to-be-prepared>

In 1962, a high-altitude Pacific nuclear test caused electrical damage 1,400 km away in Hawaii. A powerful electromagnetic pulse (EMP) – created either by a solar storm or a high-altitude nuclear explosion – poses a threat to regions dependent on electricity, as such pulses could cause outages lasting from two weeks to two years. The main problem is the availability of spare transformers. Superstorm Sandy's worst effects were in a single location. In the case of a big EMP surge, replacement transformers would be needed in hundreds of locations at the same time. The cost of an EMP pulse to the U.S. economy would likely be in the range of \$500 million to \$2.6 trillion. A report by the U.S. National Academies was even more pessimistic, guessing at a higher range and a multi-year recovery. Besides disrupting electricity such storms can also destroy satellites, disrupt GPS navigation, and make other parts of the infrastructure fail.

Predicting or worrying about disasters is a popular pastime. But we tend to take notice when somebody with money at stake becomes concerned. Financial people likely sat up when Paul Singer, manager of the Elliott Management hedge fund, warned in his latest newsletter that:

Even horrendous nuclear war, except in its most extreme form, can be a relatively localized issue, and the threat from asteroids can possibly be mitigated. The risks associated with an electromagnetic pulse, or EMP, represent another story entirely.

How right is he to worry about this?

A force of nature

Electricity and magnetism are tightly linked. Change an electric field — for example by moving charge — and a magnetic field appears. Change a magnetic field — for example by rotating a magnet — and electric fields appear. This is why electromagnets, generators and antennas work. Electromagnetic waves, whether radio, light or X-rays, are just oscillating fields.

The Earth has a vast natural magnetic field, courtesy of currents inside its core. As long as it is stable it is not noticeable except for turning compass needles. But what if something forced it to move? The change would produce currents in long conductors such as power lines or telecoms cables. The field is weak, but a shift across kilometers of cable can induce powerful currents, strong



enough to burn out fuses or damage transformers and other electronics.

A sharper push — such as generated by a nuclear explosion — can produce currents that disrupt smaller devices. In fact, microchips are easily burned out by a few volts in the wrong place.

What worries Singer is either naturally occurring geomagnetic storms, caused by the solar wind interacting with the Earth’s magnetic field, or deliberately produced electromagnetic pulses (EMPs) by nuclear weapons, or so-called e-weapons, devices that have been developed to disrupt enemy electronics. If something causes widespread and persistent black-outs and equipment damage the economic damage — and human problems — would be enormous.

Stormy sunlit days

Could something like this happen? In 1859 a solar storm, the “**Carrington event**,” named after an amateur astronomer, caused auroras down to the Caribbean, making telegraph systems across the world fail — pylons threw sparks and operators got electric shocks. It is worth noting that telegraphs are simple, sturdy systems compared to today’s fine electronics.

In 1989, a solar storm blacked out the power grid in Quebec. Small storms, a recent study shows, can cause noticeable bumps in insurance claims for industrial electrical equipment.

More recently, a near-miss was reported in July 2012, where Earth dodged a plasma cloud ejected by the sun only by a few degrees. Had it hit, the consequences would be dire.

A report from Lloyds emerging risk group has reviewed the evidence. They find that a Carrington-level geomagnetic storm is almost inevitable: one about every 150 years.

This poses a threat to regions dependent on electricity: such storms could cause outages lasting from two weeks to two years. The main problem is the availability of spare transformers.

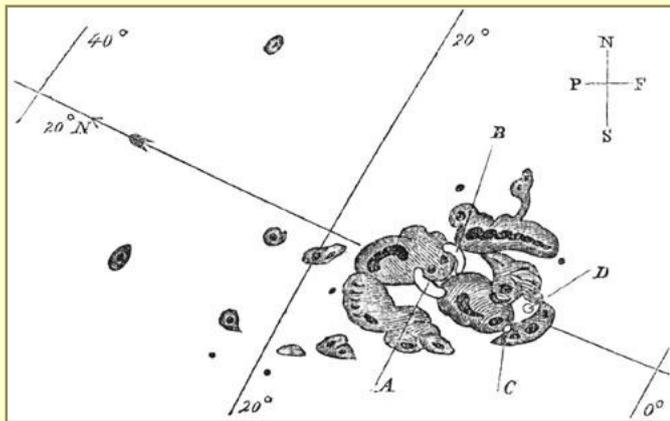
When hurricane Sandy hit New York in 2012, the main reason power could not be restored on lower Manhattan — despite the obvious wealth of the place — was that ordering replacement transformers takes months.

Sandy’s worst effects were in a single location. In the case of a big storm, replacements would

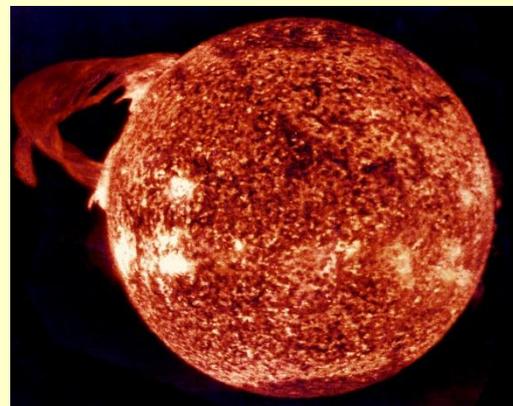
be needed in hundreds of locations at the same time. The cost of a Carrington-like event to the U.S. economy would likely be in the range of \$500 million to \$2.6 trillion. A report by the U.S. National Academies was even more pessimistic, guessing at a higher range and a multi-year recovery. Besides disrupting electricity such storms can also destroy satellites, disrupt GPS navigation and make other parts of the infrastructure fail.

The risk is real

Singer is probably right to worry about solar storms. Estimates are that there is a 12 percent risk over the next decade for a storm bad enough. Fortunately, we can improve our infrastructure when we recognize there is a problem. We can build more resilient systems, have a few back-up transformers in storage and harden devices. This costs money, but it is cheaper than a few weeks without power.



Sunspots of September 1, 1859, as sketched by Richard Carrington. A and B mark the initial positions of an intensely bright event, which moved over the course of 5 minutes to C and D before disappearing.



What is probably more worrying is the use of electromagnetic pulses created by weapons. This is a real threat,



which was discovered the hard way in 1962, when a high-altitude Pacific nuclear test caused electrical damage 1,400 km away in Hawaii (photo in next page).

In fact, deliberate destruction of enemy power grids using high-altitude detonations soon became part of the strategy of the superpowers. In the case of nuclear war there will no doubt be more things to worry about than just the power grid, but it is worth recognizing the threat posed to nearby nations.



Electromagnetic fields know no boundaries. Electromagnetic pulses from non-nuclear devices are a real possibility, either based on an explosion compressing a magnetic coil or

strong microwave fields. They have so far not been used for terrorism — presumably they are not bloody enough — but several countries have researched it.

Do we need to protect ourselves against e-weapons in the future? They are not lethal, the principles to build them are well known and it is not hard to imagine some people thinking they have good reasons for disrupting centers of power, finance or data. So, yes, defense against them would be a good idea.

That there are back-up copies and that data centers can be hardened might be less helpful than it looks if everybody needs new computers, networks, phones, cars and printers simultaneously — the disruption could be quite profound. Building more resilient gadgets would be to our advantage.

In the end, an electromagnetic disaster might cost trillions, harm millions of people and weaken society — perhaps on a global scale. It is a global catastrophic risk worth reducing. But it does not represent an existential risk just yet. But we are rapidly becoming more dependent on our fragile and vast electrical infrastructure. Some insulation is needed.

Anders Sandberg is James Martin Research Fellow, Future of Humanity Institute & Oxford Martin School at University of Oxford.

Abu Dhabi nuclear plant site prepares for 17,000 new arrivals

Source: <http://www.thenational.ae/news/uae-news/abu-dhabi-nuclear-plant-site-prepares-for-17-000-new-arrivals>

When the UAE's first nuclear-power plant opens at Barakah in 2017, an estimated 2,000



people will be working on the site and living in Al Ruwais with their families.

The area is undergoing major developments in preparation for the new community, said Fahad Al Qahtani, the external communications director at Emirates Nuclear Energy Corporation (Enec).

“To quote our chief executive, for every nuclear-plant employee we will need six workers in supporting services,” Mr Al Qahtani said. “These supporting services include schools, shops, restaurants and so on.”

This means the town, in the Western Region 240 kilometres



west of Abu Dhabi city, will see rapid growth, with at least 17,000 people arriving: 2,000 plant workers with 3,000 family members, plus 12,000 support workers.

"We are working closely with the Abu Dhabi Government, the Urban Planning Council and the Western Region Development Council [WRDC] on developing the region," Mr Al Qahtani said.

According to the Al Gharbia Investment Road Map, which was set up by WRDC, nuclear power will contribute Dh62 billion in capital to

Mohamed Hamad bin Azzan Al Mazrouei, the director general of WRDC.

Companies in the UAE have secured more than US\$1bn (Dh3.7bn) in contracts for products and services to support the construction at Barakah, Mr Al Qahtani said.

"The contracts have been awarded through joint collaboration between EneC and the Korea Electric Power Corporation [KePCo] over the past three years as part of efforts to support and develop the local industry and cover a range of products and services, including marine dredging, the provisioning of steel, metals and cables, housing projects and site construction activities," he added.

EneC's chief executive, Mohamed Al Hammadi, said the world-class nuclear programme would need an extensive supply chain.

"The UAE has a large pool of experienced suppliers and we have found that many local suppliers are able to meet the high standards for safety and quality that we demand because



the Western Region.

In March, WRDC announced the region was set to become the country's next development hot spot, with economic output expected to top Dh500bn by 2030. In 2010, GDP in the region was Dh243bn.

"In the next five years, Al Gharbia will witness the completion of the initial stages of a number of multibillion-dollar projects, such as the Madinat Zayed residential developments, a complex that will feature more than 100 apartments, retail shops, a health club, a mosque and offices, and the Ruwais Refinery Expansion, owned by Takreer, which when finished in the first quarter of 2014 will produce a total of 832,000 barrels per day of oil," said

of their wealth of experience with the oil and gas industry," he said.

More than 180 UAE companies had been awarded contracts, Mr Al Hammadi said, and hundreds of local companies had registered for future supply opportunities.

A number of local companies were also working with EneC to become certified Nuclear Competent companies, he said, a key certification to become approved providers to the nuclear-energy programme.

"This new, high-technology industry brings economic growth, job opportunities, and supports the long-term development of Abu Dhabi and the UAE," Mr Al Hammadi said.

Jordan, Russia to ink deal for nuclear reactor studies in September

Source: <http://jordantimes.com/jordan-russia-to-ink-deal-for-nuclear-reactor-studies-in-september---toukan>

August 14 – **Jordan will sign an agreement with Russia in September to start conducting studies on the country's first nuclear reactor for power generation, Khaled Toukan, chairman of the Jordan Atomic Energy Commission, said Thursday.**



“The Cabinet approved signing a project development agreement with Russia and we will sign the deal with the Russian partners in Moscow in September,” Toukan told reporters following a meeting with experts from the International Atomic Energy Agency.

The agreement opens the door for starting studies on the project, including an environmental impact assessment, cooling the reactor, financing for the venture, the cost of building the reactor and the cost of electricity it generates, he said.

The governments of the two countries will sign an agreement before the end of this year to show commitment to the implementation of the project, Toukan added.

The studies, which will cost some JD46 million, will be financed by Jordan and completed in two years.

In October 2013, Jordan announced that it has selected Russia to build the country’s first two nuclear reactors in a bid to produce atomic energy within the next decade.

The government selected **Russian state-owned firm Rosatom as its preferred vendor to construct two 1,000-megawatt (MW) nuclear power plants east of Amman by 2022.**

Under the deal, Rosatom has agreed to take on 49 per cent of the plants’ \$10 billion construction and operation costs on a build-own-operate basis, with the government shouldering the remaining 51 per cent and retaining a majority share in the plants.

Jordan has become the third Arab state to pursue peaceful nuclear energy, with the United Arab Emirates set to build four reactors with a combined 5,600MW capacity by 2020 and Egypt reaffirming in 2013 its plans to establish a 1,000MW reactor by the end of the decade.

The scientist and the nuclear smuggler: unexpected connection

By Egle Murauskaite

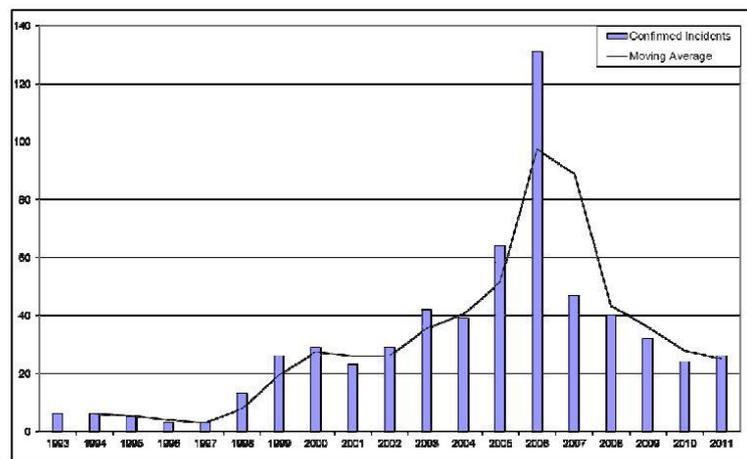
Source: <http://thebulletin.org/scientist-and-nuclear-smuggler-unexpected-connection7372>

The complicity of scientists, willing or unwitting, in the smuggling of radioactive materials has been a long-standing concern of the nonproliferation community. After the disintegration of the Soviet Union, the US Cooperative Threat Reduction program offered alternative livelihoods to impoverished nuclear scientists, in hopes of dissuading them from selling their knowledge to governments or terrorists seeking nuclear weapons or materials. A similar, if smaller effort was later launched to redirect Iraqi scientists who had

worked on Saddam Hussein’s weapons of mass destruction (WMD) programs to peaceful employment. Today, international threat-reduction and scientist-engagement programs focus on promoting best practices among professionals working with sensitive materials and raising the level of physical security of facilities to prevent diversion or misuse of nuclear material. And new efforts are underway to address growing concerns about the potential radicalization of scientists working in biological and chemical laboratories.



Confirmed incidents involving theft or loss, 1993–2011



Although the aforementioned efforts represent significant progress in nonproliferation, they fail to recognize an important component of the smuggling process: Scientists are consistently sought out—by their acquaintances or friends of friends—to test the quality of radiological or nuclear materials bound for the black market.

Consider, for instance, one of the latest significant cases of nuclear smuggling, in which Garik Dadayan, an Armenian residing in Russia, procured highly enriched uranium (HEU) from contacts in Novosibirsk. In 2003, Georgian authorities apprehended Dadayan when he attempted to sell 270 grams of HEU. He was arrested again in 2010 when he provided 18 grams of HEU for accomplices to sell. Significantly, in 2002—before setting up the deals—Dadayan had approached his acquaintance Hrant Ohanian, a retired scientist at the Yerevan Physics Institute, asking him to test the sample. Ohanian agreed and reportedly was able to test the HEU without difficulty. Similarly, in 2002, six Lithuanian men were caught attempting to sell nearly a kilogram of cesium 137 to a German national. Before arranging the transaction, the men took the material to the Physics Institute in Vilnius to verify its quality.

The scientific community has been used to verify the quality of illicit radiological or nuclear materials for decades. **For instance, in 1994, a loosely-connected network of individuals from the former Soviet Union was caught attempting to sell the largest quantity of illicitly obtained HEU known until that time.**

Eduard Baranov, a former employee at the Obninsk Institute for Physics and Power Engineering (IPPE) in Russia, had diverted HEU from the facility and convinced his neighbor, Alexander Scherbinin, to sell 2.7 kilograms of HEU on his behalf. Scherbinin was introduced to a former Czech nuclear scientist, Jaroslav Vagner, who agreed to assist with the search for buyers—but first,

Vagner had a sample of Scherbinin's HEU tested. His Polish acquaintance, Leszek Niemec, sent it to Landshut, Germany, and successfully verified its high level of enrichment. Another individual connected to this loose network, Vaclav Havlik, a Prague-based trader, procured pellets of low-enriched uranium (LEU) from a different source and also got it tested through an acquaintance before offering it for sale in June 1994.

Most interdicted attempts to sell illicit radioactive materials have involved small groups of loosely-connected individuals collaborating for that specific transaction, and three key features of the illicit radioactive materials market necessitate third-party verification of quality: the highly specialized nature of the product; the lack of expertise of the persons handling it; and the relatively low levels of familiarity and trust among smugglers. By nature, the need for independent verification of illicitly obtained radioactive materials before they are traded is comparable to seeking home value appraisals before a seller and buyer can comfortably close the deal, or requiring an independent audit before two companies complete a merger. Thus, the nonproliferation community should recognize that unscrupulous scientists not only function as the sources of illicit radioactive materials, but also as quality evaluators.

While increasingly effective measures have been instituted to prevent the diversion of radioactive materials from laboratories and research institutes worldwide, these measures are failing to consider the possibility that scientists may be approached by colleagues, acquaintances, or friends to verify the authenticity and quality of illicitly obtained radioactive materials. Assisting with such a quality test is not being treated as behavior as condemnable as diverting nuclear material to private hands, and professional curiosity in the exercise—



or perhaps reluctance to get an acquaintance in trouble—often leaves these incidents unreported. Actively encouraging timely notification about requests for outsider material verification could make a big difference in early interdiction efforts. Given the difficulty of obtaining radioactive materials to begin with, such efforts may present a good chance of disrupting or at least seriously delaying radiological and nuclear material smuggling operations. Notably, it has been typical that the sellers of nuclear and radiological materials

have been interested in testing quality—not the buyers. Thus, intercepting an operation at such an early stage would also likely offer strong leads to those responsible for diverting the materials to the seller.

Greater awareness within scientific communities and reporting mechanisms for quality verification requests could offer an important addition to the toolkit for curbing proliferation and countering nuclear terrorism efforts.

***Editor's note:** The views and conclusions expressed in this article are solely those of the author and should not be interpreted as necessarily representing the official policies or positions, either expressed or implied, of START, the US Department of Homeland Security, or CNS.*

***Egle Murauskaitė** is a research and training specialist at the US National Consortium for the Study of Terrorism and Responses to Terrorism (START). Previously, she held the position of research associate at the James Martin Center for Nonproliferation Studies (CNS). She is the co-editor of a volume, *Regional Security Dialogue in the Middle East*, and the author of several publications exploring WMD-related challenges.*

Remember?



A girl in isolation for radiation screening looks at her dog through a window in Nihonmatsu, Japan on March 14, 2011.



The Ubiquitous Threat: IEDs, Africa and the World

By Frank G. Rando

Source: <http://www.cbrneportal.com/the-ubiquitous-threat-ieds-africa-and-the-world/>

Terrorism and asymmetrical warfare push the limits of engagement and foster the loss of ethical boundaries. Widespread fear, panic and social upheaval ensue, in addition to mass casualties and infrastructure destruction and disruption, whenever an act of terrorism is involved. Such is the case when even the most simplistic, but effective, Improvised Explosive Device (IED) is detonated anywhere in the world.



As witnessed by a global audience of victims and spectators, Improvised Explosive Devices (IEDs), have taken their place as prominent and widespread tools of insurgents, terrorist factions, and even "lone-wolf" actors. While the toll of IED detonations have taken their toll in Operations Iraqi and Enduring Freedom (OIF/OEF), the stories of the casualty count from other areas of geopolitical instability, such as Africa, are moderately, or even rarely shared or mentioned, especially among the "casual observers" within the global population. Denial is bliss, and complacency replaces and thwarts awareness and preparedness. One tends to dispel the fact that what occurs on the other side of the globe may one day appear at their doorstep.

Tactical ultra-violence utilizing an IED detonation lacks discernment between

combatants and non-combatants, and with approximately 300 global incidents monthly poses a grave humanitarian threat with profound implications for both military and civilian components of societies. The following statement from Ajmal Samadi, Director of the Afghanistan Rights Monitor, makes clear the impact of IEDs on international safety and security: "The death of a foreign soldier in an improvised blast often makes headlines, but we have failed to communicate to armed opposition groups and their foreign supporters that IEDs kill and maim hundreds of innocent people and this is a clear violation of all war laws".

In addition to the physical casualties requiring both emergent and/or chronic care and rehabilitation, IEDs adversely impact societal stability, security/public safety and the progression of sustainability in many regions of the globe. This includes economic losses, population displacement in conflict-affected regions, destruction of infrastructure, loss of personal property and assets.

Terrorism and political violence in Africa is not a new, or even, recent phenomenon. Historically, coercive strategies utilizing ultra-violence have been a mainstay of achieving social and/or political goals in African states, ever since the earliest post-colonial period. The entire story, and examples of the use of IEDs against both governmental and non-governmental entities and populations in Africa are too numerous and complex to mention in this forum.

A growing transformation into radical Islamic and other genres of terrorism in regions such as North Africa and the sub-Saharan country of Nigeria, for example, poses grave implications for the entire African continent and other areas of the world, including the U.S. and West. Nigeria serves as a model, as its security and stability is essential not only to the entire African continent, but to intercontinental security.

The facts that surround Nigeria to being a central player in both continental and global security and stability stem from Nigeria's importance in economic growth in the 21st



century, as well as being the most populous nation-state in Africa, having substantial petroleum resources, and thus becoming one of the world's largest producers of oil. The infiltration of the black market into oil production and distribution has created an atmosphere of disenfranchisement and victimization, and has encouraged and generated insurgency and ultra-violence. The death toll consisting of well over 118 individuals in the aftermath of a dual terrorist bombing in the central Nigeria city of Jos is just a prime example of widespread use of IEDs in the West African region. Suicide bombings, vehicle-borne-improvised explosive devices (VBIEDs), and stationary IEDs have become commonplace in Africa. The trend of illicit small arms proliferation, such as the AK-47 assault rifle and the related armed assaults committed with this more conventional weaponry, is a phenomenon which has preceded the use of IEDs, and may serve as a strong indicator of unconventional and asymmetrical attacks utilizing IEDs. Therefore, vigilance must be maintained to thwart the trafficking of both conventional arms and high order energetic-explosive materials.

Some of the other root causes of tactical ultra violence within the African continent must also be addressed, such as poverty, endemic disease, famine, drought, and other natural and man-made events that have impacted both internal and global security. We have been aware of several terrorist factions on the African continent, such as al-Shabaab in

Somalia and al-Qaeda in in the Islamic Maghreb in North Africa, and all are adept at devising, deploying and detonating IEDs. Africa has served as a foundation and base for international and state-sponsored terrorism that have impacted other global stakeholders, as well as a fertile ground that spawns and spreads terror and political violence utilizing widely available, unconventional and opportunistic weaponry: the IED.

The disruption of funding streams for terrorist activity, as well as continued and aggressive strikes against the ability for terrorist factions organize, operate, communicate, and a robust "no-holds barred" position on non-proliferation and interdiction of both small arms and energetic materials that is enforceable must be the integrated methodology to dismantle the use of IEDs and other armaments on the African continent.

This strategy combined with realistic and achievable humanitarian and policy-making efforts to address root causes, such as poverty and corruption will continue to be the routes of achieving geopolitical stability and security in Africa and thwart the proliferation and use of the ubiquitous IED.

This strategy combined with realistic and achievable humanitarian and policy-making efforts to address root causes, such as poverty and corruption will continue to be the routes of achieving geopolitical stability and security in Africa and thwart the proliferation and use of the ubiquitous IED.

Frank G. Rando possesses over 30 years of real world experience as a public safety professional, clinician, educator, emergency and crisis manager, author and consultant in the areas of tactical, disaster and operational medicine, weapons and tactics, law enforcement /criminal investigations, counterterrorism, hazardous materials management and emergency response, toxicology, environmental safety and health, and health care and public health emergency management.

Fourth female suicide bomber hits Nigeria's Kano, kills six



Source: <http://af.reuters.com/article/topNews/idAFKBN0FZ1QH20140730>

A female suicide bomber blew herself up in a college in northern Nigeria's biggest city of Kano on Wednesday, killing six people and critically wounding another six in the fourth such attack by a woman in Kano in less than a week, a security source said.

The bomber targeted youths who were looking at a notice board for national youth service in Kano Polytechnic, the source said.

There was no immediate claim of responsibility, although



militant group Boko Haram, which is fighting for an Islamic state in religiously-mixed Nigeria, has repeatedly bombed Kano as it radiates attacks outwards from its northeast heartlands. Using female suicide bombers in the city appears to be a new tactic of Boko Haram, although they have used them on occasion for years in the northeast.



Two female suicide bombers blew themselves up at a trade show and a petrol station in Kano on Monday, killing one other person and injuring at least six others.

On Sunday, a female suicide bomber killed herself but no one else while trying to target police officers. In a separate incident on Tuesday, two suicide bombers killed 13 people in attacks on two mosques in the town of Potiskum, in Yobe state in the northeast, a medical official there told Reuters on Wednesday.

Though much of the violence is concentrated in the remote northeast, they have struck across Nigeria in several bomb attacks since April. On Sunday, they mounted a cross-border attack into Cameroon, killing at least three people there and kidnapping the wife of the vice prime minister.

University Licenses Groundbreaking Explosives Detection Technology

Source: <http://www.hstoday.us/single-article/university-licenses-groundbreaking-explosives-detection-technology/47a25bdff619d6f57761ce9c667d6286.html>

The University of Tasmania in Australia has stepped up the fight against terrorism by licensing two technologies, Scantex and CEScan, to technology commercialization firm Grey Innovation.

Scantex and CEScan have been developed in collaboration with Australian forensic and policing authorities to detect homemade explosives, such as those used in London, Madrid, Bali and Boston bombings. Among the funding agencies are the National Security Science and Technology Center and the US Department of Homeland Security.

CEScan is the first comprehensive instrumentation in the world to detect the full range of explosives, including military, commercial and homemade inorganic and peroxide explosives, overcoming the limitation of existing screening techniques that struggle to detect modern explosives. CEScan with its breadth of capability is expected to find application in centralised analytical environments such as forensic and customs laboratories.



Using the same base technology, Scantex has been designed as a field deployable version of CEScan system that provides fast detection of homemade explosives, making it ideal for use in airports and similar high-throughput environments.



The technology was invented by Professor Michael Breadmore and his team from the University's Faculty of Science, Engineering and Technology.

"Cracking the problem around separating and identifying inorganic molecules was the breakthrough we needed to create CEScan and Scantex," Breadmore said. "Now we can detect trace levels of inorganic explosives, as well as the other more routine classes of dangerous materials, in under a minute."

Incorporating these technologies into commercial grade units, and ensuring that those machines can be relied on for such critical information, is the role being taken on by Grey Innovation.

Grey Innovation's Managing Director, Jefferson Harcourt, said as the licensee and co-developer, the company would move the technology from the lab to the market place.

"The ability to detect a wide range of modern high explosives with this level of sensitivity, and to do it quickly, is a huge step forward in terms of counterterrorism technologies," Harcourt said.

"Instrumentation in this space has to stand up to significant regulatory scrutiny, needs to be dependable, and has to be cost effective. Initial discussions with potential partners have already commenced."

The University's Director of Business Development and Technology Transfer Darren Cundy said there was always an expectation that the research would need to be further developed by private industry.

"As we've been working with Grey on a range of projects that need this type of capability, they were a natural fit when we looked for partners," Cundy said. "While we recognise that there is still much to do before we see products being sold, this is a natural step in the translation of the University's research outputs and we have high hopes that ultimately it will generate strong returns for us and our commercial partners."

"We Have 75 Female Suicide Bombers" – Boko Haram

Source: <http://247ureports.com/?p=54858>

The arrival of Boko Haram to the Nigerian scene during the administration of the late President Yar'Adua may have struck Nigerians as a temporal nuisance that will have its stay and then disappear. But six years later, the Boko Haram nuisance appears ever present in the Nigerian scene more than it was when it showed up. Efforts by the Nigerian security apparatus to curtail the emergence of the Islamic Jihadist group have proved little in terms of results rather it has



proved the opposite. Sensitive information available to 247ureports.com obtained through a very competent source indicates that the Islamic Jihadist has adopted the Palestinian model of Jihadism in its usage of young girls as suicide bombers on buses and crowded places.

According to the information gathered, the latest move by the Islamist Jihadist group to rain terror in Nigeria led the leaders of Boko Haram into a union-ship with the leaders of Hezbollah to

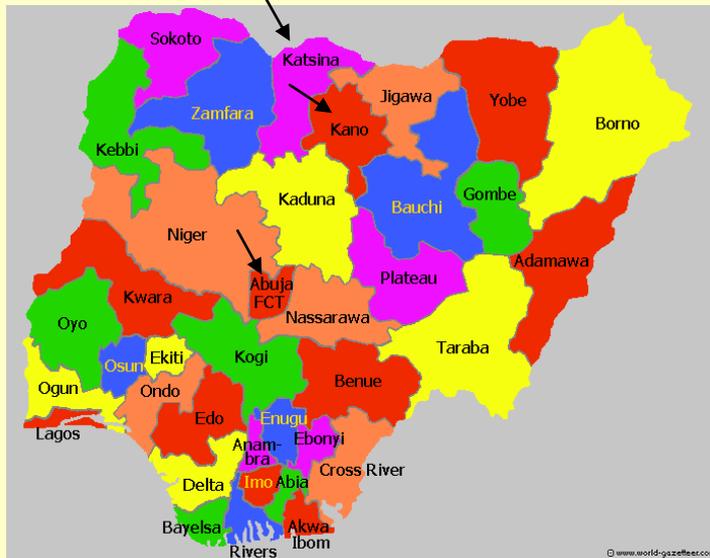


help recruit and train young innocent girls as potential suicide bombers for use in parts of northern Nigeria. As gathered, the partnership between the Middle Eastern Jihadist group and the Nigerian Jihadist group reportedly have resulted in the successful recruitment and training of over 177 young girls under the ages of 15.

The source continued to reveal that out of the 177 suicide bombers, 75 were already in Nigeria to execute suicide missions in three northern States of Katsina, Kano and the Federal Capital Territory [FCT], Abuja. The types of attacks, the source indicates would not take the shape of attacks that the Nigerian security authorities are used to, or would anticipate. *“The year will end as the year of Boko Haram”* says the source as he tried to emphasize on the preparedness of the Islamic Jihadist group in unraveling the polity before the campaigns for 2015.

The source who claims to have full access to the Islamist group explained that the group has become highly tuned into the politics of Nigeria in the sense that it intends to shape the outcome of the presidential elections in 2015 to favor a Muslim candidate. He explained that the attack on Malam [General] Buhari was largely part of the 2015 equation. He explained that their preferred candidate for the office of the presidency was the person of General Buhari. But Buhari’s recent and sudden criticism of the Islamic group angered the group immensely because, according to the group, Buhari’s credibility within the north may add a big bite towards discrediting the Boko Haram in the north. The source notes that the

Boko Haram group perceives themselves as well accepted by the ‘core’ Islamic north. For this reason, criticism coming from a person in the stature of Malam Buhari may cause many



within the core Islamic north to back away from secretly supporting Boko Haram. The Islamic group did not want Buhari criticisms to continue to become his campaign mantra for 2015.

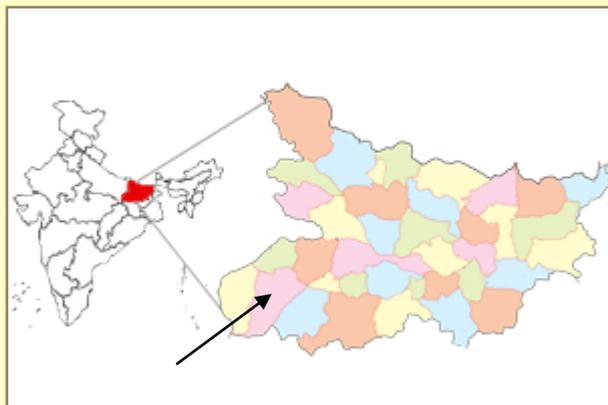
247ureports.com made efforts to contact the State Security Services [SSS] in Kano concerning the threat of increased suicide bombers on the offing but the SSS Director in Kano failed to respond to our requests. However a top security boss in Abuja spoke to our correspondent off the record. He confirmed that intelligence reports do indicate that more suicide bombers are on the way and that plenty have already arrived the country. He also added that the system is too corrupt to fight and combat the terrorist. In his words, *“insurgency can be defeated if the security agencies are overhauled. But for now it is a money making venture”*.

4,225 detonators recovered from Bihar Maoist stronghold

Source: <http://www.terrorismwatch.org/2014/08/4225-detonators-recovered-from-bihar.html>

August 07 – Over 4,200 detonators were recovered Thursday in Bihar’s Rohtas district, police said. Rohtas Superintendent of Police Chandan Kumar Kushwaha said a huge quantity of explosives, including 4,225 detonators, 1,200 gelatin sticks and 15 kg ammonium nitrate, was recovered. Acting on a tip-off, a police team raided a house in Karbandia locality near Sasaram, the district headquarter. One man was also arrested in this connection. Last week also police had recovered a huge quantity of explosives, including 3,550 detonators, 1,791 gelatin sticks and 5 kg ammonium nitrate, from a village near Sasaram. Police had arrested three people in this connection.





Rohtas is considered to be a Maoists stronghold.

According to police, recovered material, including ammonium nitrate, is used for making improvised explosive devices and bombs.

The state police along with the central paramilitary forces have intensified combing operations against Maoists in different parts of Bihar.

Last month, the Central Reserve Police Force (CRPF) in a joint operation with Bihar Police recovered a huge cache of

explosives from a Maoists hideout in Gaya district.

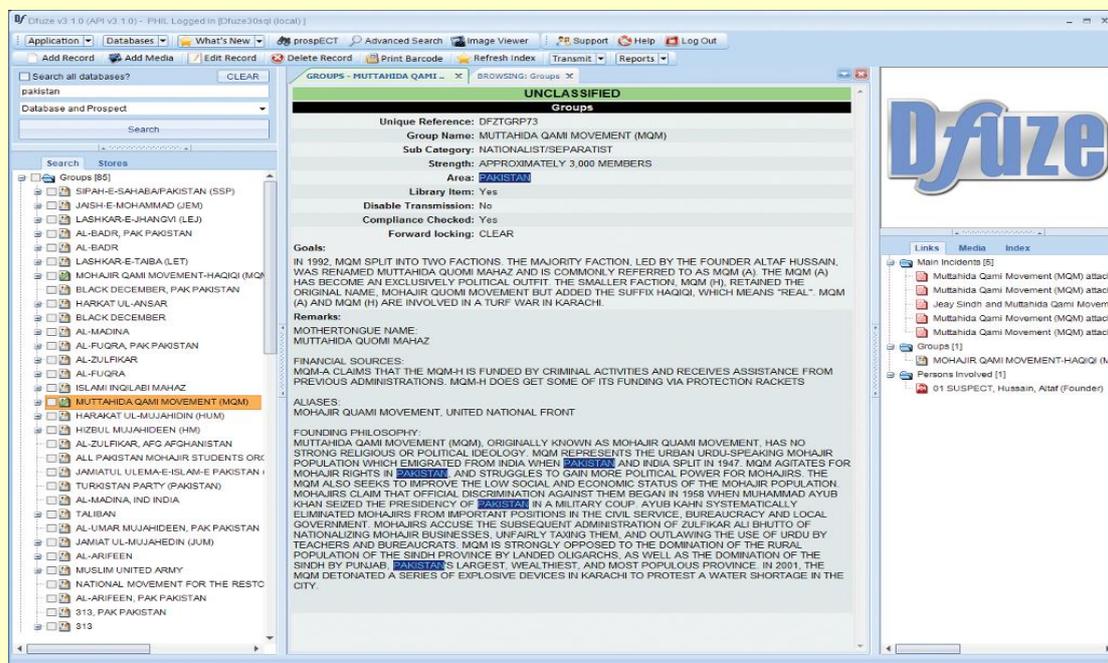
Tool helps investigators connect bomb fragments to bomb makers

Source: <http://www.homelandsecuritynewswire.com/dr20140808-tool-helps-investigators-connect-bomb-fragments-to-bomb-makers>

Authorities with the U.S. Special Operations Command (SOCOM), the Canadian military, the U.S. Bureau of Alcohol, Tobacco, and Firearms (ATF), and law enforcement agencies in the United Kingdom have adopted a crowdsourcing system called DFuze to help agencies in twenty-five countries connect bomb fragments to bomb makers or

worldwide. DFuze also serves as a reference library for research and training.”

DFuze, developed in the United Kingdom and first used as Scotland Yard’s bomb database, is now owned by Intelligent Software Solutions (ISS). The Colorado-based company has developed DFuze into multiple platforms, including a Web interface, a mobile app, and



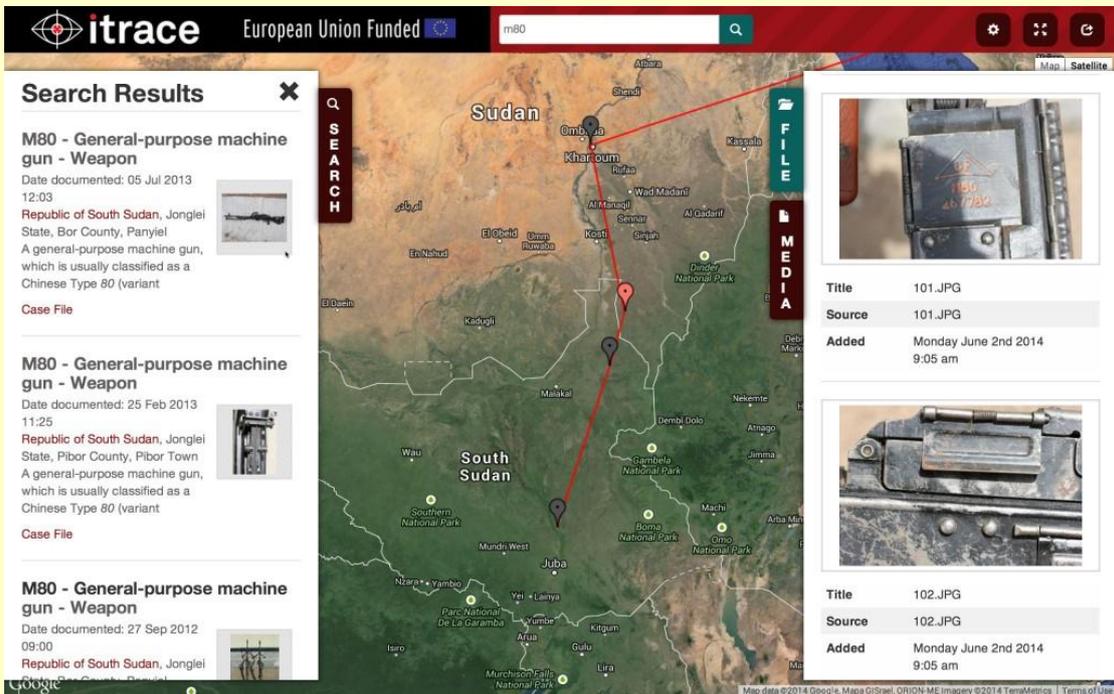
individuals who could be connected to a specific bomb. According to the ATF, DFuze “establishes an information highway that facilitates and promotes the sharing of information between ATF, participating members, and National Bomb Data Centers

an open-source database called ReportDesk. The technology allows users to share bomb images and data to assist pending investigations. “It’s mainly aimed at fast time dissemination of information from



bomb scenes or from terrorist incidents,” Neil Fretwell an operations director at ISS and one of the creators of DFuze told *Defense One*. Fretwell, a former lead investigator for the U.K.

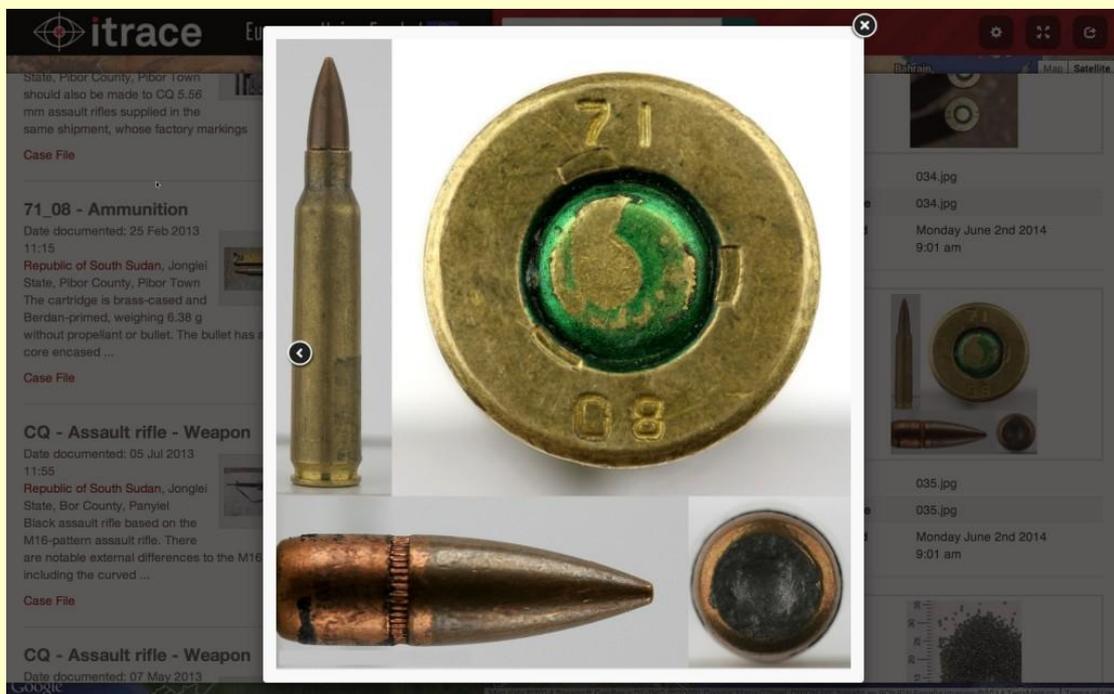
them onto a compact disk...sticking them on the back of a motorbike with a blue light and physically running them back to Scotland Yard. It was nonsense,” he said. Fretwell and his



Police National Bomb Data Center, describes his experience while working the scene of the 2005 London subway bombings and how that led to developing DFuze into a crowdsourcing

colleagues then decided that the DFuze system needed an upgrade.

Today, DFuze has inspired the creation of iTrace (photos) a global weapons tracking



application. “I was down in one of the tunnels...the information was needed urgently back in the control center and at the other scenes. We were taking images, downloading

system used by the European Union and Conflict Armament Research (CAR), a group founded by former United



Nations weapons monitors. Using information provided by CAR field work, iTrace tracks the movement and groups associated with weapons and ammunition used by militias in Africa. "We learned that solely focusing on one country when looking at weapons doesn't uncover the full picture," CAR's director of operations, Jonah Leff, told the *Washington Post*. "The U.N., governments and NGOs I

think really started addressing this issue in the late 90s, but very little is understood about the minutia and trade of illicit weapons globally." iTrace is currently available to diplomats at the U.N. and will be available to the public in September. "We document one weapon at a time, one crate of ammunition at a time, and build a case around it," Leff said.

Shooting victim charged with possession of WMD

Source: <http://www.wwaytv3.com/2014/08/15/shooting-victim-charged-with-possession-of-wmd>

Wilmington Police have charged a shooting victim after they say they found homemade bombs at his home.

Around 9:30 p.m. Wednesday officers responded to a ShotSpotter alert in the 300 block of Barclay Hills Drive. When they got there, they found Silas Pipkin Dobyms, 25, who told police he was walking when some men asked him to come over to them. He refused, and then heard 3-5 shots fired. Police say one of the shots hit Dobyms in the arm. Before he went to the hospital, police say Dobyms asked the officers to go back to his house at 314 Barclay Hills Drive to make sure it was locked up. Police say when they got to the home they found two bottles that appeared to be Molotov cocktails by the front door. When they looked inside they saw another Molotov cocktail on a table just inside the front door. Police say the items were bottles filled with what smelled like gasoline with a gasoline soaked cloth hanging out. They also found a military-style bulletproof vest in plain view inside. Police say the fire department came and destroyed the devices, and Dobyms went to the hospital. Officers later served Dobyms with a warrant for possession of weapons of mass destruction. According to the New Hanover County Jail, Dobyms was booked in last night around midnight and released under \$35,000 secured bond about an hour later.

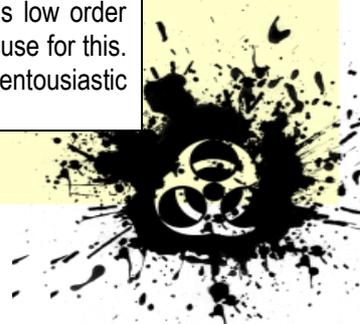


EDITOR'S COMMENT: Charged with possession of WMDs... Most probably this case is currently



under investigation (read also the comments accompanying the article above). But despite this specific incident is the overall directive towards the right direction? For those who say no – I think that they must redefine what WMDs are. Are they only CBRN agents? Is a Molotov bomb or a onventional bomb a WMD? Is it eliciting terror? For those who say "yes" – they have also to redefine the charging procedures since they can be out of control if not properly addressed. In Greece in many instances police found caches of Molotovs in apartments, basements or even inside universities (photo) not to mention the wide use of

Molotovs during demonstrations. If our legal system does not respond aggressively to this low order explosive device then the "M" of WMD might become a reality and then there will be no excuse for this. Prevention is always better than treatment. But treat with care because sometime over-entouasiastic treatment might not be very beneficial for the patient/victimim.



The Newest Weapon in the Fight Against Land Mines Could Be...Plants

Source: <http://gizmodo.com/the-newest-weapon-in-the-fight-against-land-mines-could-1622408134>



Land mine being defused in Cambodia. AP Photo/Heng Sinith

Land mines are not only explosive but also poisonous, leaking toxins into the soil that make plants sick. That's *unfortunate* for the plants but *fortunate* for us—if we can figure out how to look for sick plants as harbingers of land mines. Airplanes equipped with a low-cost sensor that captures non-visible light might be the answer.

LiveScience's Becky Oskin reports from the annual meeting of Ecological Society of America, where a group of researchers from Virginia Commonwealth University are presenting just this idea. That a bunch of ecologists would be interested in land mines actually makes a lot of sense; land mines lurking underground can subtly shape the ecology of an area.

The VCU researchers did their field research at an unusual place though, a "privately owned experimental minefield in South Carolina, where [DARPA] once buried fake land mines for a research project," writes Oskin. The National Explosives Waste Technology and Evaluation Center is

where researchers can (safely) experiment on new ways to detect land mines.



At the experimental mine field, VCU researchers found that **not all plants reacted to explosives like TNT and RDX the same.** **Woody plants** were less affected than herbaceous ones with soft stems. On the other hand, common **weeds** like the nutsedge (photo – left) seemed completely unaffected. The makeup and health of an area with dense vegetation—where traditional mine detection methods might be difficult—could be a clue to land mines underneath. To that end, the researchers envision an entire "Explosive Specific Index" cataloguing how buried explosives affect different plants.

A winged elm damaged by exposure to explosive chemicals.



The key, though, is a fast and cheap way to scan across large swathes of vegetation. That could mean hyperspectral imaging from airplanes or from the ground. Hyperspectral imaging can also light outside of the visible spectrum, which is helpful because infrared, for



example, can reveal damage that doesn't show up in visible light. Plants could one day reveal secrets long buried underground, if we just know what to look for.

Beach walker throws live World War 2 GRENADE for his dog thinking it was a stone

Source: <http://www.mirror.co.uk/news/uk-news/beach-walker-throws-live-world-4066726>

A beach walker threw a stone for his dog to fetch - only to discover that it was a live wartime GRENADE.

The man picked up the barnacle-encrusted "stone" for his pet to chase along the sands without realising it was deadly World War 2 explosive.

In an incredible stroke of luck, an off-duty military explosive expert also on the seafront at Dovercourt, near Harwich, Essex recognised the dog's new "toy" and immediately raised the alarm.

A 100-foot cordon was hastily put up by police around the grenade as a bomb disposal team

Inspector Paul Butcher of Essex Police said: "Anyone who finds a grenade should on no account touch it but call the police immediately.

"We think the grenades may have been in a



crate that ended up in the sea during World War Two and that it might now be breaking up or has been disturbed by dredging work in the area.

"The result is that these five devices have all been washed ashore on the same stretch of the bay so we are asking people to be vigilant if they go onto the beach and dial 999 if they find any of these devices.

"Some have been covered in barnacles but the one found on Saturday looked almost like new despite the fact it had been in the sea for



rushed to the scene. It is the fifth World War 2 hand grenade that has been washed up on the same beach over the last five weeks.

Yesterday, another similar grenade was discovered less than a quarter of a mile away.

many years." All the grenades have been taken away by the Army's Explosive Ordnance team and destroyed in controlled explosions on the beach.



Don't fear the robot car bomb

By Patrick Lin

Source: <http://thebulletin.org/don%E2%80%99t-fear-robot-car-bomb7379>



Within the next few years, autonomous vehicles—alias robot cars—could be weaponized, the US Federal Bureau of Investigation (FBI) fears. In a recently disclosed report, FBI experts wrote that they believe that robot cars would be “game changing” for law enforcement. The self-driving machines could be professional getaway drivers, to name one possibility. Given the pace of developments on autonomous cars, this doesn't seem implausible.

But what about robotic car bombers? If car bombs no longer require sacrificing the driver's life, then criminals and terrorists might be more likely to use them. The two-page FBI report doesn't mention this idea directly, but this scenario has caused much public anxiety anyway—perhaps reasonably so. Car bombs are visceral icons of terrorism in modern times, from The Troubles of Northern Ireland to regional conflicts in the Middle East and Asia.

In the first half of 2014, about 4,000 people were killed or injured in vehicle bombs worldwide. In the last few weeks alone, more than 150 people were killed by car bombs in Iraq, Afghanistan, Yemen, Somalia, Egypt, and Thailand. Even China saw car bombings this summer.

America is no stranger to these crude weapons either. In the deadliest act of domestic terrorism on US soil, a truck bomb killed 168 people and injured about 700 others in Oklahoma City in 1995. That one explosion caused more than \$650 million in damage to hundreds of buildings and cars within a 16-block radius. In 1993, a truck bomb parked underneath the World Trade Center killed six people and injured more than a thousand others in the ensuing chaos. And earlier this year, jihadists were calling for more car bombs in America. Thus, popular concerns about car bombs seem all too real.

But what do automated car bombs mean to criminals and terrorists? Perhaps the same as anything else that is automated. Generally, robots take over those jobs called the “three D's”: dull, dirty, and dangerous. They bring greater precision, more endurance, cost savings, labor efficiencies, force multiplication,

ability to operate in inaccessible areas, less risk to human life, and other advantages.

But how would these benefits supposed to play out in robot car bombs? Less well than might be imagined.

Pros and cons

For the would-be suicide car bomber, a robotic car means eliminating the pesky suicide part. By replacing the human driver who is often sacrificed in the detonation of a car bomb, an autonomous vehicle removes a major downside. This aspect is related to the worry that nation-states may be quicker to use force because of armed drones, since those robots remove the political cost of casualties to their own side. When costs got down, adoption rates go up; therefore, we can expect to see an increase in suicide car-bombing incidents, driven by autonomous technologies.

Or so the thinking goes.

But this analysis is too pat. Part of the point for some guerilla fighters—though probably not for ordinary criminals—is martyrdom and its eternal benefits. So, dying isn't so much of a cost to these terrorists, but rather more of a payoff. This demographic probably wouldn't be tempted much by self-driving technology, since they are already undeterred by death.

Of course, it may be that a more calculating terrorist, who still seeks glory, would like to do as much damage as possible before he kills himself. (Though some suicide bombers are women, most of them are still men.) In this case, he may want to mastermind several car-bombing attacks before finally dying in one. Robot cars would enable him to do so, and still allow him to get credit for his work, an issue of importance to terrorists, if not to criminals.

And at the least, those not motivated by ideology might not want to die quite so soon. For them, a robotic driver would be an attractive accomplice.

However, other options are already available for terrorists who do not want to harm themselves—yet these options have not created any panic about car-bombing attacks. For instance, both criminals and guerilla fighters have been known to recruit and

train others to do their bidding. Those designated as drivers sometimes are not even aware of their explosive cargo, which avoids the trouble of indoctrinating them toward fanatical self-sacrifice. Terrorists could kidnap innocent people and coerce them to become suicide bombers, which is reportedly occurring today in Nigeria.

So if ease and costs are considerations, there are better alternatives than transforming robot cars into mobile bombs. For one thing, the only production cars being built today with self-driving capabilities are the Mercedes Benz S-

getting the same job done as autonomous car bombs.

Besides bombing, are there post-execution reasons for using a robot car, such as minimizing forensics evidence? A captured driver, or even the DNA of one who is blown up, can attribute an attack to a particular group. But the same could be achieved by stealing a car and coercing an innocent person to drive. Robot cars may actually be worse for the criminal who wants to keep a low profile. If they are networked and depend on GPS for navigation, the cars could be tracked as soon



Class sedan (that sells for about \$100,000) and the Infiniti Q50 sedan (about \$40,000)—not exactly tools for the budget-conscious terrorist, even if prices do fall in the future. Even then, their capacity to operate autonomously is primarily limited to things such as staying within a lane and following the flow of traffic on a highway.

Google's self-driving car makes even less sense for this evil purpose. As the most advanced automated car today, it would cost more than a Ferrari 599 at over \$300,000—if it were for sale, which as a research vehicle it isn't. (Even if a terrorist could steal it, good luck figuring out how to turn it on.) Anyway, the car can operate autonomously only around Google's headquarters, since ultra-precise maps beyond that area don't yet exist. In sum, it is not a good choice for targets outside Mountain View, California.

If a fanboy terrorist really did want to go high-tech, he could more easily rig his own car to be driven by remote control. Or kidnap engineers to do the work, as drug cartels in Mexico have done to build communication systems. Or just get some kamikaze micro-drones. All of these options are more likely and more practical,

as they leave the driveway of the suspect under surveillance. GPS records could be searched to piece together a timeline of events, including where the car has been on the days and weeks leading up to its use as a weapon. Furthermore, a self-driving car without a human in it at all won't be in production any time soon. A human will always be "in the loop" for the foreseeable future; at the moment, any "self-driving" car is supposed to have someone in the driver's seat, ready to take the wheel at a moment's notice, such as when an unexpected construction detour or bad weather interferes with the car's sensors and a human operator must quickly retake control. So a robot car bomb with no driver in it would likely raise immediate suspicions, if the car would even move at all.

Admittedly, hacks have already appeared that disable the safety features meant to ensure a human is present and alert. Networked and autonomous cars present many more entry points for hackers, possibly allowing a very knowledgeable criminal to cyber-hijack a robot car.



Theoretically, a terrorist could want to use a robot car as a bomb while he's still in it—that is, forego the opportunity to spare his own life. It could be that he tends to get lost easily, wants to read last-minute instructions behind the wheel, has to stay in contact with his home base, or must baby-sit the trigger mechanism. A robot car would offer these benefits, however minor they may be.

Possible solutions

The threat of robot car bombers, then, seems unlikely but not impossible to become a reality. Some solutions to that possible threat include requiring manufacturers to install a “kill switch” that law enforcement could activate to stop an autonomous vehicle. This plan was already proposed in the European Union for all cars in the future. Or sensors inside the car could be used to detect hazardous cargo and explosives, similar to the sensors at airport

At the end of the day, there's still no substitute for good old-fashioned counterterrorism, human intelligence, and vigilance: in recent weeks, security checkpoints foiled car-bombing plots in Northern Ireland and Jerusalem. Overall, it makes more sense to use these traditional methods; it is easier to continue to use checkpoints, and regulate and monitor the ingredients used in car bombs, rather than oversee the cars themselves.

In truth, in the idea behind robot cars, domestic and international security is facing a very old threat. The problem isn't so much with robots but with stopping enemy vehicles from penetrating city walls with a destructive payload, which is a problem as old as the Trojan horse of ancient Greek mythology. (There's a reason why a certain kind of malware goes by the same name). Robot cars merely present a new way to deliver the payload.

The Switchblade

In backpack
Antenna
Video sites
Control panel
Launcher

1 Drone removed from backpack and loaded into launcher
2 Drone launched and wings and tail unfold
3 Soldier directs drone using control panel, joystick and video sites, via nose-mounted camera
4 When target is reached soldier remotely arms missile and wings retract
5 Missile explodes upon hitting target

The miniature 'backpack' drone is manufactured by the California-based firm AeroVironment. It runs on a quiet electric motor, is guided either by GPS or manually by a nose-mounted camera

Specifications	
Drone weight	5-6lbs
Speed	50mph
Range	4.4miles
Normal altitude	500ft
Maximum altitude	15,000ft
Launch time	30sec
Wingspan	4.4ft
Length	2ft
Cost	\$10,000

security checkpoints. Or regulators could require special registration of owners of autonomous vehicles, cross-referencing customers with criminal databases and terrorist watch-lists.

But any of these options will face fierce resistance from civil rights advocates and other groups.

And a determined terrorist can get around technological safeguards and firewalls.

<http://www.wired.com/2011/10/tiny-kamikaze-drone/>

Maybe this is a problem that doesn't demand immediate action and is just part of the “new normal”—if it even comes to pass. For hundreds of years, just about every kind of vehicle has been turned into a mobile bomb: horse-drawn buggies, boats, planes,



rickshaws, bicycles, motorcycles, and trains. This could be a case of misplaced priorities. Or, as journalists Matthew Gault and Robert

even though the actual threat posed by car bombs is generally located far elsewhere. Most suicide car bombs happen in the Middle East in a low-tech way, whereas they are very rare in the United States. But because most of the news coverage about a hypothetical robot car bomb has occurred in the US media, it gives the false impression that it's a first-world problem. Autonomous cars would have a hard time operating on Afghanistan's dirt roads without lane markings, for instance, even if one could be obtained there.



Perhaps the reason for America's obsession is that the car bomb is a special, iconic

Beckhusen phrased it in *War Is Boring*: "Americans freak out over small threats and ignore big ones," For example, a terrorist with a single well-placed match in California during the summertime could easily do a massive amount of economic damage and disrupt transportation, businesses, and ecosystems. It's the ultimate in low-tech terrorism, yet could plausibly cause hundreds of millions of dollars in damage. But the appearance of just one robot car bombing could set back the entire autonomous-driving industry, in addition to the loss of life and the property destroyed. And there are other uses, misuses, and abuses related to autonomous cars that should be of just as much—if not more—concern.

weapon of terror—our prized possession turned against us. Different from rockets and drone missiles that fall from the sky, car bombs can be more insidious. They would infiltrate civilized society, sneaking up on its most vulnerable points. Like matches, cars are omnipresent in the modern world, and thus



nearly impossible to control. But very few elaborate car bombings have been attempted, even though they could be done today via remote control or through the use of a kidnapped driver, for example. Simple still works. As an actual threat, the robot car bomb seems overblown.

First-world problems

Weirdly, robot cars bombs seem to be a decidedly Western—or even American—fear,

Patrick Lin is director of the Ethics and Emerging Sciences Group and associate philosophy professor at California Polytechnic State University, San Luis Obispo. He is also an affiliate scholar at Stanford Law School's Center for Internet and Society and a visiting senior research fellow at Australia's Centre for Applied Philosophy and Public Ethics. Lin was the lead editor of Robot Ethics: The Ethical and Social Implications of Robotics.



The SWAMP: A Key Resource in Improving Software Assurance

Activities

Source: <http://www.dhs.gov/st-snapshot-swamp-key-resource-improving-software-assurance-activities>



The Software Assurance Market Place, or SWAMP, is an online, open-source, collaborative research environment that allows software developers and researchers to test their software for security weaknesses, improve tools by testing against a wide range of software packages, and interact and exchange best practices to improve software assurance tools and techniques.

“The goal of the SWAMP is to aid in the development of a healthier and safer cyber environment, and that starts with creating better quality software,” said Kevin Greene, Department of Homeland Security Science and Technology Directorate, Cyber Security Division, SWAMP Program Manager. “We’re doing something unique, we’re providing software developers the opportunity to test software and leverage multiple software analysis tools together in one space to improve the accuracy of their results.”

Built in a high-performance computing environment, the SWAMP allows users to leverage a wide-range of software packages, test cases, and community projects while addressing weaknesses within the software through an assessment platform comprised of five open-source tools--PMD, FindBugs, CppCheck, GCC, and Clang, as well as more than 100 open-source software packages. In the future, the tool repository will expand to include dynamic and binary code assessments, commercial software analysis tools, new platforms – including mobile – and offer Application Programming Interfaces (APIs) for

third-party services and to support continuous integration as part of the software development process.

According to Greene, the SWAMP’s designers went to great lengths to ensure the site was secure, including implementation of identity-based controls to protect submitters’ intellectual property. Software may be submitted either as public or private, based on the submitter’s desired security level. For software packages that are private, only those who are granted access by the project owner may access the results. Public packages rely on a crowdsourcing approach and encourage technical exchange and collaboration, resulting in better quality open-source software.

“Software requires several checks and balances during the development phase. Likewise, if someone is developing software for you, you would need to validate whether that software can be trusted. The SWAMP serves as a resource to vet software and ensure it meets individual security requirements before installed.”

The SWAMP was made available to users in February 2014, and has been drawing a great deal of interest from academia, federal government, industry, and freelance software developers. Since then, users have been registering and uploading software packages and testing and vetting software for weaknesses that could lead to vulnerabilities. Software developers who test their software early and often can decrease the cost of software failure, weed out common bugs, and contribute to community-wide cyber knowledge.

► For more information on the SWAMP, visit <https://continuousassurance.org>. To access the SWAMP, visit <https://www.mir-swamp.org>.

Hacker Says Passenger Jets at Risk of Cyber Attack

Source: <http://www.ndtv.com/article/world/hacker-says-passenger-jets-at-risk-of-cyber-attack-570731>

Cybersecurity researcher Ruben Santamarta says he has figured out how to hack the satellite communications equipment on passenger jets through their

WiFi and inflight entertainment systems - a claim that, if confirmed, could prompt a review of aircraft security.



Santamarta, a consultant with cybersecurity firm IOActive, is scheduled to lay out the technical details of his research at this week's Black Hat hacking conference in Las Vegas, an annual convention where thousands of hackers and security experts meet to discuss emerging cyber threats and improve security measures. His presentation on Thursday on vulnerabilities in satellite communications systems used in aerospace and other industries is expected to be one of the most widely watched at the conference.

"These devices are wide open. The goal of this talk is to help change that situation," Santamarta, 32, told Reuters.

The researcher said he discovered the vulnerabilities by "reverse engineering" - or decoding - highly specialised software known as firmware, used to operate communications equipment made by Cobham Plc, Harris Corp, EchoStar Corp's Hughes Network Systems, Iridium Communications Inc and Japan Radio Co Ltd.

In theory, a hacker could use a plane's onboard WiFi signal or inflight entertainment system to hack into its avionics equipment, potentially disrupting or modifying satellite communications, which could interfere with the aircraft's navigation and safety systems, Santamarta said.

He acknowledged that his hacks have only been tested in controlled environments, such as IOActive's Madrid laboratory, and they might be difficult to replicate in the real world. Santamarta said he decided to go public to encourage manufacturers to fix what he saw as risky security flaws.

Representatives for Cobham, Harris, Hughes and Iridium said they had reviewed Santamarta's research and confirmed some of his findings, but downplayed the risks.

For instance, Cobham, whose Aviation 700 aircraft satellite communications equipment was the focus of Santamarta's research, said it is not possible for hackers to use WiFi signals to interfere with critical systems that rely on satellite communications for navigation and safety. The hackers must have physical access

to Cobham's equipment, according to Cobham spokesman Greg Cairnes.

"In the aviation and maritime markets we serve, there are strict requirements restricting such access to authorised personnel only," said Cairnes.

A Japan Radio Co spokesman declined to comment, saying information on such vulnerabilities was not public.

Buggy "Firmware"

Black Hat, which was founded in 1997, has often been a venue for hackers to present breakthrough research. In 2009, Charlie Miller and Collin Mulliner demonstrated a method for attacking iPhones with malicious text



messages, prompting Apple Inc to release a patch. In 2011, Jay Radcliffe demonstrated methods for attacking Medtronic Inc's insulin pumps, which helped prompt an industry review of security.

Santamarta published a 25-page research report in April that detailed what he said were multiple bugs in firmware used in satellite communications equipment made by Cobham, Harris, Hughes, Iridium and Japan Radio Co for a wide variety of industries, including aerospace, military, maritime transportation, energy and communications.

The report laid out scenarios by which hackers could launch attacks, though it did not provide the level of technical details that Santamarta said he will disclose at Black Hat.

Harris spokesman Jim Burke said the company had reviewed Santamarta's paper. "We concluded that the risk of compromise is very small," he said.

Iridium spokesman Diane Hockenberry said, "We have determined that the risk to Iridium subscribers is minimal, but we are taking precautionary measures to safeguard our users."

One vulnerability that Santamarta said he found in equipment from all five manufacturers was the use of "hardcoded" log-in credentials,



which are designed to let service technicians access any piece of equipment with the same login and password.

The problem is that hackers can retrieve those passwords by hacking into the firmware, then use the credentials to access sensitive systems, Santamarta said.

Hughes spokeswoman Judy Blake said hardcoded credentials were "a necessary" feature for customer service. The worst a hacker could do is to disable the communication link, she said.

Santamarta said he will respond to the comments from manufacturers during his

presentation, then take questions during an open Q&A session after his talk.

Vincenzo Iozzo, a member of Black Hat's review board, said Santamarta's paper marked the first time a researcher had identified potentially devastating vulnerabilities in satellite communications equipment.

"I am not sure we can actually launch an attack from the passenger inflight entertainment system into the cockpit," he said. "The core point is the type of vulnerabilities he discovered are pretty scary just because they involve very basic security things that vendors should already be aware of."

SATCOMS vulnerable to hacking

Source: <http://www.homelandsecuritynewswire.com/dr20140811-satcoms-vulnerable-to-hacking>

Satellite communications systems (SATCOMS) used by soldiers on the front lines, airplanes, and ships are vulnerable to hacking, according to analyst Ruben Santamarta of IOActive. At the recent Black Hat cybersecurity conference, Santamarta presented his research showing that communications devices from firms Harris, Hughes, Cobham, Thuraya, JRC, and Iridium are vulnerable to attack due to security flaws

Defense One reports that the Cobham Aviator 700D, a common SATCOM in military aviation, could be hacked to cause "catastrophic failure." While none of the vulnerabilities discovered could directly cause a plane to crash, or override pilot commands, they could delay or intercept communications, exposing security and classified information to bad actors. The most serious vulnerability on the Cobham Aviator 700D allowed a hacker access to systems swift broadband unit (SBU), and the satellite data unit (SDU). "Any of the systems connected to these elements, such as the Multifunction Control Display Unit (MCDU), could be impacted by a successful attack," Santamarta writes in his paper. "The SBU contains a wireless access point." The MCDU provides vital information such as the amount of fuel left in a



built into the systems, most notably, backdoors, or special entry points which are designed for fast or emergency access into systems.

SATCOMS developers insist that backdoors do not pose a security risk, and consider them a "common practice in electronic products," because vendors and technicians sometimes forget passwords. Santamarta refutes saying "I can't recommend ever a back door. It's a security risk. It's not a good idea."

plane. If compromised, a hacker could give a pilot wrong information about the plane, causing the pilot to take actions based upon misinformation.

Cobham spokesman Greg Caires claims that the backdoor on the Cobham Aviator 700D helps ensure ease of maintenance, and "we determined that you have to be physically present at the terminal to use the



maintenance port,” refuting the ability to hack the system via Wi-Fi. Santamarta reiterated, however, that while certain attacks require physical access, other vulnerabilities within the SBU “can be attacked through the Wi-Fi.” In

marketing the Cobham Aviator 700D, Cobham states that “aviator 700D becomes the aircraft’s very own Wi-Fi hotspot in the sky, supporting in-flight use of smart phones, personal tablets and laptops.”

Meet MonsterMind, the NSA Bot That Could Wage Cyberwar Autonomously

Source: http://www.wired.com/2014/08/nsa-monstermind-cyberwarfare/?mbid=social_fb

Edward Snowden has made us painfully aware of the government’s sweeping surveillance programs over the last year. But a new program, currently being developed at the NSA, suggests that surveillance may fuel the government’s cyber defense capabilities, too. The NSA whistleblower says the agency is **developing a cyber defense system that would instantly and autonomously neutralize foreign cyberattacks against the US, and could be used to launch retaliatory strikes as well.** The program, called **MonsterMind**, raises fresh concerns about privacy and the government’s policies around offensive digital attacks.



Although details of the program are scant, Snowden tells WIRED in an extensive interview with James Bamford that algorithms would scour massive repositories of metadata and analyze it to differentiate normal network traffic from anomalous or malicious traffic. Armed with this knowledge, the NSA could instantly and autonomously identify, and block, a foreign threat.

Cryptographer Matt Blaze, an associate professor of computer science at the University of Pennsylvania, says if the NSA knows how a malicious algorithm generates certain attacks, this activity may produce patterns of metadata that can be spotted.

“An individual record of an individual flow only tells you so much, but more revealing might be patterns of flows that are indicative of an attack,” he says. “If you have hundreds or thousand of flows starting up from a particular place and targeted to a particular machine, this might indicate you’re under attack. That’s how intrusion detection and anomaly-detection systems generally work. If you have

intelligence about the attack tools of your adversary, you may be able to match specific patterns to specific tools that are being used to attack.”

Think of it as a digital version of the Star Wars initiative President Reagan proposed in the 1980s, which in theory would have shot down any incoming nuclear missiles. In the same way, MonsterMind could identify a distributed denial of service attack lobbed against US

banking systems or a malicious worm sent to cripple airline and railway systems and stop—that is, defuse or kill—it before it did any harm.

More than this, though, Snowden suggests MonsterMind could one day be designed to return fire—automatically, without human intervention—against the attacker. Because an attacker could tweak malicious code to avoid detection, a counterstrike would be more effective in neutralizing future attacks.

Snowden doesn’t specify the nature of the counterstrike to say whether it might involve launching malicious code to disable the attacking system, or simply disable any malicious tools on the system to render them useless. But depending on how its deployed, such a program presents several concerns, two of which Snowden specifically addresses in the WIRED story.

First, an attack from a foreign adversary likely would be routed through proxies belonging to innocent parties—a botnet of randomly hacked machines, for example, or machines owned by another government. A counterstrike could therefore run the risk of embroiling the US in a conflict with the nation where the systems are located. What’s more, a retaliatory strike could cause unanticipated collateral damage.



Before returning fire, the US would need to know what it is attacking, and what services or systems rely upon it. Otherwise, it could risk taking out critical civilian infrastructure. Microsoft's recent move to take down two botnets—which disabled thousands of domains that had nothing to do with the malicious activity Microsoft was trying to stop—is an example of what can go wrong when systems are taken down without adequate foresight.

Blaze says such a system would no doubt take the attribution problem—looking beyond proxies to find exactly where the attack originated—into consideration. “Nobody would build a system like this and be unaware of the existence of decentralized botnet attacks laundered through the systems of innocent users, because that’s how pretty much all attacks work,” he says. That does not, however, make so-called hackback attacks any less problematic, he says.

The second issue with the program is a constitutional concern. Spotting malicious attacks in the manner Snowden describes would, he says, require the NSA to collect and analyze *all* network traffic flows in order to design an algorithm that distinguishes normal traffic flow from anomalous, malicious traffic.

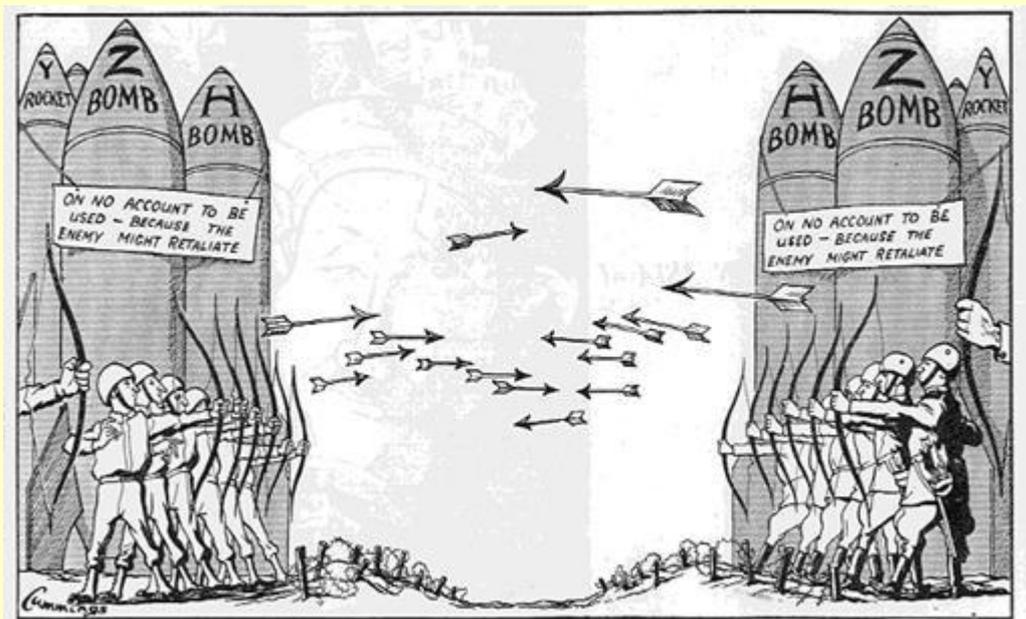
“[T]hat means we have to be intercepting all traffic flows,” Snowden told WIRED’s James Bamford. “That means violating the Fourth Amendment, seizing private communications without a warrant, without probable cause or even a suspicion of wrongdoing. For everyone, all the time.”

It would also require sensors placed on the internet backbone to detect anomalous activity. Blaze says the algorithm scanning system Snowden describes sounds similar to the government’s recent [Einstein 2](#) (.pdf) and [Einstein 3](#) (.pdf) programs, which use network sensors to identify malicious attacks aimed at U.S. government systems. If that system were secretly being extended to cover all U.S. systems, without public debate, that would be a concern.

Although MonsterMind does resemble the Einstein programs to a certain degree, it also sounds much like the Plan X cyberwarfare program run by Darpa. The five-year, \$110 million research program has several goals, not the least of which is mapping the entire internet and identifying every node to help the Pentagon spot, and disable, targets if needed. Another goal is building a system that allows the Pentagon to conduct speed-of-light attacks using predetermined and pre-programmed scenarios. Such a system would be able to spot threats and autonomously launch a response, the *Washington Post* reported two years ago.

It’s not clear if Plan X is MonsterMind or if MonsterMind even exists. The *Post* noted at the time that Darpa would begin accepting proposals for Plan X that summer. Snowden said MonsterMind was in the works when he left his work as an NSA contractor last year.

The NSA, for its part, would not respond to questions about the MonsterMind program.



access to a supervisor’s machine, and, theoretically, knowledge of the supervisor’s login credentials, to upload their own images into the system. But in the version of the control software they obtained for the Rapiscan 522B, the supervisor’s password screen could be subverted through a simple SQL injection attack — a common hacker tactic that involves entering a special string of characters to trigger a system into doing something it shouldn’t do. In this case, the string would allow an attacker to bypass the login to gain access to a console screen that controls the TIP feature.

“Just throw [these] characters into the login,” Rios says, and the system accepts it. “It tells you there’s an error, [but then] just logs you in.”

Using the console, an attacker could then direct the system to superimpose weapons or other contraband onto the x-ray images of clean bags to disrupt passenger screening. Or the attacker could superimpose images of clean bags onto the operator’s monitor to cover the true x-ray image of a bag containing contraband.

Upon seeing a weapon on the screen, operators are supposed to push a button to notify supervisors of the find. But if the image is a fake one that was superimposed, a message appears onscreen telling them so and advising them to search the bag anyway to be sure. If a fake image of a clean bag is superimposed on screen instead, the operator would never press the button, and therefore never be instructed to hand-search the bag.

It’s not clear if the Rapiscan 522B controller that the researchers tested was deployed in an airport. Rapiscan systems, and the TIP feature, are also used in embassies, courthouses and other government buildings, as well as at border crossings and ports to scan for smuggled goods, though Rapiscan says the version of TIP that it sells to TSA is different from the version it sells to other customers. And the TSA says there’s no chance the researchers got their hands on the software used by the agency.

“The Rapiscan version that is utilized by TSA is not available for sale commercially or to any other entity; the commercial version of the TIP software is not used by TSA,” says TSA spokesman Ross Feinstein.

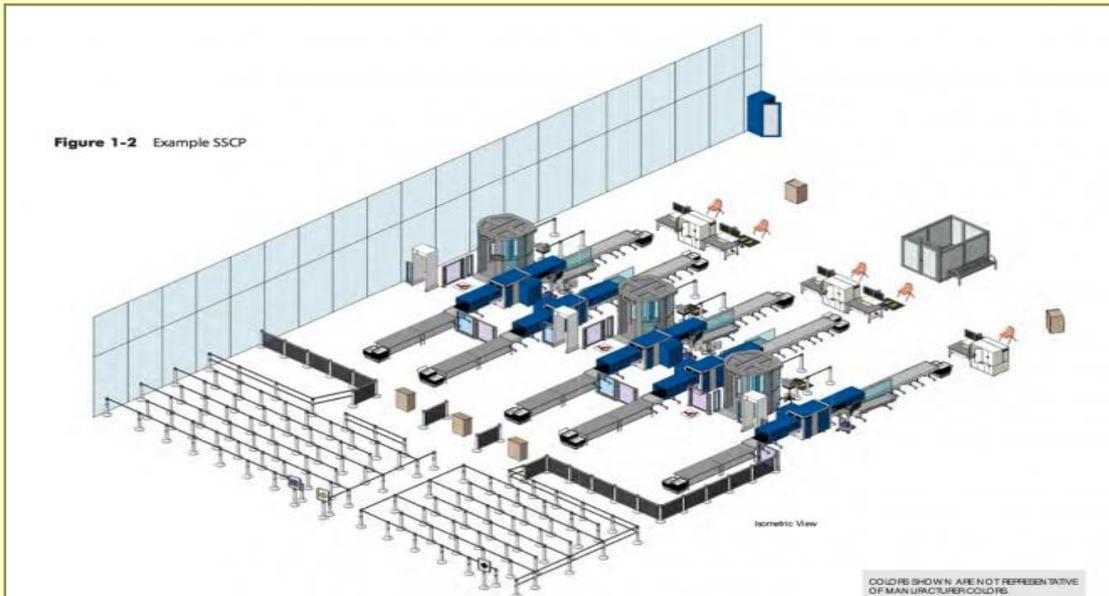
“The agency uses its own libraries and settings. Furthermore, the 522B systems are not currently networked.”

“Prior to decommissioning any TSA unit, this proprietary software in use by TSA is removed,” adds Feinstein.

The researchers plan to present their findings today at the Kaspersky Security Analyst Summit here.

The researchers’ findings are interesting in part because airport security devices are generally not accessible to white-hat hackers who regularly analyze and test the security of commercial and open source products, like the Windows or Linux operating systems, to uncover vulnerabilities in them.

The TSA has approved scanners from three vendors — Rapiscan, L3 and Smith. The TIP feature is



required in all such systems, but the researchers can’t say for certain whether the others work in the same way or can be subverted as easily.



The Rapiscan system came with a database of about two dozen different images of weapons from which to choose. Through a console, supervisors can set the frequency with which fake images appear on screen – for example, every 100 bags scanned by the system – as well as add or modify the library of images from which to choose.

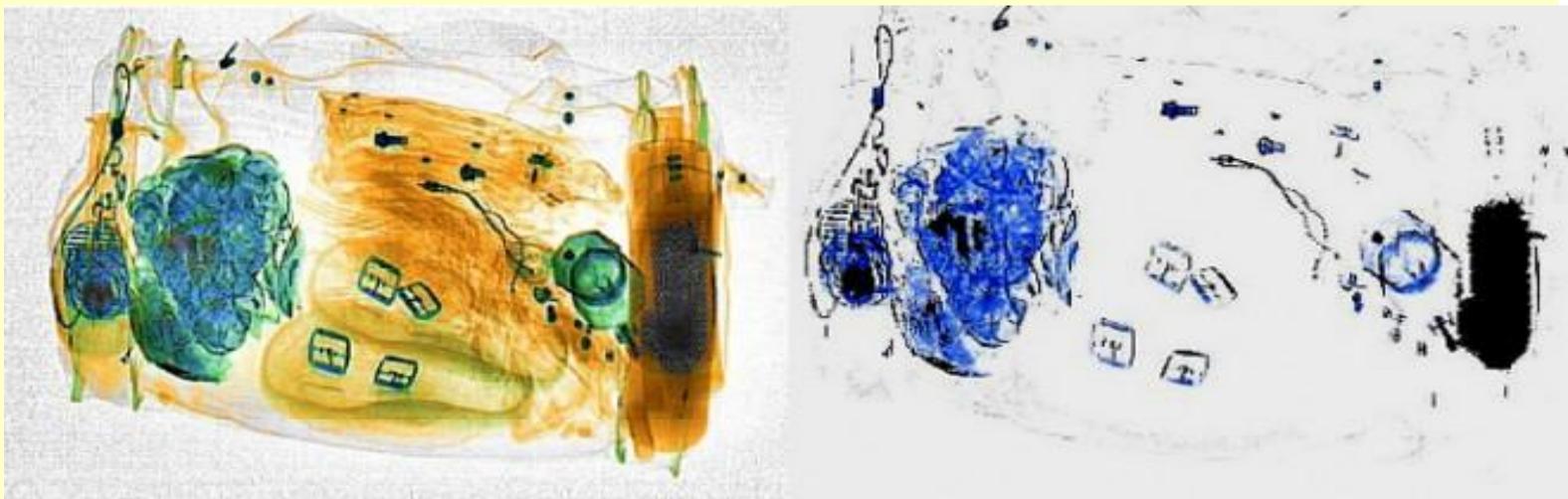
Rapiscan denies the supervisor password vulnerability exists, and claims the researchers must have purchased a machine that was misconfigured. Executive Vice President Peter Kant also denies that an attacker would be able to superimpose anything on the operator's screen; he says an algorithm determines how the contraband is projected into the bag, to avoid inserting an image of a gun that is too big for the bag.

But Rios says that he found each image has an accompanying file that tells the system how to use the image, and an attacker could simply upload his own instruction file to ensure that his rogue image blocks out the real x-ray image beneath it.

In addition to the login bypass, the researchers found that all of the operator credentials were stored in the system in an unencrypted text file. "Rapiscan could encrypt them, and they should," Rios says. "It's so outrageous that they didn't. If anyone, ever gets access to the [Rapiscan] file system, they will have access to all the user accounts and passwords in cleartext. No need for keyloggers or malware, just read them out of the text files."

Rios says the Rapiscan software he examined is based on Windows 98. More recent Rapiscan machines run on Windows XP. Neither of these operating systems is supported by Microsoft today.

"There are plenty of remote exploits for Win98 and WinXP that affect these systems," says Rios, suggesting that hackers could use these to hijack a supervisor's system to obtain access to the console for baggage scanners.



Images courtesy Qualys

The baggage scanners at airports are not connected to the public internet. But neither are they entirely isolated systems. TSA regulations require baggage scanners and other security equipment at large U.S. airports to be wired to a central network called TSANet.

As described in a recent job announcement for a government contractor, the TSA's Security Technology Integrated Program aims to connect "the myriad of transportation security equipment (TSE) to one network," so that not only are systems at a single airport connected to one another, they're also connected to central servers.

TSANet has been described as an overarching network that connects to local area networks at nearly 500 airports and TSA offices for the exchange of voice, video and data communications to share security threat information between airports and to broadcast information from TSA headquarters to field offices. A 2006 inspector general report found security problems with the network.

Rios and McCorkle purchased the Rapiscan system secondhand from an online reseller in California. The Rapiscan system generally sells for \$15,000 to \$20,000 in surplus, but they were able to obtain it for just \$300 because the seller incorrectly thought it was broken.



They also obtained and examined two other systems — one for detecting explosives and narcotics, and a walk-through metal detector — that they plan to discuss at a future point.

Last spring, Rapiscan lost part of its government contract for a different system it makes — the so-called nude body scanners — because the company failed to alter its software after privacy groups complained that the body images the machine produced were unnecessarily detailed. The company was forced to remove 250 of its body scanner machines from airports, which were replaced with machines made by a different company.

Then in December, Rapiscan lost the baggage screening contract too, following a complaint by a competitor — Smiths Detection — saying the company had used unapproved foreign parts in its system — specifically an “x-ray light bulb” produced by a Chinese company.

New software can thwart cyber attacks

Source: <http://economictimes.indiatimes.com/magazines/panache/new-software-can-thwart-cyber-attacks/articleshow/40343780.cms>

German scientists have developed free software that can help prevent cyber attacks.

Scientists at the Technische Universitat Munchen (TUM) developed the software which they claim can thwart five western intelligence agencies using the Hacienda software to identify vulnerable servers across the world in order to control them and use them for their own purposes.

According to a report published by journalists at Heise Online, Hacienda is a port scanning programme. Port scanners are programmes that search the Internet for systems that exhibit potential vulnerabilities. The report said that Hacienda is being put into service by the "Five Eyes," a federation of the secret services of the US, Canada, the UK, Australia and New Zealand.

"The goal is to identify as many servers as possible in other countries that can be remotely controlled," said Dr Christian Grothoff, Emmy Noether research group leader at the TUM Chair for Network Architectures and Services.



Grothoff and his students at TUM have developed the "TCP Stealth" defence software, which can inhibit the identification of systems through both Hacienda and similar cyberattack software and, as a result, the undirected and massive takeover of computers worldwide.

The connection between a user and a server on the Internet occurs using the so-called Transmission Control Protocol (TCP).

The user's computer first has to identify itself to a service by sending a data packet to the server. "This is the user asking, 'Are you there?'" said Grothoff.

The service then answers the user's request; within this response alone, there is often information transmitted that adversaries can use for an attack.

The free software developed by TUM researchers is based on the following concept: There exists a number that is only known to the client computer and the server.

On the basis of this number, a secret token is generated, which is transmitted invisibly while building the initial connection with the server.

If the token is incorrect, the system simply doesn't answer, and the service appears to be dead.

While similar defensive measures are already known, the protection capabilities of the new software are higher than that of extant techniques, researchers said.

► **Read more on Hacienda software at:**

<http://www.heise.de/ct/artikel/NSA-GCHQ-The-HACIENDA-Program-for-Internet-Colonization-2292681.html>



California builds a sophisticated Emergency Response Training Center

Source: <http://www.homelandsecuritynewswire.com/dr20140729-california-builds-a-sophisticated-emergency-response-training-center>

Citing the need for further emergency training, some Sacramento County officials have proposed a plan to construct a \$56 million training facility for Californian emergency responders which would handle all types of training and scenarios.

As the *Sacramento Bee* reports, the massive facility would have the ability to train crews in a nearly unlimited amount of situations. For example, emergency crews might be “required to douse a real 727 jet as it lies in pieces across a field...or make spit-second decisions on how to approach a derailed train leaking crude oil, or figure out how to quickly pull survivors out of a partially demolished and unstable building after a terrorist bombing or earthquake.”

“This is a one-stop shop,” said Sacramento Metropolitan Fire District Chief Kurt Henke,

Though the effort had been in the works for some time, a fear of increased shipments of crude oil throughout the state has prompted people such as the state Office of Emergency Services chief Kim Zagaris to lobby the legislature for the resources necessary.

“The governor and Legislature have been very good with us asking what those needs are,” said Zagaris, “We’re waiting to see what comes out of this.”

Proponents for the training center are also seeking grants, and money from private companies for support. Federal Express donated a 727 jet, and the group is also seeking rail cars as other props.

Representatives of the Valero Refining Company, which plans

on shipping around 100 cars of crude oil throughout the Sacramento area daily, have responded favorably toward the prospect of the ERTC.



“Anything you can think of, you can set it up at this facility.”

Though plans have not been fully confirmed for the site, construction of the facility — dubbed the Emergency Response Training Center (ERTC) — has already begun on 53 acres near Mather Field in Rancho Cordova.

“Much of the specialized training we require is only available out-of-state,” said Valero spokesman Chris Howe, “We have been in touch with state representatives about their plans. If a facility and program were available nearby and met our training needs, we would consider it.”

Henke noted that the planning group had not yet determined what it would charge emergency service

agencies to utilize the facility for training, but noted that in the recession environment of 2014, many groups would like to secure well-rounded training for their teams.

“We’re doing a cost analysis right now, to make sure we set a legitimate price point,” he said.

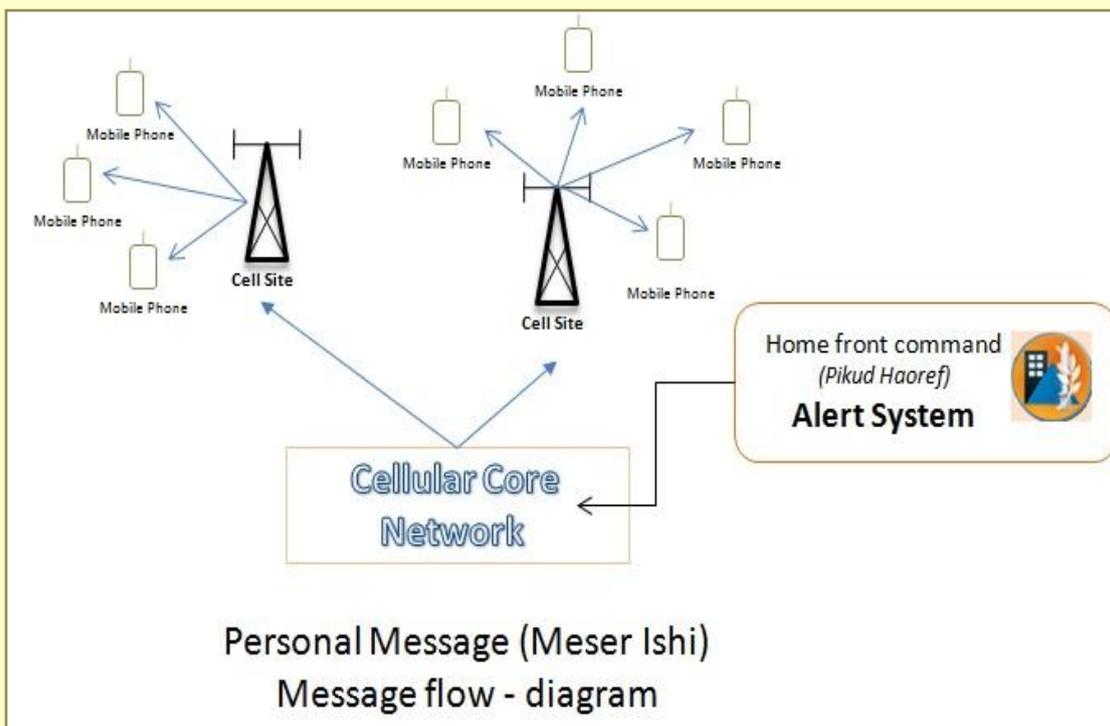


Israel's New Emergency Messaging System

Source: <http://i-hls.com/2014/07/israels-new-emergency-messaging-system/>

A new Israeli emergency messaging system began operations on Friday, July 25, covering almost the entire country. The system, known as "Meser Ishi" (Hebrew for "personal message"), sends text messages to almost every Israeli cellphone user – but so far only to subscribers of Israel's three main cellular service providers: Cellcom, Pelephone and Partner. These new messages, similar to

message is broadcast. Unlike the standard method of operation used in cellular networks – a process called paging, in which the network searches for a specific device for calls, SMS messages or web surfing – the CB process calls for the cellular site to broadcast to all phones connected to it at that moment, without any knowledge of their identity. It's a one-way process, and the cellular network has no way



normal SMS text messages, are sent when rocket and missile launches are detected, urging recipients to find shelter.

The Home Front Command emergency messages are broadcast on a unique channel called CB (Cell Broadcast), an inherent part of the ongoing communications process in every active cellular device – active even during calls, web surfing or use of various apps.

The CB channel is defined by the international communications regulation body, dictating its structure, application and use by end users to the cellular manufacturers (manufacturers of end point devices and vendors of cellular network core components).

The CB signal broadcast originates from a single cellular site or a group of sites (at the discretion of the cellular provider), sent to every device getting service from that site while the

of knowing if the subscriber received the CB message or not (unlike an SMS or a call, where the phone reports any failures or disturbances back to the network).

The IDF's Home Front Command divided the country into specific emergency regions, and the cellular providers, in turn, feed the CB messages only through sites providing cellular coverage for that specific region.

The original goal was to use the broadcasting channel to enable location-based services (LBS), such as advertising, weather, municipal messages and more. The main advantage of this system is its speed, the immediacy in which messages are receiving by phones, without relying on complex protocols or internet surfing conditions.



The low levels of demand for CB services, and location-based services in general, led to both end device manufacturers and infrastructure vendors to neglect the technology, causing many compatibility issues between manufacturers and cellular service providers, in Israel and abroad.

The “Meser Ishi” technology development process began in 2008 (!). Adapting the technology for local cellular networks, a project led by the IDF’s Home Front Command, began in 2010 with a huge, 30-million-shekel budget. Israel’s three main cellular providers, after initially resisting the changes, eventually complied with the regulations laid out by Israel’s Ministry of Communication. Most of the subscribers who own Android-based smart phones, in addition to owners of older devices, will receive the Home Front Command messages.

Aside from the many advantages of receiving alerts on cellular phones, there are a few technological and practical disadvantages:

- “Leakage”: Sometimes, usually due to a cellular network’s management of its radio resources, subscribers will receive alerts even if they are outside the alerted region

- Configuration: Some devices have various options that have to be configured by the user before enabling the service (language, channels, etc.)
- Regulation (1): There have been ongoing discussions regarding regulation for five years now, including Ministry of Communication cellular device import licenses requiring CB support.
- Regulation (2): The Ministry of Communication succeeded in forcing only the three main providers to cooperate with the Home Front Command. The licenses given to other providers by the state do require them to support CB messages, but that requirement is not enforced enough.

Subscribers of smaller cellular providers (Golan Telecom, HOT Mobile), whose service is not based on the infrastructure of the three main providers, will not be able to receive the Home Front Command CB messages. Subscribers of virtual providers (MVNO), such as Rami Levi and Alon Cellular, will receive the CB messages, subject to the same limitations as subscribers of the main providers (types of devices, coverage areas, etc.).

New Application – DefenCall

Source: <http://defencall.com/how-it-works/>

DefenCall makes customized personal emergency apps (with panic button) for smartphones.

The big red button initiates a call to 911 or your emergency services and simultaneously notifies your key personnel via text and email. Whatever your emergency protocols, notification lists, message

priorities, user base size, action plans, or existing apps may be, DefenCall can bring it all together for you to protect your people more efficiently by getting the right information to the right people right away.



So, if you, or persons you know, are responsible for the safety of a group of people, this

would be used by faculty, staff, students, employees, guards, drivers and anyone else who may contribute to or be helped by safety and security information and rapid response.

Core Functions

The “alerting” feature of DefenCall mobile applications offers three basic levels of protection:





Emergency Alert – This is the “big red button” prominently displayed on the main screen of every application. Tapping it triggers an immediate message to emergency responders, flashes a red screen on a monitor of the security personnel and it dials the emergency number automatically. The message includes the user’s name, GPS location and phone number.



“SMS” Buddy Alert – This message is triggered by tapping the triangular “caution” symbol icon and is sent to a user-configured list of contacts by text message. The message includes the user’s name, GPS location and phone number. These contacts can be friends, parents, colleagues or other people. This is intended for use in situations where the user wants help, but does not think the authorities need to be involved, because it is not a true emergency.



“Just Check In” – This “piece of mind” function is triggered by tapping on the green “check” icon and sends a message indicating the user is “OK” to a pre-configured contact by text message or email. Check-in messages include the user’s name, GPS location and phone number. This function is especially useful for reassuring parents or friends that everything is alright, for example when the user has reached a destination.

DefenCall Button Functions

Button	Action	Info	Recipient
		 "Emergency"	 Authorities Administrators
Message Content: DEFENCALL EMERGENCY - "User" has an emergency here <link>. Phone: 14155551212			
		 "Help"	 Friends
Message Content: DEFENCALL - "User" is here <link>and needs your help. Phone: 14155551212			
		 "Checking in"	 Parents
Message Content: DEFENCALL - "User" is safely checking in from here <link>. Phone: 14155551212			

Additional Functions

Additional functions enhance the protection features of DefenCall products with additional capabilities:

- **Safety Resources** – Every DefenCall product includes links to “what to do” information that could be crucial in an emergency. Basic information is provided by FEMA and can be customized to include links to information provided by user organization. Examples of information include everything from preventing theft to how to deal with alcohol poisoning or an earthquake.
- **Localized Resources** – User organizations can add additional content such as campus transit maps, links to services like campus escorts or Saferides and other services.
- **“Tip” Function** – Allows users to report dangerous or illegal situations. This ability to crowdsource data turns users into additional eyes and ears to increase safety. This can also be used within a “See Something Say Something” campaign.



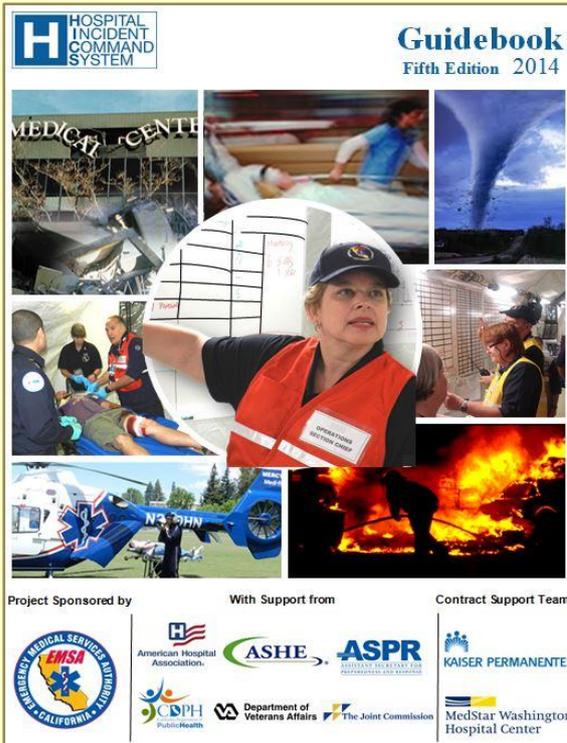
- **Auto Callback** – Emergency alerts can be configured to generate an automatic call from the monitoring dashboard to the user’s mobile phone.
- **Voice Call Buttons** – To connect to local police or security.

Hospital Incident Command System

Source:http://www.emsa.ca.gov/disaster_medical_services_division_hospital_incident_command_system

The California Emergency Medical Services Authority (EMSA) is pleased to release the Hospital Incident Command System (HICS) 2014 Guidebook. This Fifth Edition has been

Management Team" to eliminate any potential confusion with other engaged response teams such as deployed state or federal resources sent to help manage an incident



- ✓ A Patient Family Assistance Branch has been added under the Operations Section to address patient family needs during a response.
- ✓ An Employee Family Care Unit Leader has been included in the Support Branch within the Logistics Section to assist healthcare staff and clinicians by providing support for their families.
- ✓ Greater emphasis has been placed on incident action planning including the introduction of new, more practical tools.
- ✓ The Incident Planning Guides (IPGs) and Incident Response Guides (IRGs) have been reformatted and consolidated or expanded for improved application among hospitals.
- ✓ The HICS Forms have been revised to be more consistent with those used by the Federal Emergency Management Agency (FEMA). Additionally, there are 3 new HICS Forms available for hospital use: Incident Action Plan (IAP) Quick Start; the HICS 200: IAP Cover Sheet; and the HICS 221: Demobilization Check-Out.
- ✓ A new chapter addressing the implementation of HICS during off hours and for small and rural hospitals has been added.

expanded to meet the needs of all hospitals, regardless of their size, location or patient care capabilities. Lessons learned from real-world emergencies have been incorporated into this version of HICS from the 2009–10 National HICS Survey, the 2011 HICS National Stakeholders’ Summit, and from examples provided by the HICS Secondary Review Group members who once again evaluated the draft materials and provided their comments and suggestions to all proposed changes.

This revision includes the following updates:

- ✓ The term, "Incident Management Team" has been changed to "Hospital Incident

This guidebook and the accompanying HICS tools should be considered, "living documents." That is, as hospitals adopt these new materials, no doubt additional best practices and lessons learned will be considered. Consequently, recommendations will evolve and lead to the next HICS update.

► You can download the new version from source’s URL.



New Bay Area hospital is constructed to withstand the most severe earthquake

Source: <http://www.homelandsecuritynewswire.com/dr20140804-new-bay-area-hospital-is-constructed-to-withstand-the-most-severe-earthquake>



The new Stanford Hospital is being constructed to withstand the most severe tremors. The new hospital will be placed on 206 base isolators, enormous parallel steel plates with a sort of ball bearing suspension system between them, providing a buffer between the building and the moving ground. Each plate can move as much as three feet in any direction, allowing the building to shift up to six feet during seismic activity. Reducing horizontal movement during an earthquake minimizes the strain on a building’s vertical load-bearing structures. When completed, in 2017, the building will be one of the most seismically safe hospitals in the country, able to continue operations after an 8.0, or “great,” earthquake.

The odds of a major earthquake occurring in the Bay Area are high. Stanford University is located close to the San Andreas Fault, one of the world’s most active faults, and the Hayward Fault, which has been called a “tectonic time bomb.”

Numerous smaller faults run the length of the Peninsula. The U.S. Geological Survey predicts a 63 percent probability of a 6.7 earthquake within the next twenty years for the Bay Area — similar in magnitude to the quakes that rocked Chile and Japan in March.

A Stanford University release reports, though, that the new Stanford Hospital is being constructed to withstand the most severe tremors. When completed, in 2017, the building will be one of the most seismically safe hospitals in the country, **able to continue operations after an 8.0, or “great,” earthquake.**

Buffer system

The new hospital will be placed on 206 base isolators, enormous parallel steel plates with a sort of ball bearing suspension system between them, providing a buffer between the building and the moving ground. Each plate can move as much as three feet in any direction, allowing the building to shift up to six feet during seismic activity. Reducing horizontal movement during an earthquake minimizes the strain on a building’s vertical load-bearing structures.

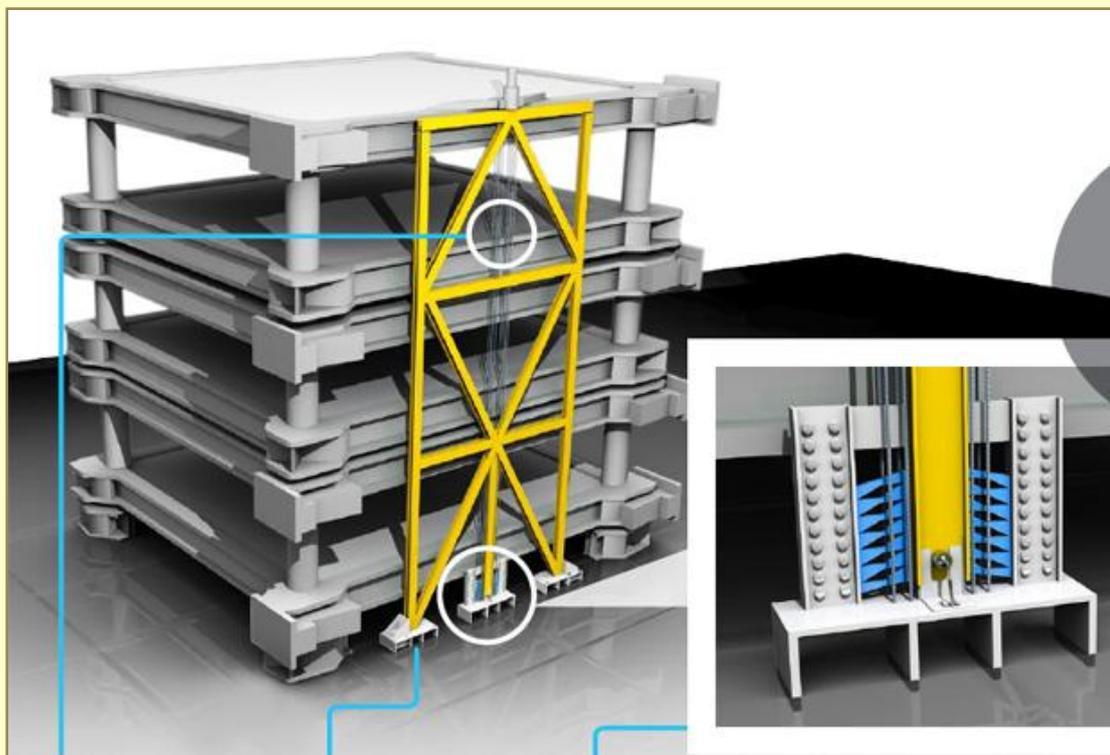
Because the base of the hospital is able to move at the same rate as the shaking ground, the building itself will barely shift.

“During an earthquake, the earth jerks one way and then another — as if you are standing on a carpet that is being pulled back and



forth,” said Bert Hurlbut, vice president of construction for the new Stanford Hospital. “But we’re talking about a tremendous force of horizontal acceleration. Since it’s impossible to

super-sized ones each weighing 8,900 pounds (4.5 tons). Two years in the making, the steel plates were cast in Texas and manufactured by Earthquake Protection Systems, a design firm



prevent an earthquake, we’re building structures that keep people safe by dampening the energy and ensuring structural integrity. Following Southern California’s devastating Northridge earthquake in 1994, the California State Legislature mandated strict seismic safety regulations for facilities that provide emergency or surgical services. Lucile Packard Children’s Hospital Stanford is incorporating a different but equally efficient system for seismic safety into its expansion project, which will open to patients in 2017.

Safety measures

The release notes that because Stanford is the only designated level-1 trauma center on the Peninsula, it is imperative for the hospital to be up and running in order to receive the brunt of casualties in the event of an emergency. The hospital is recognized by the American College of Surgeons as being capable of providing total care for every aspect of injury — from prevention through rehabilitation — for both adults and children.

Two sizes of base isolators have been custom-made for the hospital: 154 “large” ones each weighing 5,400 pounds (about 2.5 tons) and 52

in Vallejo. Hoisted in place by massive cranes, many of the base isolators already have been positioned thirty feet below ground level on supports that have been dug 100 feet into the earth. Their design is so precise that there is only 1/32 of an inch of space around each bolt that holds them in place. The design also allows enough leeway for the building to be jacked up if any of the isolators need to be checked or replaced.

Construction challenges

“The base isolators are only part of the solution,” Hurlbut said. “The building and all its components also have to be able to move and not touch anything.”

That means the hospital’s concrete and steel foundation has to be constructed with a cushion of air around it, and any structural elements that contact the ground have to be flexible as well. Each doorway, staircase, and ambulance bay is designed like a drawbridge so that it can slide back and forth, and all pipes and utility connections — medical gas, diesel, water, electricity, etc. —



have to be able to move in any direction as well. The foundation walls, thirty-five feet deep, are shored up with 50-foot steel beams and 70-foot tieback rods placed at an angle to create a kind of bucket in which to position the building. The pedestrian bridge that will connect the new Stanford Hospital with the existing hospital facility has been a particular challenge, said Hurlbut. The solution was to create pin joints at each end so that it could move almost 5 feet in any direction. "It's sort of like a jet walkway

connecting you from the gate to your plane," he said.

To facilitate all the ongoing problem-solving needs for such a complex project — and to stay on schedule — the architects, engineers, general contractor and subcontractors work together in an open compound adjacent to the construction site.

"Construction, design and operations all go hand in hand," Hurlbut said. "We've made the process fully integrated."

Kansas, Missouri invest in tornado safe-rooms

Source: <http://www.homelandsecuritynewswire.com/dr20140804-kansas-missouri-invest-in-tornado-saferooms>

Last year's tornado season prompted officials in Kansas and Missouri to invest heavily in safe rooms to shelter residents from future severe weather events.



The Garrison Community Center in Kansas City will construct a safe room this summer, funded in part by grants from the Federal Emergency Management Agency (FEMA). The 1,300 occupancy safe room will be built to withstand the highest-rated tornadoes, said Bob Lawler, project manager of Kansas City Parks & Recreation Department.

Emily Dunavent, vice president of the American Tornado Shelter Association and director of development for **Atlas Safe Rooms**, a Joplin-based safe room installer, has seen a rise in safe room inquiries from cities and businesses.

Last week officials in Crocker, Missouri opened a new school cafeteria that doubles as a

safe room, built to withstand tornado winds of up to 250 mph, and can survive being hit by a 67 mph projectile vertically or 100 mph horizontally. "If you read the sign outside, it is hundreds of miles per hour wind this building could take from a direct hit by a tornado... if you look at the steel beams, the concrete, it is unreal," Crocker R-II School Board head Kris York said. "In Joplin, 116 people lost their lives because they had no place to go." The cafeteria was built with \$776,000 of FEMA funds. The *Kansas City Star* notes that schools tend to be popular choices for safe rooms, but new funding from FEMA is helping cities build safe rooms in other public spaces. In Johnson County, the juvenile detention center and two Public Works administration buildings have received FEMA grants to build safe rooms. FEMA has agreed to provide 75 percent of the funds needed to build safe rooms for public use, but the rooms must meet a number of requirements including having a back-up generator, bathrooms, and thick concrete walls.

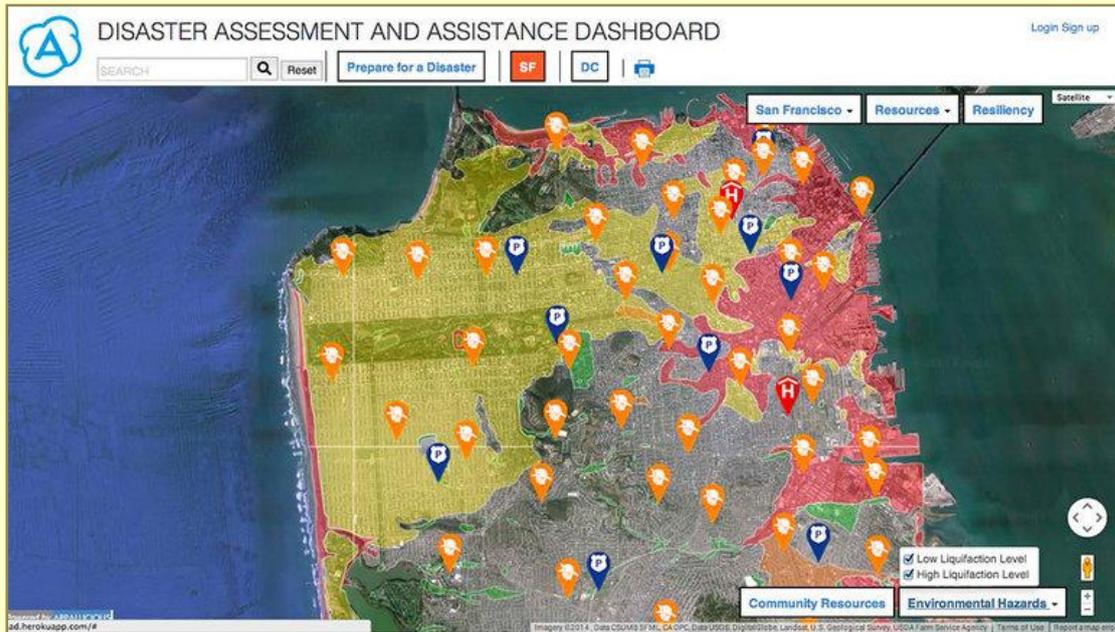


Tech firm creates software pairing response systems with open data

Source: <http://www.homelandsecuritynewswire.com/dr20140805-tech-firm-creates-software-pairing-response-systems-with-open-data>

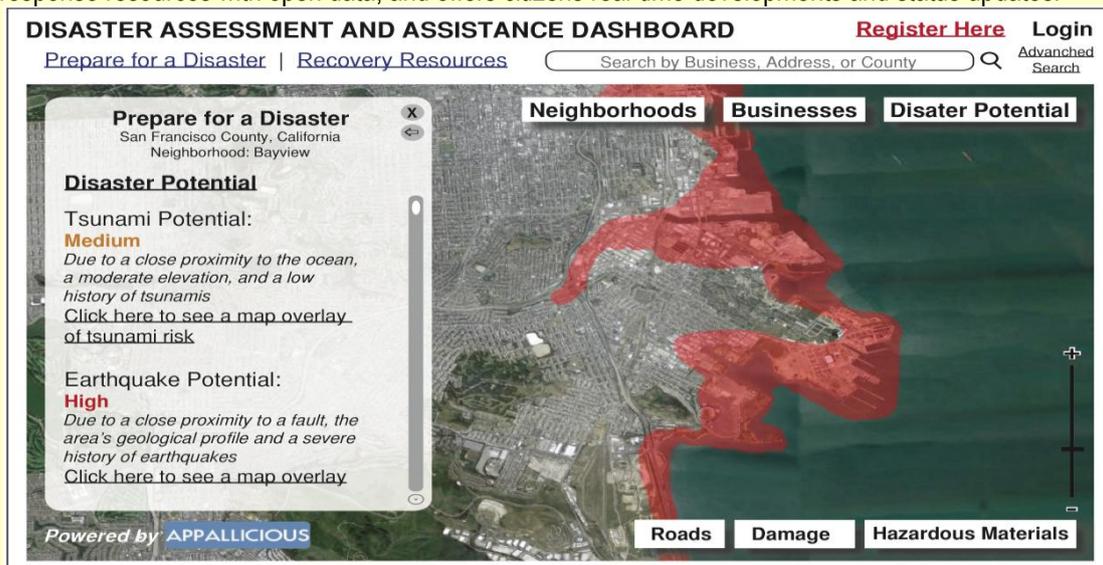
Appallicious, a San Francisco-based open data tech company, has unveiled what it refers to as the Disaster Assessment and Assistance Dashboard (DAAD). The application, still in the beta testing stage, was shown at the Innovation for Disaster Reponse and Recovery Demo Day, held at White House last week.

The company says that **DAAD offers a combination real-time data and agency notations that combine to aid and coordinate responses.**



56

Yo Yoshida, the founder of Appallicious, called upon by the Federal Emergency Management Agency (FEMA) to create the system, said that the platform is being billed “as a solution that pairs local disaster response resources with open data, and offers citizens real-time developments and status updates.”



Thanks largely to the abundance of open data, the dashboard is able to harness emergency response data in real-time and across multiple departments and agencies. Once fully operational, it will function as a central hub for information in the event of a



disaster — using more than 100 different interfaces that upload data. Additionally, the hub will work in accordance with all manner of local government organizations such as fire stations, police stations and hospitals to further create a larger picture during the actual moments of an emergency. Also of interest is the ability of DAAD to link to local labor and financial resources to operate a community economy as a further tool. The dashboard allows residents and companies to post their skills (such as CPR training), locations and equipment — all of which ultimately might aid in recovery. “It’s something that breaks down the barriers of all the silos of all the different departments [responding to a disaster], so you can create these high-level layers that help everyone facilitate and communicate at so many different levels, both pre-disaster and post-disaster,” Yoshida said. Following the FEMA endorsement, San Francisco District 2 county supervisor Mark Farrell, said that the city adopted DAAD because of “its ability to centralize help for residents.” Yoshida has disclosed that Appalicious are in discussions with other metropolitan cities, including Washington D.C., about the possibilities of incorporating the system elsewhere. The dashboard is available as a free option for smaller cities who can also customize and upgrade the application based on need.



White House Innovation Day Highlights Disaster Response, Recovery

By Elaine Pittman

Source: <http://www.emergencymgmt.com/disaster/White-House-Innovation-Day-Disaster-Response.html>

Emergency managers converged with the tech community in Washington, D.C., to discuss tools that can create more resilient communities and also positively impact disaster preparedness, response and recovery. The White House Innovation for Disaster Response and Recovery Initiative Demo Day on July 29 showcased new innovations in both government and the private sector that aim to aid the survivors of large-scale emergencies. The key goal is to “find the most efficient and effective ways to empower survivors to help themselves,” said U.S. Chief Technology Officer Todd Park, adding that there have been many technological advancements since Hurricane Sandy in 2012. “We all know that tech in the wake of a disaster isn’t helpful,” Park said. So the demo day sought to highlight new initiatives and how

emergency managers can work with and benefit from them. “You all here today and the effort that’s associated with this really do help bring the whole-of-nation approach to building preparedness because it relies upon integrating the efforts of the private sector, nongovernmental actors, communities, individuals, federal, state, local, tribal and territorial governments,” said Rand Beers, deputy homeland security adviser to the White House National Security Council. “What we need to do is to build on this collective group of people who are committed to making our country safer and to responding to these kind of issues.” Numerous government agencies and companies made announcements during the event, including:

CITY72 TOOLKIT — San Francisco launched an open source tool based off its emergency preparedness portal, SF72 portal. The City72 Toolkit helps emergency managers create their own site, while benefiting from lessons learned by San Francisco. Kristin Hogan Schildwachter, external affairs specialist for the city’s Department of Emergency Management, said current messaging focuses on pushing people to extremes and doesn’t build on current tools that the public is already using to communicate. The customizable Web platform is also in use in Johnson County, Kan., and branded as JoCo72.



AIRBNB — The sharing economy platform used to locate a place to stay now has memorandums of understanding in place with Portland, Ore., and San Francisco to work



with the cities before, during and after an emergency. Airbnb's director of public policy and civic partnerships, Molly Turner, outlined the four parts of the partnership:

1. to identify hosts who will house emergency workers and survivors;
2. to provide preparedness materials to hosts;
3. to provide emergency alerts to hosts and their guests about hazards; and
4. to provide community response training to hosts, helping them to become community leaders.

POWER OUTAGE DATA — Going forward, a number of electric companies will publish their power outage and restoration data in a standard format so that tools like Google Crisis Map can make the information easily accessible to the public. During Hurricane Sandy, this information wasn't openly available, leading Google to post links to the different utilities' sites but not being able to incorporate it into its information, according to Nigel Snoad of the company's Crisis Response and Civic Innovation arm. He also said another addition is that Google will include crowdsourcing capabilities in the Crisis Map.

LANTERN LIVE — Inspired by lessons learned from Sandy where situational awareness was lacking, particularly around the status of fuel and which gas stations were open, the U.S. Department of Energy is preparing to beta test Lantern Live, a new mobile app. Its features will include: the status of gas stations; the ability to report a power outage and downed power lines with geolocated information; and emergency preparedness tips.

DISASTER ASSISTANCE AND ASSESSMENT DASHBOARD — Appalicious launched a new disaster dashboard that aims to make rebounding after devastation more manageable.

GEOQ — The National Geospatial-Intelligence Agency announced its crowdsourcing tool, GeoQ, which allows users to upload geo-tagged photos of an area impacted by an emergency. Raymond Bauer, the agency's technology lead, said the tool is available for anyone to participate or work with the code via open source.

NOW TRENDING ON TWITTER — Helping emergency managers and public health officials, a new website, nowtrending.hhs.gov, searches Twitter data for health and natural disaster topics and analyzes that data. Karen DeSalvo, national coordinator for health IT, said the tool scours social media and looks for topics that could turn into public health emergencies.

DISASTER DATA — Coming soon, the new site disaster.data.gov aims to become a resource for preparedness and can also be used during and after an emergency. More than 100 tools from the public and private sectors have been submitted for inclusion on the site, and it will also host disaster-related data sets.

Additional announcements made at the event, via information from the White House, include:

The DHS and the Zoonotic and Animal Disease Defense Center of Excellence are piloting the AgCONNECT suite of pluggable mobile and Web-based desktop applications in 15 states and more than 60 laboratories.

Getaround is launching a disaster assistance policy and Web portal to help educate people about how to find or share a vehicle following a disaster.

Microsoft is adding the Yammer survivor network to its disaster-response program's portfolio of solutions for use in the wake of a disaster.

NPR Labs developed an emergency alerting system that could provide timely emergency information to the 36 million Americans who are deaf and hard-of-hearing, using a battery-operated radio and Android tablet.



SeeClickFix is sharing its database of citizen requests to help generate actionable data regarding the current state of infrastructure during and immediately after a disaster.

TaskRabbit announced a new mobile Web interface, the TaskRabbit Needs for First Responders, which provides a marketplace to connect local service providers with those who need assistance.

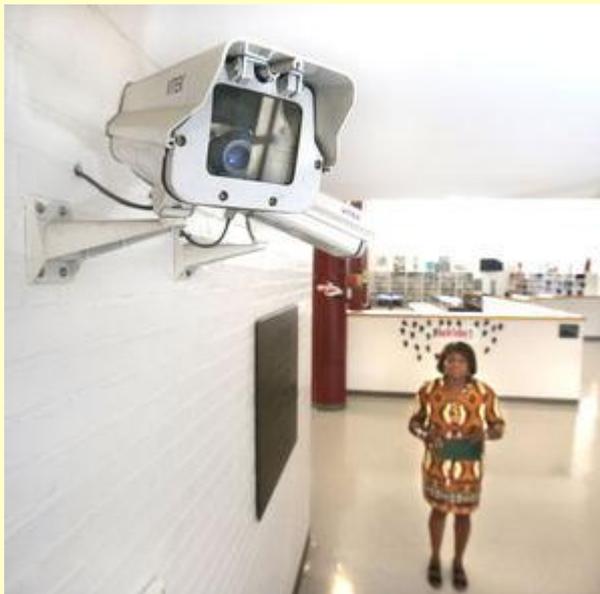
Twilio is open-sourcing a framework for developers to stand up effective communications solutions during emergency response.

The Weather Co. is building a localized alerting platform that will enable state, local and private authorities to manage and distribute alerts.

Elaine Pittman is the associate editor of Emergency Management magazine. She covers topics including public safety, homeland security and lessons learned. Pittman is also the associate editor for Government Technology magazine.

Alabama schools deploy 3-D virtual mapping to prepare responders

Source: <http://www.homelandsecuritynewswire.com/dr20140807-alabama-schools-deploy-3d-virtual-mapping-to-prepare-responders>



The Alabama Department of Homeland Security has recently institutionalized a detailed 3-D mapping system, called **Virtual Alabama**, which aims to create maps of public buildings in order to prepare responders in the event of a security emergency.

As the *Anniston Star* reports, the tactic behind Virtual Alabama is to immerse local responders to the intricacies of key structures before the knowledge is ever needed.

Recently, like other places within the state, the city of Anniston is developing maps of the county's school's in order to prepare.

Darren Douthitt, the superintendent of Anniston City Schools, said "It's another

layer of security."

The program introduces first responders and school administrators to online images which are layered with information including emergency safety plans, the locations of hazardous materials, evacuation routes, and places designated as safety zones during disasters as well as live video surveillance feeds.

In the time of a crisis, emergency staff can have instant access to detailed information during the initial chaos that can be profoundly critical for the implementation of quick and effective operations.

Currently there are 36,000 users at more than 3,000 different agencies that are familiarizing with the software online. Virtual Alabama is only available for



government and education officials. Superintendents of schools also have the ability to choose which employees have access to the system.

Experts with the system, a 14-person staff located at Auburn University at Montgomery, are working to map the remaining schools in the state and incorporate them online. They are continuously training new administrative officials at the school, and report that of the state's 1,500 schools only 200 are still in need of mapping and training.

Regarding incorporating the software into the coming school year, Douthitt added, "A lot of people reacted to Newtown (the deadly 2012 school shooting at Sandy Hook Elementary in Connecticut). I'd rather have it and not need it, because we want to make sure our kids and our staff [are] as safe as possible."

IDIRA project – Interoperability of data and procedures in large-scale multinational disaster response actions

Source: <http://www.idira.eu/index.php/project>



IDIRA is a research project funded by the European Commission for a duration of four years (2011-2015), gathering eighteen partners to focus on the interoperability of data and emergency procedures in response to large-scale disasters.

In order to develop a new capability for more efficient multi-national and multi-organisational disaster response actions, a technological framework covering recommendations for operational procedures and a set of fixed, deployable and mobile components including data and voice communication assets will be developed and tested in real-life scenario trainings within Europe.



The intended end-users of the IDIRA developments are on-scene commanders and those overseeing the response to a disaster in the command and control rooms as well as strategic and tactical civil protection staff. The fixed IDIRA infrastructure will support them with relevant information from manifold sources for the preparation and response phase.



The deployable IDIRA infrastructure will perform as information hub and on-scene access point; it can be used during the response phase and will provide basic communication means as well as a shared information space for all involved forces integrating information about needs, resources and on-site conditions thus providing a shared operational picture enhanced by decision support functionality. The mobile components of IDIRA will be used by the commanding personnel on-scene for flexible interaction with the information space.

► **Partners:** Germany, Austria, **Greece** (National & Kapodistrian university of Athens, Ministry of Defense, Center for Security Studies, SatWays, NEA), UK, Italy, Czech Republic & Switzerland

The IDIRA Communication Network

During large-scale disasters, the on-site communication infrastructure is often destroyed or overloaded.



Consequently, emergency response organisations cannot rely on having a communication network operational. IDIRA supports the activities of international disaster response units by hardware and software solutions, which need an existing communication infrastructure to ensure the maximum benefit for the response units.

In IDIRA, an independent easy-to-install mesh-based broadband communication network for emergency response

organisations has been developed. This system can be installed within a few minutes. As it is based on WLAN technology, there is no need for an application of frequencies. Self-aligning antennas ensure that the system can be installed by non-expert users. So-called Wireless Gateways are spread across the operational area and span a mesh network. The tablet devices of the response units can access the network for interacting with the IDIRA system. The Wireless Gateways can be mounted on vehicles, existing poles or small transportable poles provided by IDIRA.

The communication network will be further enriched to provide as much offline functionality of the IDIRA system for the end-users as possible. The Wireless Gateways will be extended by so-called Communication Field Relays, which provide different uplink technologies and ensure that the basic IDIRA functionality can be accessed, even if the mesh-network and the uplink connections are not operational.



First-Time Application of IDIRA Components During Real Large-Scale Disaster

After several days of heavy rain in late May and early June 2013, ongoing flooding in Germany began. Flooding and damages have primarily affected southern and eastern Germany, including the State of Saxony. The flood then progressed down the Elbe River, leading to high water and flooding along their



banks. Thousands of people were affected and damages into the millions have been caused. During this difficult time, IDIRA results were for the first time applied in practical use to support real large-scale disaster management. The members of the IDIRA team, Kamen, Patrick and Marcel, were present in the affected region almost all of the time and supported the disaster management forces. Thereby Fraunhofer components that are integrated in IDIRA and other proven components for disaster management and control and communication were used by the staffs in Dresden, by the German Red Cross, by the local and regional command and control of fire brigades in the affected region at the border to the Czech Republic. In addition, IDIRA components are currently used for donations management for the support of the flood victims in close cooperation with the German Red Cross. IDIRA components are also currently used for collecting information about flooded areas from social media sources.

Bilateral Classroom Training in Greece, 4-5 June 2013

The Bilateral training (Greece - Italy) of the IDIRA project took place at the Center of Security Studies



premises. The aim of the event was to give a condensed overview on the procedures of international disaster management, especially regarding current and evolving IT systems for assisting it with the use of the IDIRA systems and functionalities. Existing knowledge on international disaster relief, covering both the Red Cross/Red Crescent as well as EUCP contexts, were deepened and in the consequent training and evaluation part, the end user participants had to solve the posed problems in a forest

fire scenario-based tabletop exercise, using the provided IDIRA software prototypes. The end users not only had to demonstrate their individual leadership and collaborative skills, but also prove the intuitive usability of the tested IDIRA IT-Systems. During the training, the consortium partners had the opportunity to present the results of the IDIRA project so far to numerous potential users coming from diverse domains (fire brigades, military, earthquake experts, police, rescue teams, etc.). The partners received



valuable feedback from the users which will support the progress of the IDIRA development. Fruitful discussions and extensive training sessions are a promising starting point for the trainings that follow the coming months, and for the further development of the IDIRA architecture and system in general.

Advances in Dubai Ambulance Service

Source: <http://www.thenational.ae/uae/health/new-red-ambulances-in-dubai-for-critical-patients#ixzz3A4AAI9Xi>

Ambulances in Dubai are to be colour coded according to what sort of patient they are carrying. Patients in intensive care, whose lives are at risk, will be transported in red ambulances. Pink ambulances will be assigned to expectant mothers and dark green vehicles to patients who are morbidly obese.



Light green ambulances are for people with special needs, and blue vehicles will be assigned to general cases.

Essa Al Ghafari, deputy executive director of Dubai Corporation for Ambulance Services, said the new coloured vehicles would be easily identified by drivers, who could then make way for the emergency services.

Ambulance chiefs complained last week that car drivers were causing crashes and risking lives by refusing to give way to ambulances rushing to respond to emergency call-outs.



Nine emergency vehicles have been involved in accidents since National Ambulance launched its service in February, because motorists failed to pay proper attention or yield right of way.

Ambulance disinfection system

A system to prevent the transmission of infectious diseases onboard ambulances will soon be



implemented by the Dubai Corporation For Ambulance Services (DCAS).



The technology, MicrosafeCare, can easily destroy viruses that infect the respiratory tract and is safe to use with no side effects. It is an aerosol disinfection system that sterilises hard surfaces.

Non-emergency patients' transportation

Khalifa Darai, chief executive of DCAS, told Al Ittihad, the Arabic-language sister newspaper of The National, that the product will protect paramedics as well as patients with communicable diseases, including influenza.

The system will be used in 170 ambulances and mobile clinics, and will apply to 1,100 personnel at DCAS who deal with patients, including 700 paramedics, 350 drivers and 50 emergency medical technicians.



The method can also be beneficial to the Roads and Transport Authority for use in public transport and Dubai Health Authority, Mr Darai said.

Specially adapted taxi-ambulances are to be used to transport people with disabilities, the elderly and non-emergency patients to and from hospitals, the Roads and Transport Authority has announced.

Awnak, only the third service of its kind in the world after the UK and Ireland, will use specially converted vans that allow for wheelchair access.

“The launch of this service signals the huge attention accorded by the RTA to the disabled and elderly, who have full rights and duties,” said Yousef Al Ali, chief executive of RTA Public Transport Agency.

“All community members are required to care for these segments [of the population] and provide them with all services to meet their needs and protect their rights as active individuals.”

At the moment 10 vehicles will be used during an initial three-month phase and 20 drivers have been picked to undergo training.



Texas coastal areas still unprepared for disaster

Source: <http://www.homelandsecuritynewswire.com/dr20140811-texas-coastal-areas-still-unprepared-for-disaster>

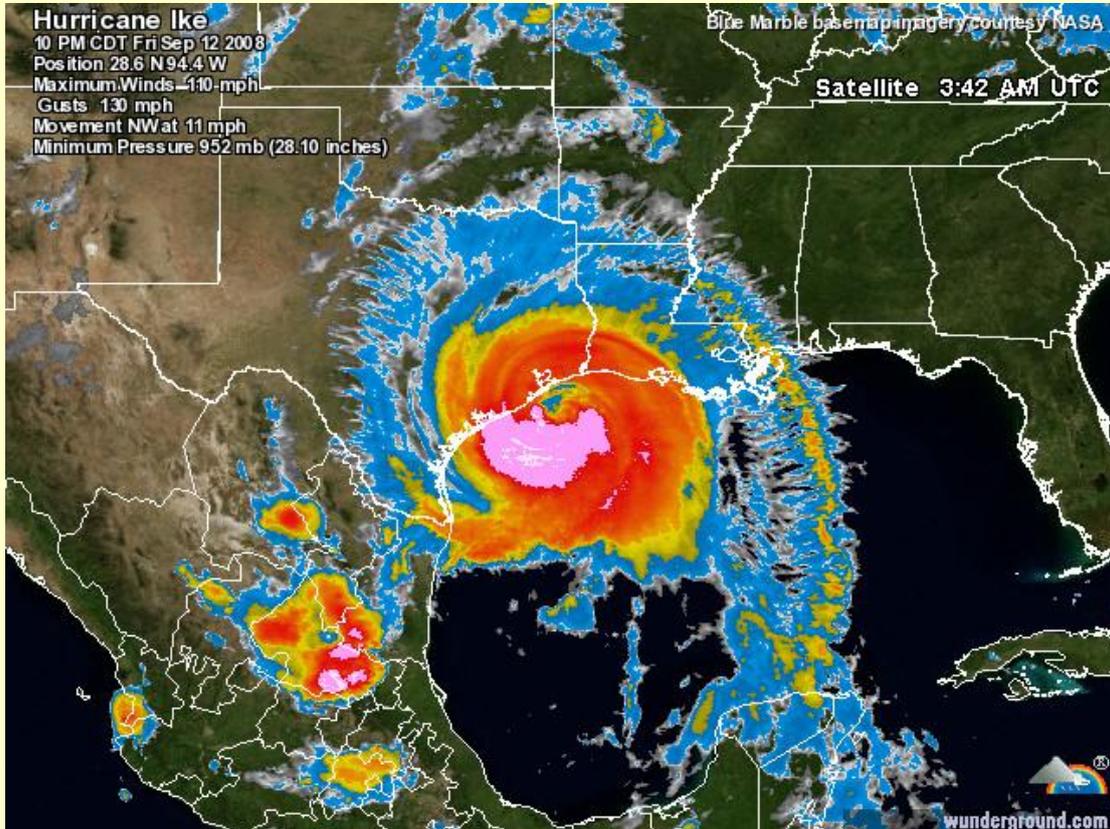
When Hurricane Ike struck Galveston, Texas in 2008, leaving billions of dollars in damages and at

least 100 people dead, residents knew that they were underprepared. Since 2009, less than half of the \$3.1 billion



allocated by the federal government to Texas for rebuilding efforts after Ike has been spent. Some considered it an improvement, though, since less than 20 percent of the funds were spent since 2011, when two different state

Katrina and Sandy, Texas has not developed a plan to protect its coast, and the state has failed to seek the same level of federal funding after Ike as the two other states sought after their hurricanes.



agencies were leading recovery efforts. Today, the General Land Office (GLO) has control and 45 percent of the recovery funds have been spent.

At last week's hearing of the Joint Interim Committee to Study a Coastal Barrier System, held on Texas A&M University's Galveston campus, experts warned legislators that the coast is underprepared for another Ike-like hurricane. "Are we ready for the next storm?" state Representative Armando Walle (D-Houston) asked during the hearing, noting that since 1980, Texas's Gulf Coast has experienced nineteen significant storms that occurred during the month of August.

No, "we're not protected. We are extremely vulnerable," said Jim Blackburn, an environmental lawyer from Houston who also directs the Severe Storm Prediction, Education, and Evacuation from Disasters Center at Rice University.

According to the *Texas Tribune*, unlike Louisiana and New York after Hurricanes

Today, researchers at Texas A&M University have proposed the "Ike Dike," a large seawall-type barrier or gate which would span the entire Galveston Bay, along with extending a seawall on Galveston Island across the Bolivar Peninsula. Critics say that plan would disrupt the local fishing industry by cutting off Galveston Bay from salty sea water that allows oysters and other species to thrive.

As researchers and government engineers try to recommend alternative solutions to protect the Texas coast, they face a challenge in deciding the most important areas to protect. Tony Williams, an environmental review coordinator at the GLO told lawmakers that not all plans will be accepted by all people, but a plan must be implemented soon. "People are going to ask, 'Why are you protecting this person and not me?'" However, he warned that if nothing is done, "people will say, 'Why did you not protect me when you had the opportunity?'"



2014-2018 FEMA Strategic Plan

Source: <http://www.fema.gov/media-library-data/1405716454795-3abe60aec989ecce518c4cdba67722b8/July18FEMAStratPlanDigital508HiResFINALh.pdf>

The 2014-2018 FEMA Strategic Plan advances the Agency’s mission to support our citizens and first responders to ensure that as a nation we work together to build, sustain, and improve our capability to prepare for, protect against, respond to, recover from, and mitigate all hazards. For 2014 to 2018, FEMA will focus on five



FEMA

5 STRATEGIC PRIORITIES

16 KEY OUTCOMES



PRIORITY 1: Be Survivor-Centric in Mission and Program Delivery

- Disaster services are transparent, efficient, and effective in meeting the needs of survivors.
- Local leaders and tribal officials are better prepared and positioned for effective recovery and mitigation.
- Individuals and communities know the steps to take, have the tools required, and take appropriate actions before, during, and after disasters.



PRIORITY 2: Become an Expeditionary Organization

- Unified and coordinated Federal response and recovery operations successfully support and complement state, local, tribal, and territorial incident operations.
- FEMA’s incident workforce is appropriately staffed and managed to rapidly mobilize, efficiently deploy, and effectively engage in multiple sustained operations in the response, recovery, and mitigation mission areas.
- Incident operations are efficient, timely, and predictable.



PRIORITY 3: Posture and Build Capability for Catastrophic Disasters

- Capability gaps are identified and addressed in National Preparedness System planning, training, and exercises.
- Partnerships, tools, and resources are in place to support national-scale response and recovery operations for catastrophic disasters.
- Survivors, bystanders, and grassroots organizations are better prepared and positioned to take immediate independent response actions in catastrophic events.



PRIORITY 4: Enable Disaster Risk Reduction Nationally

- The whole community uses the best-available data and analytic tools to make better risk-informed decisions before, during, and after disasters.
- Whole community partners make resilient investments in development and rebuilding.
- Congressionally mandated reforms are implemented to advance flood insurance affordability, financial stability of the National Flood Insurance Program, and reduction of the risks and consequences of flooding nationwide.



PRIORITY 5: Strengthen FEMA’s Organizational Foundation

- FEMA has a qualified, effective, and engaged workforce recognized for its excellence.
- Integrated analytics capabilities support effective and efficient operations and greater consistency and transparency in decision-making.
- FEMA’s strategy, resources, and performance outcomes align to maximize mission impact.
- Business processes are transparent and produce consistent, high-quality results.

strategic priorities, institutionalizing key improvements while building Agency capacity and strengthening national capabilities for disaster preparedness. The five priorities outlined below, along with their associated outcomes, will spur cross-Agency collaboration, guide



allocation of resources, and inform how all FEMA employees approach their work. These efforts will further integrate two strategic imperatives into the Agency's programs and operations: a whole community approach to emergency management and a culture that fosters innovation and learning.

► Read the full report at source's URL.

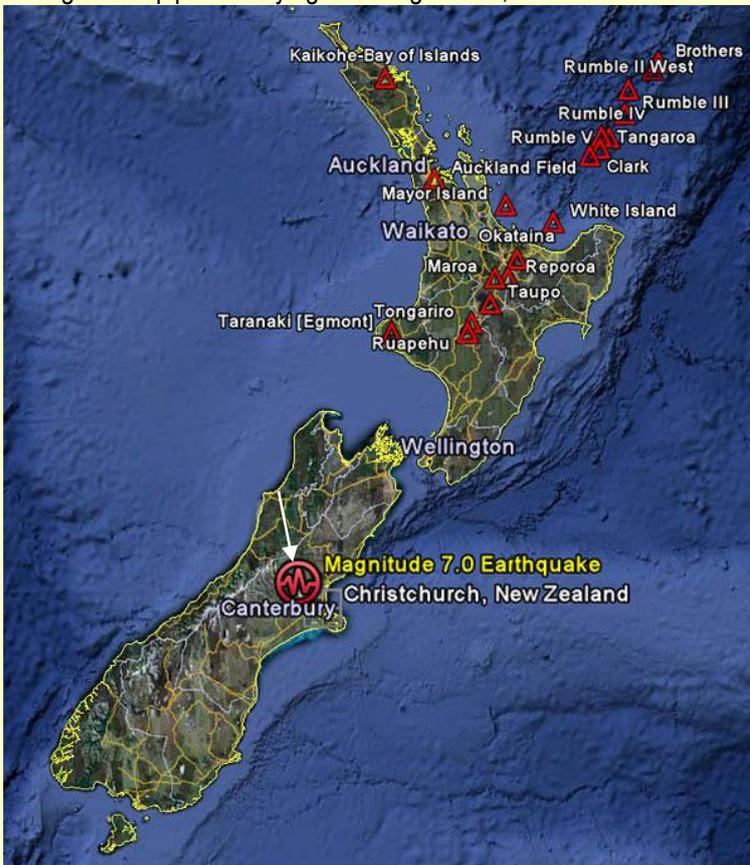
Resilience on the fly: Christchurch's SCIRT offers a model for rebuilding after a disaster

By David Killick (Citiscopes)

Source: <http://www.homelandsecuritynewswire.com/dr20140815-resilience-on-the-fly-christchurch-s-scirt-offers-a-model-for-rebuilding-after-a-disaster>

You don't see it, but you certainly know when it's not there: infrastructure, the miles of underground pipes carrying drinking water,

Most people here don't see the extent of repair work going on underground. They just notice roadworks and seemingly millions of orange cones that have sprouted up all over the city. Yet the organization created to manage Christchurch's infrastructure rebuild has a vital role, and it's become something of a global model for how to put the guts of a city back together again quickly and efficiently after a disaster.



stormwater and wastewater, utilities such as gas and electricity, and fiber-optics and communications cables that spread like veins and arteries under the streets of a city.

No showers, no cups of tea or coffee, no flushing toilets, no lights, no heating, and no traffic lights — a modern bustling city immediately shuts down. Factor in damaged roads, bridges, and retaining walls above ground, and the situation is dire.

That calamity hit Christchurch, New Zealand, in a series of earthquakes that devastated the city in 2010 and 2011.

It's called SCIRT, which stands for Stronger Christchurch Infrastructure Rebuild Team. It's a sort of consortium consisting of the local government, two national government agencies, and five civil engineering firms. They've teamed up to rebuild the city's water systems, underground utilities, roadways and other components of its so-called "horizontal infrastructure." SCIRT is tasked with spending

\$NZ 3 billion (\$2.5 billion U. S.) on more than 650 projects by December 2016. The work is almost halfway done and appears on track to be finished on time.

Just as important, SCIRT's mission is to rebuild these systems stronger and better able to withstand another quake. That's sometimes as simple as replacing broken earthenware and concrete pipes with flexible plastic ones. At a time when many cities face growing threats from natural disasters, SCIRT offers an



example for local leaders around the world to learn from.

“What we are creating is a template to create a disaster recovery framework for action,” says Duncan Gibb, SCIRT’s general manager. “The structure that we’ve used here is effectively transferred across from construction, and it can be used in construction anywhere.”

Waves of destruction

Before 2010, nobody would have imagined the terrible fate that befell this city of 360,000. Although New Zealand sits on a major tectonic plate boundary, the Christchurch fault lines were unknown. Nobody expected a big earthquake to strike in this location.

The first quake struck on September 4, 2010. It measured 7.1 on the Richter scale, but was centered just outside the city. It damaged

volcanoes” began to bubble up from below. It was the worst “liquefaction” event ever recorded anywhere, according to experts. Streets choked with silt and house foundations sank into the ground. Massive craters appeared in roads. Whole suburbs were declared “red zones” and abandoned. Other suburbs, mostly in the more interior west, fared much better and escaped with light damage. However, just about every household has been impacted in some way.

The overall cost of the Christchurch rebuild is estimated at \$NZ 40 billion (\$34 billion U.S.) — approximately 10 percent of New Zealand’s GDP. That compares with an estimated 2 to 3 percent of GDP for Japan to recover from the earthquake and tsunami of 2011.

The rebuilding of what goes above ground — the so-called “vertical rebuild” — is proving challenging. Many people have been battling with insurance companies and a government-funded insurer known as the Earthquake Commission to settle claims on lost or damaged properties. Affordable housing and traffic congestion are now emerging as big problems. Disputes have arisen over how the city and the CBD should develop, the kind of



buildings, but no lives were lost. A second earthquake on February 22, 2011, measured 6.3 but was more devastating. It hit directly underneath the city at lunchtime, killing 185 people. A further 18,000 aftershocks continued to inflict damage throughout 2011.

The compact central business district of Christchurch was destroyed. Older masonry buildings crumbled. The neo-Gothic Christ Church Cathedral, the city’s namesake, looked like a bomb hit it. The top floor of the early twentieth-century building I worked in, The Press building, caved in, killing one and seriously injuring others. I was in the more modern central library at the time. It stood up well but will still have to come down. Hundreds of buildings have been demolished, including most high-rise office buildings and hotels.

On the eastern side of the city close to the Pacific Ocean, the ground liquefied and “sand

buildings that are needed, and who pays for them.

The horizontal rebuild run by SCIRT is faring much better. That’s vital, because the water systems, utilities and roads need to be in place before much construction can happen above ground.

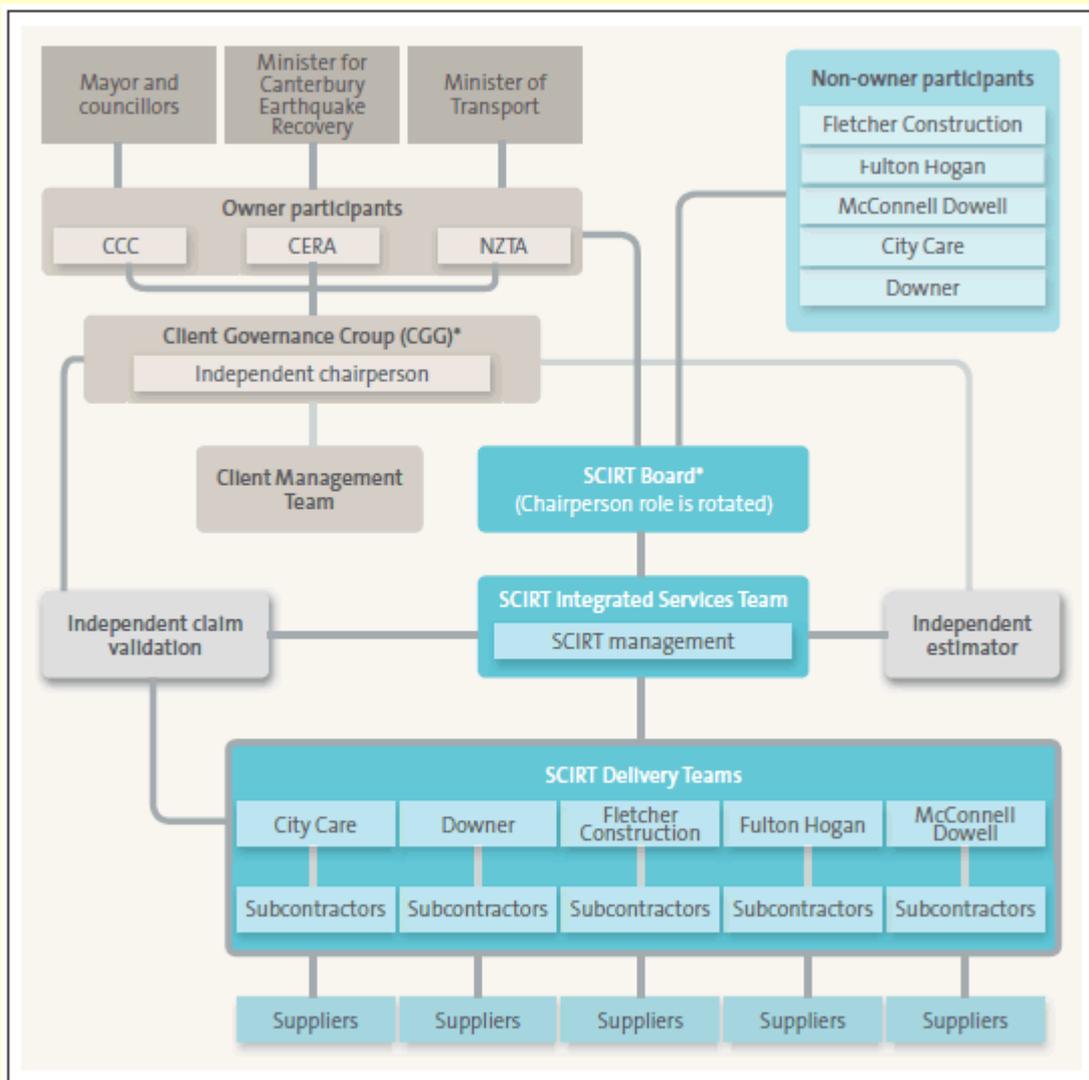
Alliance model

To understand what makes SCIRT’s approach innovative, you have to know how the conventional model for building infrastructure in New Zealand works. Normally, public-sector clients put out projects for tender, and competing civil engineering companies bid for the work. The process for awarding just one project can take months and runs the risk of construction delays and cost overruns.



Instead, SCIRT is a co-operative model. The public-sector owners of the infrastructure pay for the work, and lend staff to SCIRT to manage and coordinate projects and set

According to Gibb, an Australian who came to Christchurch to build SCIRT, "The whole objective was to create an organization that encompasses both collaboration and



overall direction. The five engineering firms are participants in SCIRT, and lend design and fulfillment teams to sketch out and deliver projects. All parties share the risks of building in a place where the geology itself has changed in ways that are still being revealed; they also share information with each other on what they're finding when they dig into the ground.

SCIRT comprises three government agencies: the Canterbury Earthquake Recovery Authority, Christchurch City Council, and the New Zealand Transport Agency. The engineering companies are: City Care, Downer, Fletcher, Fulton Hogan, and McConnell Dowell. The organization was created by the national government of New Zealand in September 2011.

competition." Companies still compete for projects and receive a fee, but the central agency makes the big decisions and sets priorities without going through the traditional hoops. SCIRT determines the budget and the fees, and allocates projects. Because costs and fees are set in advance, contractors do not make runaway profits.

SCIRT managers allocate work based on key performance indicators that include the cost, timeliness and value of the delivered projects. "Those who perform better get allocated more work," says Gibb. "Poor performance erodes the fee; good performance increases the fee." All contractors started out being allocated an equal amount of work; however,



each company's share has now altered. Gibb calls SCIRT's structure an "alliance agreement." It's based on a model originally developed by oil companies in the North Sea for drilling offshore oil rigs: "Lots of risk, lots of unknowns," Gibb says. All parties agree to explicit goals and objectives. "They are all focusing on the same outcomes that will either drive success for all parties or failure for all parties. In a traditional arrangement, a client can be really successful and the contractors do really badly, and vice versa."

In SCIRT's model, construction organizations maintain their own independence, systems and procedures. By being independent, they ensure safety, quality, environmental, and commercial outcomes are optimized; there is no unnecessary duplication of procedures. That is also a win for public funders, through savings on bureaucracy.

Advantages are time savings, control over budgets, less complexity, and — as engineers



love to say — just getting things done. Efficiency and performance are paramount. Funders, contractors and the public are expected to benefit. It's hard to argue with the results so far: Cost escalations have been kept down and the budget is on track.

SCIRT sunsets in December 2016, when emergency repairs are complete. After that date, staff from the partner agencies and contractors will go back to their parent organizations.

Laurie Johnson, a San Francisco-based disaster recovery consultant who is studying what's going on in Christchurch, says the SCIRT model is one cities everywhere should

look at. "It's essentially bringing together the design, the construction and the funding into one organization that is working together seamlessly from beginning to end," Johnson says.

Public relations

Apart from its commercial model, SCIRT has won accolades for its engagement with a deeply rattled public. Rebuilding projects often close roads and make the city's bad traffic problem worse; SCIRT sends out regular emails announcing where projects will be underway so that drivers can plan their commutes. SCIRT even sends people out to knock on doors and distribute leaflets to make sure people know what is going on.

"We do a huge amount of traffic modeling and all sorts of work so that we sequence our jobs so they are close to each other to make sure that there's always an alternate route," Gibb says. "Then we've got to advise the public of what the route is."

Sometimes, SCIRT and the community will celebrate the completion of a project, such as last November's grand re-opening of a causeway that links the city with some of the seaside suburbs (the festivities included cake stalls and home-baked goods.) Engineers also have noticed that school kids are fascinated by the sight of machines digging holes in the ground, laying down pipes and paving roads. SCIRT has been running sessions at schools near work sites so that kids can learn more about construction and how to stay safe while works are in progress. Indeed, the whole city is a living workshop.

Gibb, who has thirty years of construction experience, says he was well prepared for the technical and management task, but the people side has been equally important. "I came along and thought this is a construction project," Gibb says. "Well, **actually, it's a disaster recovery project.** And when you take that into context and you understand that not only are the people in your team suffering from this but the people in the community, and when you are more mindful of that, you can actually work with minimum additional effort to help build the resilience back into the community."

Citiscopes is a nonprofit news outlet that covers innovations in cities around the world.

► Read more about SCIRT at: <http://www.oag.govt.nz/2013/scirt/part2.htm>



The world faces water shortage by 2040

Source: <http://www.homelandsecuritynewswire.com/dr20140730-the-world-faces-water-shortage-by-2040>

Three years of research show that by the year 2040 there will not be enough water in the world to quench the thirst of the world population and keep the current energy and power solutions going if we continue doing what we are doing today. It is a clash of competing necessities, between drinking water and energy demand.

Water is used around the world for the production of electricity, but new research results show that there will not be enough water in the world to meet demand by 2040 if the energy and power situation does not improve before then.

The analysis is included in two new reports that focus on the global electricity water nexus have just been published. Three years of research show that by the year 2040 there will not be enough water in the world to quench the thirst of the world population and keep the current energy and power solutions going if we continue doing what we are doing today. It is a clash of competing necessities, between drinking water and energy demand. An Aarhus University release reports that behind the research is a group of researchers from Aarhus University in Denmark, Vermont Law School, and CNA Corporation in the United States.

In most countries, electricity is the biggest source of water consumption because the power plants need cooling cycles in order to function. The only energy systems that do not require cooling cycles are wind and solar systems, and therefore one of the primary recommendations issued by these researchers is to replace old power systems with more sustainable wind and solar systems.

The research has also yielded the surprising finding that most power systems do not even register how much water is being used to keep the systems going.

By 2020 the water issue affects 30-40 percent of the world

"It's a huge problem that the electricity sector do not even realize how much water they

actually consume. And together with the fact that we do not have unlimited water resources, it could lead to a serious crisis if nobody acts on it soon", says Professor Benjamin Sovacool from Aarhus University.

Combining the new research results with projections about water shortage and the world population, it shows that by 2020 many areas of the world will no longer have access to clean drinking water. In fact, the results predict that by 2020 about 30-40 percent of the world will have water scarcity, and according to the researchers, climate change can make this even worse.

"This means that we'll have to decide where we spend our water in the future. Do we want to spend it on keeping the power plants going or as drinking water? We don't have enough water to do both", says Professor Benjamin Sovacool.

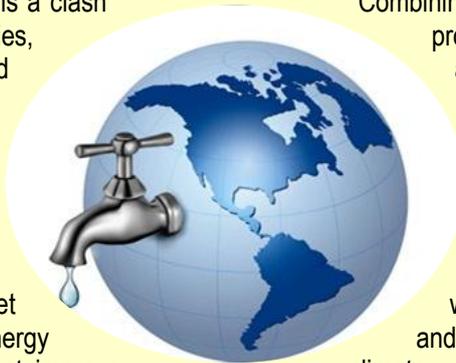
How to solve the problem?

In the reports, the researchers emphasize six general recommendations for decision-makers to follow in order to stop this development and handle the crisis around the world:

- Improve energy efficiency
- Better research on alternative cooling cycles
- Registering how much water power plants use
- Massive investments in wind energy
- Massive investments in solar energy
- Abandon fossil fuel facilities in all water stressed places (which means half the planet)

Close up on France, the U.S., China, and India

The team of researchers conducted their research focusing on four different case studies in France, the United States, China and India respectively. Rather than reviewing the situation on a national level, the team narrowed in and focused on specific utilities



and energy suppliers. The first step was identifying the current energy needs, and then the researchers made projections as far as 2040, and most of the results were surprising. All four case studies project that it will be impossible to continue to produce electricity in this way and meet the water demand by 2040.

"If we keep doing business as usual, we are facing an insurmountable water shortage — even if water was free, because it's not a matter of the price. There will no water by 2040 if we keep doing what we're doing today. There's no time to waste. We need to act now", concludes Professor Benjamin Sovacool.

Climate Change: If we pretend it isn't happening, will it go away?

By Lawrence M. Krauss

Source: <http://thebulletin.org/climate-change-if-we-pretend-it-isn%E2%80%99t-happening-will-it-go-away7333>

I happened to be in Canberra last week as the Australian government repealed its tax on carbon emissions, which has required the country's biggest emitters to pay as much as 25 Australian dollars (about \$23.50, US) per metric ton of carbon dioxide spewed into the atmosphere. With the vote in the Australian Senate, following a previous vote in the House of Representatives, Australia—one of the world's largest per capita emitters of carbon—moved from being well ahead of the international curve to the back of the pack when it comes to reducing greenhouse gas emissions.

The climate change debate that has raged in the public forum in Australia—and, in similar form, in the United States—has unfortunately been governed more by politics, ideology, and money than by facts. For example, much to my dismay, after appearing on a television program in Australia, on which I ended up debating a senator from the governing Liberal Party on issues that included climate change, I offered to come to his office to show him data on climate trends, including sea level rise and ocean acidification, with the hope that the data might affect the policies he advocated. He told me that he wasn't interested in such a discussion, because he had a constituency that supported his current opposition to carbon emission controls, and that is what mattered to him.

Of course, as a scientist, I feel particularly strongly that the public is ill served by politicians who ignore empirical evidence while making and speaking out on policy. But as the dramatic Australian vote made news worldwide, another, less-publicized set of legislative actions took place in the United States, and they could wind up being even

more insidious than the Australian climate change retreat. Rather than ignore the science associated with climate change predictions, one house of the US Congress attempted to ensure that the appropriate science on climate change would simply be discontinued.

On July 10, the House approved the fiscal 2015 Energy and Water Appropriations bill on a 253-170 vote. In the bill, Congress unfortunately cut funding for such things as renewable energy, sustainable transportation, and energy efficiency; perhaps even more worrisome, however, were a series of amendments successfully attached to the bill. Each would, in its own way, specifically prohibit scientists at the Energy Department from doing precisely what Congress should mandate them to do—namely perform the best possible scientific research to illuminate, for policymakers, the likelihood and possible consequences of climate change.

Oklahoma Republican Congressman James Lankford's amendment prohibited funding for "proposing or implementing any executive order related to the 'social cost of carbon.'" In this way, the Energy Department would presumably be prohibited from embarking on studies that might calculate the possible benefits of legislation that limits carbon dioxide emissions or the economic risks associated with climate change.

A second amendment by Arizona Republican Paul Gosar prohibited funding for the Energy Department's Climate Model Development and Validation program. One of the things that climate change deniers often pull out of their hats when arguing against acting to stem climate change is a claimed skepticism about the validity of existing climate models.



I have recently countered one such skeptic on television here in Australia by accepting this skepticism—and then challenging him to present what *his* models predicted. (Of course he didn't have any). The point was not merely rhetorical. If there is serious concern about the robustness of ongoing climate modeling, it is inconsistent with a desire to prohibit scientists from being able to improve their models.

A third science-defunding amendment, this time pushed by West Virginia Republican David McKinley, would prohibit the Energy Department from supporting climate change activities associated with the National Climate Assessment and the Intergovernmental Panel on Climate Change report. That's right: The Energy Department would be prohibited from responding to the two landmark reports that reflect the best international scientific scholarship available on climate modeling and the possible impacts of human greenhouse gas production, locally, nationally, and internationally.

It is one thing to decide, as the Australian government has sadly done, that short-term political expediency trumps long-term policy goals when it comes to reducing the impact of climate change. It is another, however, to

decide that the very possibility of human-induced climate change is so contrary to what one would *like* to believe—that scientific activities capable of producing factual results running counter to this belief are so threatening—that any such science should be prohibited.

The House appropriations bill is not likely to become law in its current form. The White House has already signaled its intent to veto the bill; the Senate would undoubtedly require changes before the bill came anywhere close to the president's signing desk. Still, the intent of these amendments, and the fact that they could pass a house of Congress, should concern everyone interested in the appropriate support of scientific research as a basis for sound public policy.

The analogy of an ostrich burying its head in the sand to avoid danger is clichéd but, even so, particularly appropriate to this case. An ostrich that buried its head in the sand on an ocean beach would seem particularly poorly situated to avoid a possibly rising tide. Sillier still: The ostrich that, with its head underground, refused to allow others to keep watch, to see if the tide comes in.

A theoretical physicist, Krauss is co-chair of the Bulletin's Board of Sponsors and director of the Origins Project at Arizona State University. The author of several books, including The Physics of Star Trek, Quintessence: The Mystery of Missing Mass in the Universe and Fear of Physics: A Guide for the Perplexed, he has won several honors for translating difficult scientific concepts into language general readers can understand. His most recent book is A Universe from Nothing.

Islamic State may soon unleash catastrophic flood on Baghdad

Source: <http://www.infowars.com/islamic-state-may-soon-unleash-catastrophic-flood-on-baghdad/>



On Sunday (Aug 03) the Islamic State, formerly ISIS, took control of the Mosul Dam during a battle with Kurdish forces.

The Mosul Dam is situated on the Tigris River in the western governorate of Ninawa, upstream of the city of Mosul. It is the largest dam in the country and the fourth largest in the Middle East holding at full capacity 2.7 cubic miles of water. It provides electricity for nearly 2 million people in Mosul.

The dam is considered the most dangerous in the world. It is estimated that a sudden collapse would submerge Mosul under 65 feet of water and Baghdad under 15



feet. Baghdad has a population of over 7 million. It is estimated 500,000 would perish if the dam failed.

Earlier this year ISIS took control of the **Fallujah Barrage**, a small dam on the Euphrates near Fallujah in Al Anbar Governorate.

Between January and April ISIS opened and closed the gates of the Fallujah Barrage ten times, causing extensive flooding in Anbar province.

The flooding resulted in the displacement of 715 families from Abu Ghraib, according to Iraq's Ministry of Migration and Displacements.



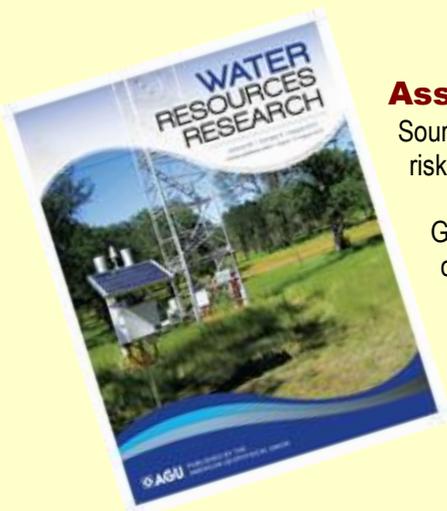
According to the leader of the Sons of Iraq Council, Mohammad Al-Hayis, ISIS had planned to use the dam as a weapon.

"ISIS has two objectives: on the one hand, they want to drown the areas surrounding Fallujah, but the sudden attack by the army foiled that plan; on the other hand, they want to cut off water supply to the central and southern governorates in order to give their war a sectarian dimension," Al-Hayis told Asharq Al-Awsat in April.

In June, as ISIS moved in on the Haditha Dam on the Euphrates, the Iraqi army announced it would open the floodgates of the dam to prevent ISIS from using it as a weapon.

"Alarmed army officers told employees to stay inside and to be prepared to open the dam's floodgates if ordered to do so, one employee said," The New York Times reported on June 25, 2014.

The Haditha Dam is the second largest in the country.



Assessing flood risk in a changing climate

Source: <http://www.homelandsecuritynewswire.com/dr20140805-assessing-flood-risk-in-a-changing-climate>

Growing consensus on climate and land use change means that it is reasonable to assume, at the very least, that flood levels in a region may change.

Then why, ask Rosner et al. in a new study, do the dominant risk assessment techniques used to decide whether to build new flood protection infrastructure nearly always start with an assumption of "no trend" in flood behavior?



A Wiley release reports that in an argument grounded in an analysis of the inherent limitations of statistical analyses, the authors suggest that researchers' typical starting assumption that flood behavior is not changing — even in the face of suspected trends in extreme events and knowledge of how difficult such trends are to detect — causes water managers to undervalue flood protection benefits, opening the door to unnecessary losses down the line.

When researchers assume no trend, statistical errors could cause them to overlook of the risks of underpreparing for changing flood conditions. Often, potential flood damage due

to underpreparedness far exceeds the potential cost of overinvesting in flood protection infrastructure. Flipping the process around, starting with an assumption that a change in flood conditions is occurring, would give critical attention to the risk of underestimating future floods, rather than only considering the risk of wasting money on unneeded infrastructure.

The authors propose a method of risk assessment that starts with the null hypothesis of "no trend" but that explicitly assesses the effect of statistical uncertainties that may cause them to misidentify real trends and the damages those trends might produce.

— *Read more in Ana Rosner et al., "A risk-based approach to flood management decisions in a nonstationary world," Water Resources Research 50, no. 3 (March 2014): 1928-42*



MSc @ Organisational Resilience (Part-time)

Source: <http://bucks.ac.uk/courses/postgraduate/MU1OGR9/#.U-xFh2P5nrN>

This programme will equip you with the skills to help your organisation function effectively in the event of business threatening events.

Qualification: MSc

Credits: 180

Study mode: Part-time

Location: High Wycombe

Duration: Two years

Start date: October 2014



Is this course for me?



In today's multi-risk world, and looking into the future, organisations must be prepared to anticipate, respond to and recover from unexpected and undesirable events.

Mr Phillip Wood MBE MSc
Head of Faculty Enterprise & Security

Risks and threats have multiple sources and impacts and failure to manage them to satisfactory conclusions can undermine operational and financial stability.

Businesses and organisations need to be able to manage their own interests and protect their products and services, alongside those of their stakeholders, and to manage their futures effectively.

If you have, or could have, a key role to play in the resilience of a business or other organisation, this course is for you.

76

What will this course cover?

With a clear focus on developing your confidence and capabilities in organisational resilience, this programme will equip you with the necessary skills and information to give your organisation the ability to continue to function effectively in the event of business threatening events.

Throughout the programme, you will apply current theories, concepts and practices to organisational resilience. We focus on learning that is anchored in reality rather than the sterility of pure theory, exploring real problems and identifying innovative solutions which can be applied effectively in the competitive and dynamic organisational environment.

Recognising the range of businesses that need to plan for resilience, you can tailor the programme to suit your needs and specialise in areas of particular relevance to your career. Therefore, on graduation, you will have developed a focused capability on the aspect of organisational resilience that affects you, with a broader mastery of related and linked disciplines and issues.

You will be able to develop and test theories and plans which will be directly linked to your area of interest or organisational needs providing relevance, and a solid academic basis for further development, research or career progression.

Our supportive course team is drawn from practising experts from resilience disciplines, as well as from the University's own academic staff. Due to their industry knowledge and academic expertise, our tutors can provide you with the practical, managerial and intellectual skills and knowledge which will set your organisation and your people apart when planning for and responding to resilience challenges.

We pride ourselves on the support we give to you face-to-face and electronically using our virtual learning environment. Utilising our online learning package helps maximise the time spent on relating the issues in the programme to your company and minimises your time away from your workplace.



This course has been designed to make high quality education as accessible as possible for those who are unable to attend programmes on-site, but with the requirement to adhere to the highest of academic standards.

You will also benefit from a series of workshops, one within each module.

Year One modules

- Business Continuity Management and Perspectives
- Civil Protection, Crisis and Emergency Management
- Research and Dissertation
- Security Management
- Threat, Risk and Impact Perspectives

What are the entry requirements?

Applicants will normally hold a good honours degree (2:1 or above) or equivalent, although we have a flexible approach to our application process and so relevant and appropriate work and career experience, for example in the armed forces, police, security industry or in business continuity and/or emergency management will be considered in lieu of qualifications.

For further details of our international English entry requirements, please visit our [international pages](#).

How much does it cost?

Fees for 2014-15 entry

Home and EU students: £8,350

Fees quoted are for the next intake and are subject to change. Fee costs for subsequent years are subject to rise with inflation or course delivery costs.

Funding: This programme is eligible for funding under the Ministry of Defence Enhanced Learning Credits (ELC) scheme. Our ELCAS number is 1682.

For fees for international students, visit our [international section](#).

77

How do I apply?

To apply for this course, please use our direct application form.

- [Bucks direct application form](#) (pdf)
- [Application guidance notes](#) (pdf)

Once you have completed the application form, please return it to us by email:

pgadmissions@bucks.ac.uk

or post it to:

Admissions and Recruitment
Student Experience Directorate
Buckinghamshire New University
Queen Alexandra Road
High Wycombe
Buckinghamshire
HP11 2JZ

For more information for home and EU students, see our [postgraduate applications section](#).

If you are an international student, visit our [international students section](#).

What are my career prospects?

This programme is designed to strengthen your understanding of the multiple facets of organisational resilience and equip you with the necessary skills that competitive organisations seek.

On successful completion of this programme, managers will have gained the requisite knowledge and analytical skills to enable them to perform at higher management levels in their organisations whilst recent graduates or people employed outside the resilience sector are more likely to be able to obtain employment in the industry. ■

