****

## http://r54.cooltext.com/rendered/cooltext1333426312.pngLake Chagan, The Atomic Lake Filled With Radioactive Water

Source: http://www.amusingplanet.com/2014/03/lake-chagan-atomic-lake-filled-with.html

During the hey days of Cold War, the Soviet started blowing up nukes all over northeastern Kazakhstan to investigate the possibility of using nuclear power for peaceful construction purposes such as moving earth, creating canals and reservoirs, drilling for oil and so on. The tests were carried out under the banner of “Nuclear Explosions for the National Economy”. This was the Soviet version of “Operation Plowshare” – a similar program devised by the U.S.

Having borrowed the terrible idea from the U.S., the Soviet program got underway in vigor and ended up being many times larger than the U.S. Plowshare program both in terms of the number of applications explored with field experiments and the extent to which they were introduced into industrial use. While the U.S. conducted 27 tests before realizing it was a bad idea and terminated the program in 1977, the Soviets continued right up to 1989 during which as many as 156 nuclear tests were conducted.

One of the better known tests is the January 1965 test at Chagan, on the edge of the Semipalatinsk Test Site in Kazakhstan. The Chagan test was designed to test the suitability of nuclear explosions for creating reservoirs. It was the first and largest of all detonations carried in the Nuclear Explosions for the National Economy program. A 140 kiloton device was placed in a 178 meter deep hole in the dry bed of the Chagan River so that the crater lip would dam up the river during periods of high flow. The blast created a crater 400 meters across and 100 meters deep with a lip height of 20 to 38 meters. Later, a channel was cut into the crater allowing it, and the reservoir behind it, to fill up with water.

The reservoir, known informally as Lake Chagan, still exist today in substantially the same form. The water continues to be radioactive - about 100 times more than the permitted level of radionuclides in drinking water, though 100-150 meters away dose levels were at background level. At that time of its creation, the Soviet government was proud of Lake Chagan. They made a film with the Minister of the Medium Machine Building Ministry, the one responsible for the entire Soviet nuclear weapons program, taking a swim in the crater lake and water from it was used to feed cattle in the area.

It was estimated that some 20% of the radioactive products from the Chagan test escaped the blast zone, and were detected over Japan. This infuriated the USA for violating the provisions of the October 1963 Limited Test Ban Treaty, which banned atmospheric tests. The Soviets replied that it was an underground test and the quantity of radioactive debris that escaped into the atmosphere was insignificant. After several subsequent interactions, the matter was eventually abandoned

# What if, …? The German answer to Fukushima

**By Laura Innerasky**

Source: http://www.cbrneportal.com/what-if-the-german-answer-to-fukushima/

**This month the Fukushima-Daiichi nuclear disaster marked its 3rd anniversary. The catastrophe occurred in March 2011, when a tsunami released by an undersea earthquake, hit the plant and resulted in a meltdown of three out of six nuclear reactors.**

After the occurrences in Fukushima, the German government resolved a distinct transition from a nuclear to a green energy policy. Their first reaction was the suspension of the 2010 lifetime extension of nuclear power plants. Besides this, a three months moratorium on nuclear power for the seven oldest and the “Krümmel” plants has been decided. The latter, has made headlines with several reportable incidents, including three reactor scrams (emergency shutdowns). Moreover, the enacted “energy concept 2050” (adopted in September 2010) now includes an accelerated pull-out from nuclear energy, determining shutoff-dates for the remaining nine active plants, with the last ones having to be decommissioned by the end of 2022 at the latest.

Besides these political changes the government now also took the incident as a cause to reconsider its emergency plan in case of a nuclear accident and purports to establish a nationwide standardization plan. From Fukushima it for example has been deduced that evacuation radius have yet been held to small. As a result all residents within a radius of now 5 km around the plant (instead of 2 km), the so called central zone, are to be evacuated within 6 hours. Also the radius of the middle zone has been expanded from 10 km to 20 km. An evacuation in this zone is supposed to happen within 24 hours.

In addition to this, the supply to the concerned population with highly dosed iodine tablets, which saturate the thyroid so that the absorption of radioactive iodine can be avoided, has been expanded. While it was previously only a circuit of 50 km said to be provided with the tablets, authorities are now supposed to be prepared for the provision of a 100 km circuit. **These expanded so called outer zones do now even include the cities of Hamburg and Munich, since two out of nine running nuclear power plants are being operated in a distance of less than 100 km away from those cities.**

All these adjustments were carried out based on the recommendations of the German Commission on Radiological Protection, which was instructed to examine the own emergency provisions after the incidents in Japan. It has been stated that the decisions made with the changes are now based on any possible consequences of a nuclear accident instead of its low probability of occurrence, so that precaution has been raised. Also Barbara Hendricks (Social Democratic Party of Germany), Environment Minister underlined that a nuclear accident like in Japan can basically be ruled out in Germany but that nevertheless decisions about civil protection should be made regardless of probabilities of occurrence. Due to the fact that there are several nuclear power plants in neighbouring countries, which are located near the border, she also stated that in addition to the adjustments of the German contingency plan, a Europe-wide standardization plan is advisable.

German disaster management for nuclear cases involves several institutions. First of all the management mainly is the onus of each of the sixteen Federal States, yet in close collaboration with the federal government. It for example gives out “Guidelines for the Disaster Management in the Vicinity of Nuclear Facilities” as well as other instructions concerning emergency procedures.

**There are eleven “Regional Radiation Protection Centres”, which come across as control points for queries, counselling, care and observation in case of an occupational radiation accident and they are coordinated by the Institute for Radiation Protection (IfS).** Support in emergency management is primarily provided by fire brigades. Furthermore civil protection organisations like the German Red Cross (DRK), the Technical Emergency Service (THW) or the German Lifeguard Association (DLRG) are committed to support; this makes Federal States and – Government depend on volunteer workers, since they account for a sizably part of these organisations. Additionally a supplement of civil protection induced the development of the Analytical Task Force (ATF) and the Medical Task Force (MTF) as two new institutions to yield additional potential. While the ATF supports local incident commands with specialized scientists and – measuring techniques for CBRN matters, the MTF assists medical services in civil protection with special abilities and potential reinforcement, including the decontamination of casualties. But although safety precautions are arranged, it seems like German citizens still prefer the abandonment of nuclear energy in general which is not only due to safety concerns.

A survey of the Ipsos Institute, carried out in 24 countries, showed that in **Germany has the highest share of its population opposing nuclear power energy (with 79%) compared to the other partaking nations.**The anti-nuclear movement has a more than 40 year old history starting in the 1970s. Just before federal elections in 2009 a spate of mass demonstrations commenced. Thousands consistently took to the streets and especially since Fukushima the public opposition intensified with many demonstrations having tens of thousands of participants involved. **In March 2011 for example 60.000 people formed a 45 km chain from Stuttgart to the power plant of Neckarwestheim.** Also parallel demonstrations in 450 different cities have been organized, like it happened just two days after the human chain with 110.000 participants and in the same month with up to 250.000 people on the streets.

**For the time being, already 19 atomic plants have been decommissioned.** In parallel, there are still nine operating nuclear power reactors left, which produced about 12 million tons of hard coal units (SEK) in 2013. Therewith 7,6 % of the primary energy consumption in the country has been covered with nuclear energy in the last year. Since the nuclear power phase-out is now a done deal this percentage will reach the amount of zero no later than 2022, hence enabling renewable energies to take over.

***Laura Innerasky*** *works as an analyst at IB Consultancy in Singapore.*

Fukushima’s Effect on Nuclear Preparedness in the U.S.

Source: http://www.emergencymgmt.com/disaster/Fukushimas-Effect-on-Nuclear-Preparedness.html

Palo Verde Nuclear Generating Station in Arizona

Three years ago, the tsunami triggered by an earthquake in Japan caused a catastrophic failure at the Fukushima nuclear power plant, leading to the release of significant amounts of radioactive materials beginning on March 12, 2011. It was the largest nuclear power plant incident to date — called “an extremely severe nuclear accident” by Japan’s investigative committee — and one that has changed planning and preparedness efforts worldwide.

**“Fukushima woke up the world nuclear industry, not just the U.S.,”** Allison M. Macfarlane, chairwoman of the Nuclear Regulatory Commission, told The New York Times.

As with all disasters, it provided a real-world example for emergency managers and the nuclear industry to compare their plans and procedures against. Arizona, for instance, is home to the Palo Verde Nuclear Generating Station, which was named the United States’ largest power producer for the 22nd consecutive year. Located about 55 miles west of downtown Phoenix, Palo Verde adds to the list of possible emergency scenarios that Arizona responders may one day meet. And to prepare for that possibility, planning and relationships have been built and enhanced for more than 30 years.

“We’re fortunate in the state of Arizona that we have a very close-knit community that does this planning for the Palo Verde Nuclear Generating Station, and that’s been the case since the plans were first developed in the early 1980s,” said Bill Wolfe, Radiological Emergency Preparedness Program branch coordinator for the Arizona Division of Emergency Management.

Learning from past experiences, both in the U.S. and internationally, has helped hone Arizona’s plans. Wolfe said the accident at the Chernobyl Nuclear Power Plant in Ukraine in 1986 and the impact on the Turkey Point Nuclear Generating Station in Florida during Hurricane Andrew in 1992 provided opportunities for the state to examine its plans and procedures. And the Fukushima disaster did the same.

“We don’t have many opportunities in this business to experiment with real radioactive releases, so we like to take advantage of what incidents do unfortunately occur,” Wolfe said. “We track the response activities from an offsite perspective, and we look at the documents that are generated as part of that.”

During the Fukushima response, there were issues with messaging, decision-making and public involvement early on, all of which were confirmed in Japan’s after-action report, published by the Fukushima Nuclear Accident Independent Investigation Commission. The report included important insights into the emergency response and provided information for Arizona officials — and emergency managers worldwide — to use to compare how they would respond to a real-world incident and what initiatives are already in place.

The commission’s report provided key recommendations for Japan, including:

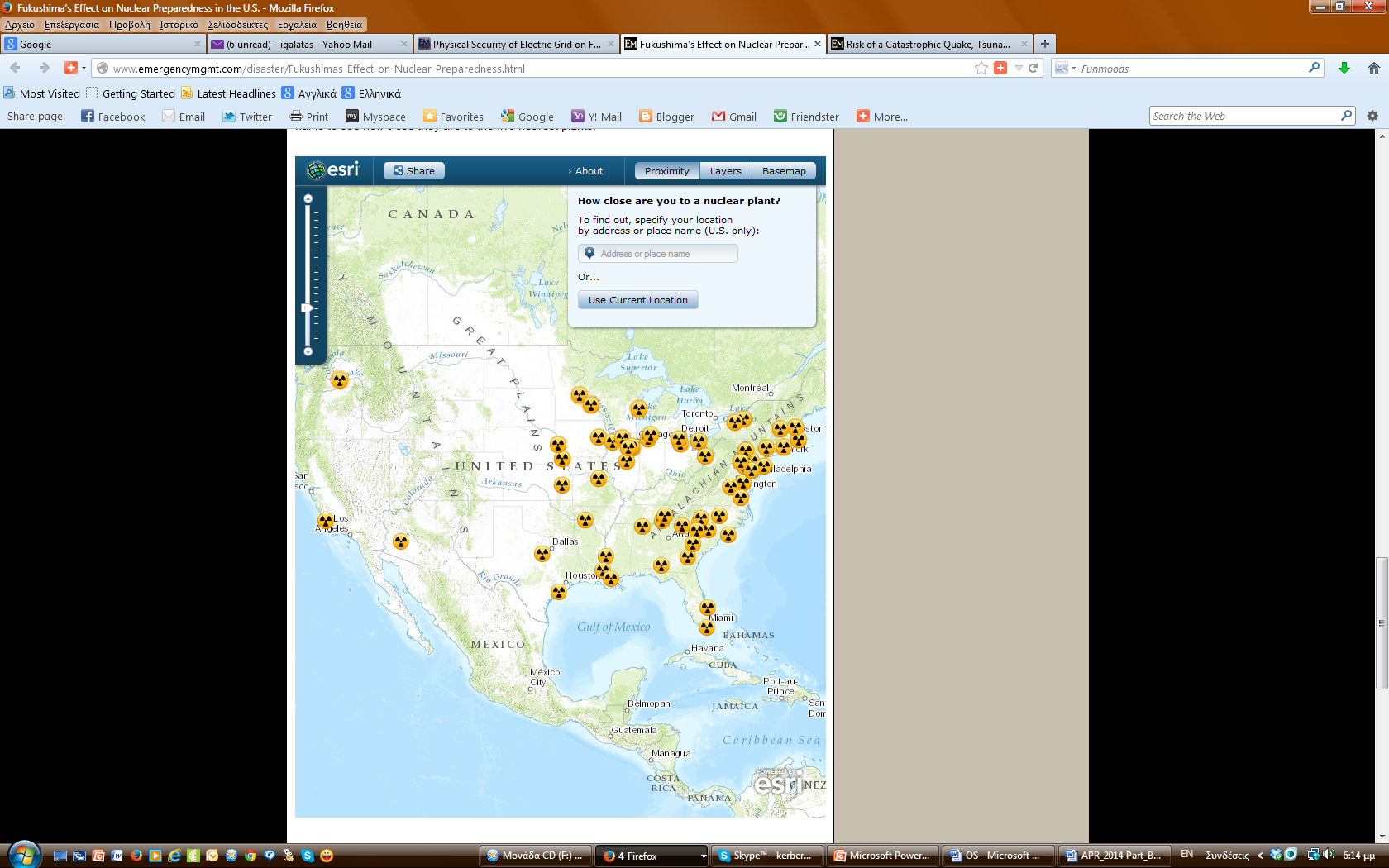
* creating a permanent committee to oversee the regulators;
* reforming the crisis management system and establishing a clear chain of command in emergency situations; and
* establishing a system to deal with long-term public health effects.

“We felt we had aggressively proceeded very well with a robust program,” Wolfe said, “and we didn’t see many things that were fundamental issues with our program.” He added that the report reinforced the process of knowing the planning zones and how they might be impacted, as well as helping to determine the validity of the 10-mile and 50-mile radiuses around Palo Verde that the state uses for planning.

In addition to planning, relationships are key in Arizona. Wolfe said there’s frequent communication between the state radiation representatives, local emergency managers and people from the power plant. Prior to working for the state Emergency Management Division, he was responsible for Palo Verde’s offsite program for 19 years and said that constant communication was in place then and allows for open conversations. “The continuing dialog allows us to share information as it happens, ask questions and to have an environment where we feel free to ask each other anything.”

That ongoing dialog also extends to the public. Messaging around a nuclear event isn’t done once a year; it must be constant and real-world examples provide an important time for public outreach. Residents also should be updated anytime they may be impacted by an event.

Emergency managers in the Pacific Northwest, where geologists warn that a similar scenario involving an earthquake and tsunami could strike at any time, are also using lessons learned from the Fukushima disaster. “Oregon recently wrote guidelines to help coastal communities annex land for emergency housing. And both states [Oregon and Washington] have new, 50-year plans to upgrade schools, bridges and utilities — though neither has committed the money,” reported The Seattle Times. Read more of Emergency Management’s coverage of lessons from Japan in Recovery Still Isn't in Sight 3 Years after Japan's Tsunami.

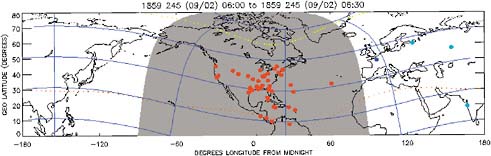
Additional planning tools are also available online. **Below is Esri’s (esri.com) nuclear proximity map, which shows nuclear plants in the U.S. with 50-mile rings around them.** Users also can enter an address or city name to see how close they are to the five nearest plants.

## Coalition sounds alarm about possible global EMP disaster

Source: http://www.homelandsecuritynewswire.com/dr20140404-coalition-sounds-alarm-about-possible-global-emp-disaster

A coalition that includes former speaker of the House Newt Gingrich and former CIA director James Woolsey has issued **a terse warning regarding apocalyptic effects that could result from a mass EMP (electromagnetic pulse) disaster or attack.**

Defense One reports that members of the coalition “are convinced that our **fragile electrical grid could be wiped out at any moment” from bursts of electrical energy caused by anything from a nuclear explosion to a solar flare from the sun, leading to chaos on a global scale.**

Peter Pry, a former CIA officer and head of a congressional advisory board on national security, as well as a member of the coalition, said “I think we’re running out of time. This gets translated into mass fatalities, because our modern civilization can’t feed, transport, or provide law and order without electricity.”

**The coalition’s members “believe a single nuclear blast at 300-400 kilometers in altitude — about the height of the International Space Station — could take down all power in the United States. Even an explosion just thirty kilometers up would take out the Eastern grid, which supplies three-quarters of the country’s power.”**

Pry goes on to say that “What happens post-detonation is not a pretty picture. You have massive industrial accidents. One hundred four nuclear reactors going Fukushima, spreading toxic clouds everywhere. Oil refineries burning down, oil pipelines exploding…Airlines crashing down.”

These disasters, Defense One point out, would just occur during the first day. The coalition believes that effects of such an event would destroy 90 percent of the world’s population in just a year.

The solutions debated in the U.S. House of Representatives include the GRID Act and SHIELD Act, both of which call for surge protectors on a national infrastructural scale. The GRID Act was voted down by the Senate in 2011, and the SHIELD Act is currently being championed by the coalition and awaits review by the House Energy and Commerce Committee.

In terms of potentially harmful solar flares, the world is already due for another. The **Carrington Event** (top photo), which occurred in 1859, interrupted the minimal electrical power grid already in place — the effects of which would be felt much more today given our modern dependence upon electricity.

## Possibility of “dirty bombs” a major terrorism threat

Source: http://www.homelandsecuritynewswire.com/dr20140401-possibility-of-dirty-bombs-a-major-terrorism-threat



**The International Atomic Energy Agency (IAEA) has warned that there were 140 cases of missing or unauthorized nuclear and radioactive material in 2013** — a pressing reminder that the possibility of possession of nuclear materials by terrorist organizations is both real and current.

Denis Flory, deputy director general of the IAEA, notes that even if the radioactive material is not weapons-grade, it can be combined with conventional explosives to create a “dirty bomb.”

He told Aljazeera America, “Even if they can’t be used for making a nuclear weapon, they can be used in radioactive dispersal devices.” Flory goes on to say that “member states had reported nearly 2,500 cases to the IAEA’s Incident and Trafficking Database since it was set up two decades ago. More than 120 countries take part in this information exchange project, covering theft, sabotage, unauthorized access and illegal transfers.”

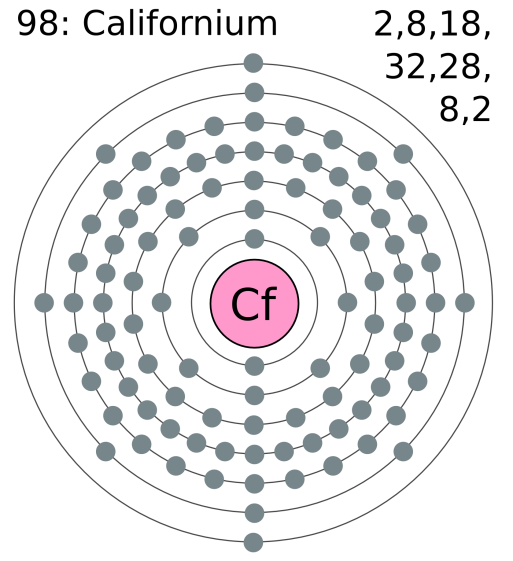
The issue is particularly poignant given the fact that leaders of 53 countries — including U.S. President Barack Obama — met last week at the Hague Nuclear Security Summit, where they called for more international action to help prevent radical groups from obtaining atomic bombs.

At the same time, additional pressure is on to ratify a 2005 amendment to the Convention on Physical Protection of Nuclear Materials. The hold up, as Aljazeera mentions, is that “There are still 27 countries — including the United States — which need to ratify the amendment, which expands the coverage from only the protection of nuclear material in international transport to also include domestic use, transport and storage.”

Matthew Bunn, a professor at Harvard University’s Kennedy School of Government, also echoed this, explaining that the lack of U.S. involvement has made it harder for the country to reinforce responsible safety measures.

He concluded that overall “The problem appears to be a combination of lack of sustained high-level attention by both the administration and Congress and disputes over unrelated issues.”

## Obscure element shows promise for nuclear waste storage

Source: http://www.homelandsecuritynewswire.com/dr20140331-obscure-element-shows-promise-for-nuclear-waste-storage

**One of the least known elements of the periodic table, californium, may hold the key to the safe and effective long-term storage of nuclear waste,** according to new research from Florida State University.

An FSU release reports that the research from chemists at that university has demonstrated that **californium (Cf) has an “amazing” ability to bond and separate other materials, as well as being extremely resistant to radiation damage**.

“It’s almost like snake oil,” stated lead researcher Professor Thomas Albrecht-Schmitt. “It sounds almost too good to be true.”

Albrecht-Schmitt says that the discovery should help researchers to design new and more effective storage containers for radioactive waste, as well as helping in the separation processes of radioactive fuel, thus allowing for greater fuel recycling.

“This has real world application,” he reiterated. “It’s not purely an academic practice. We’re changing how people look at californium and how it can be used.”

Cost may be an issue, though. Californium is relatively expensive (Albrecht-Schmitt notes that the five milligrams used in this research cost $1.4 million), but not much of it may be necessary.

*— Read more in Matthew J. Polinski et al., “Unusual structure, bonding and properties in a californium borate,”* Nature Chemistry *(23 March 2014)*

# Scientists need to educate the public over nuclear power safety

**By Robert Matthews**

Source: http://www.thenational.ae/uae/science/scientists-need-to-educate-the-public-over-nuclear-power-safety#full

When Hamad Al Kaabi set off for last week’s meeting of the International Atomic Energy Agency (IAEA) in Vienna, a place 8,000 kilometres away is likely to have dominated his thoughts – Fukushima.

As the UAE’s permanent representative to the IAEA, Mr Al Kaabi will know that what happened at the nuclear plant in Japan almost exactly three years ago is critical to perceptions of his own country’s plans.

These continue apace. The first reactors are now being built on the coast at Barakah, 300km west of Abu Dhabi City, by a South Korean consortium. If all goes to plan, around a quarter of the Emirates’ energy consumption will be met by nuclear power by 2020.

Yet the disaster at Fukushima has cast a long shadow over the very idea of nuclear power generation. It remains second only to the Chernobyl disaster of 1986, but its implications are at least as serious.

What happened to the Ukrainian reactor was the result of a series of almost unimaginable human blunders. Its design was fundamentally flawed, making it susceptible to runaway overheating. Its operators performed an unauthorised experiment that involved disabling what safety features it had.

And when the inevitable explosion took place, there was no “containment vessel” to prevent the radioactivity spreading far and wide.

In contrast, the Fukushima reactors were based on a tried and tested design, protected against both earthquakes and tsunamis, and had containment vessels.

Yet the “impossible” still happened. A devastating magnitude-9 earthquake struck this supposedly low-risk site on March 11, 2011.

Barely an hour later, a towering 14-metre tsunami struck, overwhelming the 10-metre seawall and swamping the reactors.

Acting together, these two natural phenomena succeeded in undermining the design safety features, leaving only the containment vessels to prevent utter devastation.

**The lesson seems clear – when it comes to nuclear power, even the impossible can’t be ignored.**

Anti-nuclear campaigners worldwide have seized on the event to make their case in their own countries. Last month saw demonstrations in Indonesia against plans to build further reactors, despite the power blackouts blighting the area.

Even a former chairman of the US Nuclear Regulatory Commission has spoken out against nuclear energy. Gregory Jaczko, now at Princeton University, said last month that the lesson of Fukushima is that society is not willing to tolerate accidents that are beyond prediction.

And why should we? What happened at Chernobyl and Fukushima was appalling, and if the nuclear industry can’t prevent them happening again, should we not guarantee they cannot by abandoning nuclear energy?

It is into this heated debate that some cold facts need to be brought in. The most important of these is that there is a huge gulf between perceptions of the consequences of Chernobyl and Fukushima and the reality.

Ask people to estimate the numbers of deaths from the radiation released by the Chernobyl explosion and figures often soar into the thousands. In fact, it led to around 60 direct deaths, which, while tragic, is barely half the toll in Ukraine’s coal mines every year.

Thousands of extra cases of cancer were caused by the radiation released, but the “C-word” obscures the fact that these are almost entirely thyroid cancers – which are rarely fatal. To date, the number of fatalities from these long-term effects is around 15.

As for the horror stories of deformed babies and mass outbreaks of leukaemia, these have proved entirely unfounded. While cases of both have occurred, there is no evidence they are at anything other than the “background” level.

**As a UN report into the health effects of Chernobyl put it: “Claims have been made that tens or even hundreds of thousands of persons have died as a result of the accident. These claims are highly exaggerated”.**

It’s a similar story with Fukushima. When the almost unimaginable scenes of devastation appeared, media reports warned of vast numbers of radiation-related casualties.

**Yet according to the official UN report, not one of the almost 25,000 workers involved suffered any acute effects from radiation.**

As for longer term effects such as thyroid cancer, these are likely to be so rare as to be undetectable against the general background.

Citing such statistics seems almost callous in the face of the undoubted suffering of those affected by these events. These people may not have been afflicted by the horrors invoked by campaigners, but they have unquestionably suffered severe mental anguish.

In both cases, fears of the radiation risk led to tens of thousands of people being evacuated from their homes. Their communities were broken up and their livelihoods destroyed. Parents feared for the health of their children and unborn babies.

While these fears may have been unfounded, the consequences have been anything but. Indeed, these constitute the real threat from a nuclear power disaster.

**In the months following the Chernobyl disaster, doctors noticed a rise in the numbers of abortions in some European countries affected by the fallout. The IAEA estimated the total number of terminations at more than 100,000. Anxiety levels and rates of psychosomatic illnesses also soared.**

The same has been seen in Fukushima. According to the Japanese government, **more than 1,600 evacuees have since died from causes “related to the disaster”, such as stress and even suicide. Fear of radiation can be far more devastating than radiation itself.**

**The failure of governments to tackle the misplaced fear of radiation is one of the greatest public health scandals of our time. It is leading to untold misery, even death, among thousands of people. If left unchecked, it could cause many more unnecessary deaths by robbing nations of a vital source of power.**

The fact is that the world needs nuclear power, as there is no short-term alternative. For all its failings, it is still the most reliable high-density, low-carbon source of energy currently available.

Tragically, those failings have been grossly exaggerated. A reactor explosion is rare, but it feeds into our worst nightmares.

The failings of the alternatives – from gas explosions to deaths incurred during fossil-fuel extraction – are so routine they rarely make headlines.

Some deserve wider circulation: how many realise that the world’s coal-fired power stations dump a hundred times more radiation into the environment – via isotope-rich fly-ash – than nuclear power stations?

Should we evacuate all homes around coal-fired stations? Of course not – the risk is trivial.

The risk of nuclear accidents should never be dismissed as trivial. The industry must learn the lessons of Chernobyl and Fukushima.

**And we can do our part by recognising that with nuclear power, our biggest fear is fear itself.**

***Robert Matthews*** *is visiting reader in science at Aston University, Birmingham.*

# Hundreds march through central Glasgow in nuclear weapons protest

Source: http://news.stv.tv/west-central/270610-hundreds-march-through-central-glasgow-in-nuclear-weapons-protest/

**Nuclear weapons protesters have staged a rally in central Glasgow, where Deputy First Minister Nicola Sturgeon addressed the crowds.** Organisers Scottish CND said between 1,000 and 2,000 people attended the rally in George Square on Saturday.

The demonstration, calling for the scrapping of nuclear weapons in Scotland, was preceded by a march through the city.

**Ms Sturgeon told the rally that the commitment from all of the Westminster parties to renew Trident at a cost of £100bn was a “monumental mistake” and that a Yes vote in the referendum was now the only way for Scotland to rid itself of nuclear weapons.**

Describing September’s referendum as “now or never” in the decades-long campaign to rid Scotland of nuclear weapons, Ms Sturgeon said: “For all of my political life I have been committed to the pursuit of nuclear disarmament – indeed, I was in the CND before I was in the SNP.

“But for all of my life I have lived under the shadow of the United Kingdom’s nuclear arsenal, based only a few miles away on the Clyde.

“It is, and always has been, unacceptable to me that such devastation could be launched from Scotland – but it is clearer than ever that all of the warm words from successive UK Governments about nuclear non-proliferation are just that – warm words.

“There are less than six months to go until Scotland decides what kind of country we want to be. One of the biggest choices we face is whether Scotland remains home to weapons of mass destruction, or whether we take this opportunity to remove them once and for all.

“Just think about it – as the world’s newest country, one of the first things an independent Scotland will have the chance to do is rid itself of weapons of mass destruction.

“I cannot think of any more powerful statement we can make to the world about what kind of country we will be, and what our place in the world will be.

“And instead of wasting money on weapons of mass destruction, we can start investing in a better, fairer Scotland – with our top priority being to start funding a transformational increase in childcare provision."

As well as the Deputy First Minister, Church of Scotland convener Sally Foster-Fulton, the city's Lord Provost Sadie Docherty and broadcaster Lesley Riddoch spoke at the rally.

A group of 50 protesters walking across Scotland from the Scottish Parliament to the Faslane naval base also joined the rally.

The "Spring Walk" aims to reach the naval base on the Clyde, where the UK's fleet of nuclear-armed submarines are kept, on Monday, April 7.

# Classified Nuclear Weapon Drawings Missing at Labs

Source: http://blogs.fas.org/secrecy/2014/04/drawings-missing/

**Classified design drawings used in the manufacture of nuclear weapons have not been properly and reliably maintained by nuclear weapons labs managed by the National Nuclear Security Administration (NNSA), the Department of Energy Inspector General said in a report last week.**

“NNSA sites could not always locate as-built product definitions or associated drawings for nuclear weapons and components in official records repositories.” At the Pantex Plant, “officials were concerned and surprised at the difficulty in finding as-built product definitions for the nuclear weapons,” the DoE IG report said.

At Los Alamos, the information system “allowed changes to classified nuclear weapons drawings without using an approved change notice. This practice could permit unauthorized changes to weapons drawings.” **Questioned about undocumented changes to a particular weapon drawing, “officials were unable to explain why changes were made, but told us that they ‘assumed’ the changes were needed.”**

“Over the decades of nuclear weapons development, neither NNSA nor its sites treated the maintenance of original nuclear weapons… information as a priority,” wrote DoE Inspector General Gregory Friedman.

“Not having complete and accurate [weapon production] information can have significant effects on surveillance and safety, and can lead to time-consuming and expensive recovery efforts.” See National Nuclear Security Administration Nuclear Weapons Systems Configuration Management, Audit Report DOE/IG-0902, March 26, 2014.

“NNSA is on a trajectory towards crisis,” said Norman Augustine, the venerable engineer and aerospace executive who serves as co-chair of the Congressional Advisory Panel on the Governance of the Nuclear Security Enterprise.

“The ‘NNSA experiment’ involving creation of a semi-autonomous organization [within the Department of Energy] has failed,” he said.

NNSA “has lost credibility and the trust of the national leadership and customers in DOD that it can deliver needed weapons and critical nuclear facilities on schedule and on budget,” Mr. Augustine said. He spoke at a March 26 briefing for the House Armed Services Committee.

The problems are not entirely attributable to NNSA itself, he said, but are due in part to an eroding consensus concerning the role of nuclear weapons in national security policy.

“At the root of the challenges are complacency and the loss of focus on the nuclear mission by the Nation and its leadership following the end of the Cold War,” Mr. Augustine said.

He cited “the absence of a widely accepted understanding of, and appreciation for, the role of nuclear weapons and nuclear technology in the 21st century, with the resultant well-documented and atrophied conditions of plans for our strategic deterrent’s future– in DOD as well as in DOE.”

# New Drones to Assist with Nuclear Hazards

Source: http://i-hls.com/2014/04/new-drones-assist-nuclear-hazards/

Hazardous nuclear events have the potential to cause huge levels of widespread damage to individuals and the environment. Getting close enough to these incidents to accurately assess the problem can be extremely dangerous.

Following the incident at the Fukushima power plant in Japan in 2011, for example, helicopter pilots assessing the site were exposed to significant amounts of radiation. **An AARM system integrates an unmanned aerial vehicle (UAV) with a lightweight gamma spectrometer and other positional sensors. It is lightweight and low cost, and able to capture high-resolution images.**

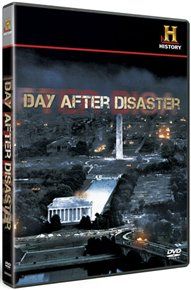
The AARM system could significantly improve the safety and effectiveness of hazard response operations, including rapid response monitoring of nuclear events. The system also supports routine monitoring at nuclear sites and naturally occurring radioactive materials at mining operations and oil and gas facilities.

According to HLS News Wire field demonstrations of the **prototype have already been performed at a uranium mining site in Banat, southwest Romania, and validated against traditional surveying methods,** attracting strong support from all areas of the U.K. nuclear industry.

# The 'Day After Disaster' – Revisited

**By Craig DeAtley**

Source:http://www.domesticpreparedness.com/Commentary/Viewpoint/The\_%60Day\_After\_Disaster%60\_-\_Revisited/

In 2009, the History Channel ran a movie called the “Day After Disaster,” which was about the detonation of a suitcase nuclear device in the nation’s capital. Over the course of nearly 90 minutes, various experts provided commentary on what the consequences might be for this type of terror attack, not just for the District of Columbia and the national capital region but also for the nation as a whole. Among the implications mentioned, hospitals and other healthcare facilities would face tremendous strain.

**Magnitude of the Incident**

If an event like this were to actually occur, the consequences would be unlike any before in the United States. Some sobering details in the movie highlighted the challenges that the remaining part of any city’s healthcare infrastructure, the adjoining region, and the national response system would face:

* **Five thousand or more persons in the 0.6-mile epicenter (Zone 1) would be “vaporized,” including first responders** whose assignments place them near the nuclear device at the time of detonation. The blast also would destroy buildings and other tangible items within this zone.
* **Ten thousand more people would die from the “flash of light” that would occur seconds after the initial explosion; and 15,000 additional people would be seriously injured from blast-wind debris and scalding heat** – including some with temporary and permanent “flash blindness.”
* The subsequent mushroom cloud that would occur a short time later and create a **fallout zone of approximately 20 miles would kill and injure thousands more.**
* **The resulting electromagnetic pulse would sever power to electronic equipment, including but not limited to**: airplanes in the sky; vehicles on the ground; and biomedical equipment such as intravenous pumps, ventilators, and electrocardiogram monitors.

**Planning & Exercising**

As with all other types of disasters, preplanning and training for this type of incident would be critical for doing the “greatest good for the greatest number of people.” For decades, government planning has occurred at various levels and has been exercised in classrooms and simulation laboratories, but often in secret without involving all members who may be directly affected – for example, the healthcare community. **Few communities have conducted well-integrated and realistic functional exercises to rehearse their response to a situation that would last longer and be more devastating than most incidents they are likely to confront.**

The healthcare system in the nation’s capital is now addressing this issue by having a multidisciplinary task force write a response plan template to assist all healthcare facilities in designing their own plans. Later in 2014, the District of Columbia’s Emergency Healthcare Coalition will present a two-day seminar to establish a clearer understanding of all the issues the coalition members will face, and realistically lay out how local, regional, and federal assets will come together in an effective response.

**Healthcare Facility Struggles**

**Hospitals and other healthcare facilities within 0.6-1 mile of ground zero (Zone 2) would sustain moderate structural damage.** **Those facilities just beyond 1 mile (Zone 3) would sustain light damage.** All of these facilities would confront conflicting priorities, including the need to treat their own injured staff and patients as well as incident survivors who eventually make their way to these hospitals. First responders – police, fire, and emergency medical services – likely would not respond to assist these survivors until hours or days later, when radiation levels have begun to subside and the environment is safe enough for the responders to conduct their lifesaving efforts.

As the hours and days move forward, hundreds of thousands of survivors would seek medical care, which would put unparalleled pressure on available healthcare facilities and clinicians to not only treat the large number of burned and traumatized patients but also manage acute radiation sickness, a condition not seen by many clinicians. Laboratories would face challenges in running the blood tests needed in order to manage these patients. In addition, the demand for ventilators, medications, and critical-care beds would necessitate the still-functioning facilities to employ their modified delivery of critical-care services plan in an effort to optimize the use of scarce resources. Mass-fatality plans also would be tested.

**Hospitals in Zones 2 and 3 also would find themselves trying to quickly assess the damages to structures and infrastructure.** Restoring lost water, power, and phone lines to a hospital is normally a utility company priority. In this situation, however, lengthy delays are likely and hospitals will have difficulty sustaining temporary workarounds. Staffing shortages caused by injury, death, or spontaneous resignation would exacerbate issues related to the absence of or damage to the needed infrastructure and quickly exhaust equipment and supplies. For all of these reasons and more, the affected healthcare community would require immediate and extensive support from their regional, state, and federal partners.

The detonation of a **suitcase nuclear device** makes for more than a scary movie. Its serious consequences mandate that healthcare systems – not just their government partners – take a realistic look at their readiness plans and training to determine if they are prepared for the day after a disaster.

***Craig DeAtley****, PA-C, is director of the Institute for Public Health Emergency Readiness at the Washington Hospital Center, the National Capital Region’s largest hospital; he also is the emergency manager for the National Rehabilitation Hospital, administrator for the District of Columbia Emergency Health Care Coalition, and co-executive director of the Center for HICS (Hospital Incident Command System) Education and Training. He previously served, for 28 years, as an associate professor of emergency medicine at The George Washington University, and now works as an emergency department physician assistant for Best Practices, a large physician group that staffs emergency departments in Northern Virginia. In addition, he has been both a volunteer paramedic with the Fairfax County (Va.) Fire and Rescue Department and a member of the department’s Urban Search and Rescue Team. He also has served, since 1991, as the assistant medical director for the Fairfax County Police Department.*

**Vulnerability of US Society to Geomagnetic Storms, Electromagnetic Pulse (EMP) & Non-Nuclear EMP Events**

**By John G. Kappenman and Phil Brooks**

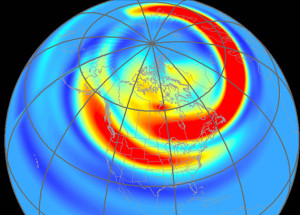
**Source:** **http://acdemocracy.org/acd-scientific-and-policy-briefing-on-emp-threats-10-april-2014/?utm\_ source=ACD-Scientific+and+Policy+Briefing+on+EMP+Threats&utm\_campaign=America%27s+ Commercial+Air+FleetNeeds+Protection+from+Shoulder-Fired+Missiles&utm\_medium=email**

Recent analysis carried out for the US FERC, the Congressional EMP Commission, FEMA (under auspices of US Presidential Executive Order 13407) and the US National Academy of Sciences has determined severe geomagnetic storms (i.e., space weather caused by solar activity) and EMP events (from a high altitude nuclear device detonation) have the potential to cause crippling and long-duration damage to the North American electric power grid.

Unlike the more familiar natural hazards or terror threats, both geomagnetic storms and EMP can have a large geographic footprint which can readily encompass major portions of the US electric power grid.  This wide spread and simultaneous disruption can cause correlated multi-point failures across the electric power grid resulting in not only the possibility of a large scale blackout of the electric grid, but also the risk of permanent damage to key apparatus constituting the backbone of the electric grid infrastructure.   The wide-spread permanent damage can cause an extremely slow pace of restoration from such a large blackout, causing multiplying effects that could hold our society at risk of catastrophic consequences, and recovery that could take years.

**Electric energy supply is the largest segment of energy usage in the US economy accounting for nearly 40% of all energy consumed.**  In contrast petroleum accounts for only 22% of current US energy consumption – which considerable US geo-political capital is expended to secure.  In addition, the operation of many other infrastructures is dependent on reliable and continuous supply of electricity to maintain their operational continuity.  Because of the underlying importance of this service, the electric power grid is a national critical infrastructure.  The loss of electric power can cascade rapidly into loss of all other vital infrastructures that supply potable water, perishable foods, perishable medications, transportation vital to maintaining a functioning society and as a result can place millions of lives at risk.

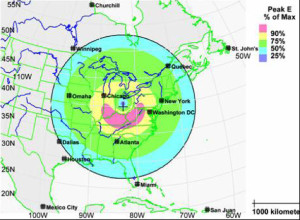
**Present day electrical grids have not been exposed to such large events, nor has their design ever been modified to withstand these threats.**  As recent detailed examinations have been undertaken concerning the interaction of these threat environments with power grids, the realization has developed that these infrastructures are becoming more vulnerable to disruption from these impulsive disturbance environments for a wide variety of reasons.

Geographic footprint of the 13 March 1989 Geomagnetic Storm.  A severe Storm is planetary in scope.  Image shows intensity of geomagnetic field disturbances in North America at 22:00 GMT.  Analyses of large historic storms indicate intensities of those storms posed a risk 3 to 10 times more severe than even this large storm, which disrupted power grids across North America.  Present day electrical power grids have not been exposed to such large events. Recent analysis indicates wide-spread, multi-year power outages are probable from damage due to these storms – a disintegrating force for our modern electricity-dependent society.

It is noteworthy that naturally occurring geomagnetic storms affect the power grid in a fashion similar to the late-time (E3) portion of an HEMP attack.  (A nuclear explosion produces electromagnetic effects of very short E1, intermediate E2 & longer E3 durations ranging from 5 nano-seconds to several hundred seconds.)  Of course, missile defense systems will not affect a geomagnetic storm – since it originates with the Sun.  **Hardening the electrical power grid is the only effective strategy to cope with this ongoing, unmitigated exposure.  Fortunately, this also provides effective protection against the E3 HEMP – a ‘two for one’ solution.**

Footprint of early-time (E1) HEMP overhead Midwest. This event would expose 83% of US major electrical substations. (Source – EMP Commission Report)

EMP risk comes from a variety of possible scenarios involving detonation of a nuclear weapon at high altitude (above 30 km).  **This may result from an intentional attack by a rogue nation or a terrorist group.**

Another valid scenario includes attack by a high power non-nuclear electromagnetic (EM) weapon – which affects a limited area unless deployed in a coordinated way.  An EM weapon produces Intentional Electromagnetic Interference (IEMI) or non-nuclear EMP.  These attacks can physically damage electrical and electronic equipment, most notably industrial systems controlling essential infrastructure like potable water treatment and delivery, wastewater collection and treatment, oil and gas pipelines, electrical power transmission & large communication systems.  An EM weapon attack on infrastructure is considered nearly as likely as cyber attacks.

An EM weapon causes an effect similar to the early-time (E1) portion of an HEMP attack.  Missile defense systems cannot prevent this attack either.  The only prevention is hardening exposed elements of the grid. Again, a ‘two for one’ benefit accrues in hardening the grid against an EM weapon pulse because this also eliminates effects of an E1 HEMP.

The severity of the hazards of geomagnetic storms, EMP and non-nuclear EMP for present day electrical power infrastructure worldwide has grown as grids themselves have expanded by a factor of 10 over the last 50 years.  Power grid design codes to account for these threats have never been instituted. Meanwhile, grids have become much more sensitive because microelectronic control systems have supplanted previous electromechanical relays & vacuum tube components – which could withstand higher levels of electromagnetic radiation.

It is still possible to remedy our circumstance with inexpensive solutions & protocols to harden both the current grid & future additions to this critical infrastructure.

***John G. Kappenman*** *is Founder & Principal of Solar Analysis Consultants and is one of the leading researchers on this topic, has provided testimony to Congress on several occasions and was a principle investigator for Congressional Commissions, FEMA, FERC and the National Academy of Sciences.*

***Phil Brooks*** *is Founder & Principal of GeoWater International which seeks to fund programmatic deployment of a paradigm-shifting water source to relieve potable water shortages in the United States and the world.  He has produced & directed a GWI video “Water Unlimited” depicting this opportunity.  A former airline pilot, Mr. Brooks has authored legislation & testimony for Congress on matters from aviation safety to US political letters. His writings have been reprinted in over 130 countries.*

# Fukushima Earth

**By Dawn Stover**

Source: http://thebulletin.org/fukushima-earth7022

Sudden nuclear disasters of the kind that occurred at the Fukushima Daiichi Nuclear Power Station three years ago may not at first glance seem to have much in common with the slow-motion planetary destruction of global warming. The two phenomena, though, are alike—and not just because they are dangerous to humankind. They unfold in similar fashion, starting with a single event which then leads to and interacts with many others. **Both are also easy to foresee—but unprofitable to avert.**

**Here’s how the slowly unfolding disaster known as climate change is similar to a nuclear power plant meltdown:**

**Common-cause failure.** In nuclear engineering parlance, a common-cause failure occurs when one event triggers breakdowns in multiple systems. At Fukushima Daiichi, for example, a huge earthquake and tsunami not only knocked out power from the grid but also destroyed nearby roads and swamped the plant’s emergency diesel generators, making it impossible to operate pumps that circulate cooling water to the reactors. The probability that any individual system—such as a single diesel generator—would fail at any given time was extremely small, which gave the false impression that there was an even more remote chance that multiple backup systems would fail simultaneously.

Climate change is likewise a matter of risk management and probabilities, as the latest report from the Intergovernmental Panel on Climate Change points out. The report urges decision makers to consider the full range of possible scenarios, “including low-probability outcomes with large consequences.”

In a changing climate, a common-cause failure is most likely to begin with an extreme weather event, such as a heat wave, flood, or prolonged drought that would destabilize critical food, water, and energy systems. While the probability of failure in any one system—an electricity blackout, say—is normally quite low, an event such as a severe heat wave would increase the likelihood of everything from agricultural losses to wildfires. Human “backups” for dealing with a heat wave—such as indoor air conditioning and outdoor lawn watering—will not operate properly if water reservoirs are too low and the temperature of nearby water bodies is too high to provide adequate cooling for electricity-generating power plants.

In the bigger picture, a January report from the Government Accountability Office warns that climate change will affect oil and gas platforms, refineries, pipelines, power lines, and a host of other critical energy infrastructure, and that these impacts “may also be amplified by a number of broad, systemic factors, including water scarcity, energy system interdependencies, increased electricity demand, and the compounding effects of multiple climate impacts.”

And the effects of climate change are not confined to our physical world—they also have a social impact. When factors such as water, agriculture, energy, and population collide, the planet’s carrying capacity is strained. Add to this the economic stratification of society into wealthy elites and poor commoners, and you have a recipe for societal collapse, according to an analysis of collapses over the past 5,000 years that will appear in the journal Ecological Economics. The elites hog natural resources and cut off their flow to the masses. Sound familiar? Just look at how American farmland, for example, once divided into many small family farms, is now being consolidated under the control of wealthy individuals and corporations.

**Complexity.** Like a nuclear power plant, the climate is an inherently complex system. As Charles Perrow explained in his book Normal Accidents: Living with High-Risk Technologies,  the complexity of tightly coupled, interactive systems, such as nuclear power plants, makes accidents inevitable.

The climate has far more complexity than a nuclear plant, making it difficult for humans to “manage” such a system without inviting trouble. Changes in clouds and ice, for example, have impacts on how much of the sun’s energy is radiated back to space. Air, land, and water are coupled systems with feedback loops. As the concentration of carbon dioxide in the atmosphere rises, the ocean becomes more acidified, changing the conditions for shellfish and other marine life.

Failures—at nuclear plants or in the world’s climate system—are not completely avoidable, but that’s not to say that nothing can be done to prevent or mitigate them. Short-sighted moves increase the odds of failure: for example, building a nuclear plant in a seismically active zone, storing a lot of spent fuel onsite in elevated pools, and allowing regulators to get too cozy with the industry they oversee. Similarly, while events such as hurricanes and droughts occur naturally, air pollution from human activities increases the likelihood of extreme weather. Inadequate preparation loads the dice even further—as we saw with the poorly constructed levees in New Orleans that failed after Hurricane Katrina, and the destruction of wetlands that once protected the city from storm surges.

Nuclear power plants can be made safer with careful attention to factors such as design, siting, personnel training, and regulatory oversight. The more focus on factors like these, the more likely the plant is to survive a disaster—and bounce back quickly afterward.

The recommendations that a task force of senior Nuclear Regulatory Commission staff made after Fukushima are equally applicable to climate change: They include mitigation strategies and infrastructure modifications to reduce risk; better instrumentation to provide reliable data about what’s happening; constant data reevaluation to understand potential effects and determine whether safety upgrades are needed; periodic re-analysis of the potential impacts of extreme events; examination of the regulatory framework to see whether it has sufficient protections and enforcement; and evaluation of strategies for containing damage when it does occur.

**Human error.** In all three of the world’s nuclear power plant meltdowns—Three Mile Island, Chernobyl, and Fukushima—human error played a significant role, and at Fukushima it was the primary cause. The Onagawa nuclear plant, located even closer to the earthquake’s epicenter, survived relatively unscathed, because its operators took a different approach to safety. But the owner of the Fukushima plant, the Tokyo Electric Power Company (Tepco), abetted by Japanese regulators and policy makers, ignored clear signs that the nuclear plant was at risk from seismic activity. Profitability trumped safety.

And so it goes with climate change. Only a few letters separate Tepco from Texaco. The biggest difference between the nuclear meltdowns at Fukushima and the melting down of the planet’s ice is that the former were a possibility rather than a certainty. With climate change, though, there is no doubt that continued business as usual will raise the planet’s temperature well beyond the danger level. And there can be no greater human error than to keep allowing humanity to destroy its own life support systems.

Oil and gas companies such as ExxonMobil, Shell, and Chevron—among the most profitable businesses in history—are well aware of the scientific consensus on climate change and have even begun to plan for an anticipated tax on carbon pollution. At the same time, however, they continue to make hefty contributions to Republican candidates who oppose such a price, and they work day and night to increase the pace of drilling, pumping, fracking, and refining.

ExxonMobil was lauded for publishing an unprecedented report to shareholders at the end of March, saying that “ExxonMobil takes the risk of climate change seriously” and addressing the potential financial impacts of carbon pricing. In the same breath, however, the company made the jaw-dropping claim that it is “on the forefront of technologies to lower greenhouse gas emissions.” In fact, ExxonMobil and its brethren are in the business of selling products that, if used as intended by the manufacturer, will raise emissions enough to kill us.

As the shareholder report states, ExxonMobil believes that it is “highly unlikely” that governments will restrict hydrocarbon production significantly enough to affect the company’s bottom line—or to put it another way, enough to stabilize the climate. **Shareholders, you can breathe a sigh of relief that profits will remain intact. Pay no attention to the climate tsunami sweeping toward shore. Never mind those warning signs left on the hillsides by earlier societies. There are generators in the basement in case anything goes wrong.**

***Dawn Stover*** *is a science writer based in the Pacific Northwest and is a contributing editor at the* Bulletin*. Her work has appeared in* Scientific American*,* Conservation*,* Popular Science*,* New Scientist*,* The New York Times*, and other publications. One of her articles is included in the* 2010 Best American Science and Nature Writing*, and another article was awarded a special citation by the Knight-Risser Prize for Western Environmental Journalism.*

# Kim's secret weapon: North Korea 'is capable of striking U.S. with a nuclear electromagnetic pulse attack'

Source: http://www.dailymail.co.uk/news/article-2601437/North-Korea-strike-U-S-nuclear-attack.html

**North Korea has the capability to deliver on its threats to carry out a nuclear electromagnetic pulse attack on the United States, it has been claimed.**

Dr Peter Vincent Pry, executive director of the Task Force on National and Homeland Security, has reportedly seen a long-suppressed government report that concludes **North Korea is capable of using an Unha-3 rocket to carry out an attack on the U.S..**

He says the U.S. would be particularly vulnerable to such an attack, as any rocket from North Korea is likely to travel over the South Pole and approach from the south - something American missile defences would apparently be powerless to stop.

Unha-3

Dr Pry made the claims in an interview with the World News Daily website, in which he was quoted as saying: 'The North Koreans are seeing what they can get away with... It shows that Pyongyang is planning something big against the U.S.'

Dr Pry's Task Force on National and Homeland Security advises U.S. Congress on matters of defence, and he was also formerly the head of the Congressionally-mandated EMP Commission, which looked into the threat of electromagnetic pulse attacks.

He told the website that he had seen a long-suppressed report prepared by the Department of Homeland Security for the Defense Department that apparently concludes that the best defence the U.S had against a North Korean attack would be to destroy the rocket on the launch pad.

This is due to the U.S. having 'no early warning radars or interceptors' to stop a missile from the south, and because the the country also lacks adequate defenses on its east coast, Dr Pry said.

An electromagnetic pulse attack involves a nuclear warhead being detonated hundreds of miles above the earth's surface, with the resulting burst of energy disrupting or destroying all electronic devices - including communications, navigation and sensor systems - in the affected area.

Such an attack on the U.S. would cripple the country's defence systems, not to mention cause chaos in any scenario where an electronic device is required - including road, sea and air transport, government and civilian communications and, of course, the throughout entire economic sector.

The leaked Department of Homeland Security report allegedly claims that North Korea's leader Kim Jong-un already successfully practiced an electromagnetic pulse attack on the U.S. in early 2013.

In spring of that year, tensions on the Korean Peninsula dramatically increased, thanks to North Korea's repeat threats of war - including releasing videos depicting a nuclear attack on Washington.

Dr Pry said the DHS report was commissioned as a result of these threats.

He also said that in December 2012 a North Korean satellite was tracked above central and eastern U.S., and could have caused nationwide destruction had it been fitted with a nuclear warhead.

Dr Pry's claims come months of insistence from the Obama administration that North Korea still did not have the capability to attack the U.S. or its allies with nuclear weapons.

The Department of Homeland Security has not yet responded to Dr Pry's allegations.

# Nagasaki survivors express support for UAE’s efforts against nuclear weapons

Source: http://www.thenational.ae/uae/nagasaki-survivors-express-support-for-uaes-efforts-against-nuclear-weapons

April 14 – Some of the last survivors of the atomic bomb blast expressed their support for countries such as the UAE that advocate the eradication of nuclear weapons.

Residents of Megumi no Oka, a nursing home for atomic bomb survivors in the city’s mountains, said they hoped countries like the Emirates would transmit their message to the rest of the world.

“I support what countries like Japan and the others that are part of the Non-Proliferation and Disarmament Initiative are doing in terms of trying to get rid of nuclear weapons,” said Misano Hamada, 98, who was living next to a shipyard just 5.8 kilometres from the bomb’s hypocentre on August 9, 1945. “I will never forget what happened, it’s not possible.”

Last Saturday, 12 countries – the UAE, Canada, Japan, Australia, Turkey, Germany, Poland, Mexico, Chile, Nigeria, the Philippines and the Netherlands – took part in the initiative which aims to create a nuclear weapon-free world. But countries like the US, China, India and Pakistan still possess nuclear arms - a move that greatly upsets the Nagasaki survivors.

“We feel it’s vital to pass on and send out messages of the preciousness of human lives and call for peace and abolition of nuclear weapons,” said Akasako Yumiko, director of the facility, which was founded by a Catholic nun who was 1.3km from the hypocentre at the time of the explosion. “Since the day of the bomb, many people here have not forgotten about their lost family members.”

Ms Hamada, who relatives all died in the bombing, said countries like the UAE could help make the world a safer place.

“I really want to see nuclear weapons being erased from the face of this planet and I hope they will,” she said. “We went through a lot of hardships and difficulties but I think I can have some hope, that’s why every morning and evening I pray for the world to become a better place.”

Masako Omagari, 89, was 3.2km from the hypocentre. She said she knew of the non-proliferation efforts of countries like the UAE through newspapers.

“I fully support them and I really ask them to continue their support so that something like this never happens again.”

She said he hoped such countries would be able to get the message across to as many people as possible around the world.

“I work as hard as I can to speak about my testimony,” said the woman, who was 21 and working as a clerk in an electric wowrkshop at the time. “I survived because I managed to escape to an air raid shelter as soon as I saw the flash of light and felt the blast. I never thought anything like this would ever happen to Nagasaki.”

Although she remained in the shelter for two months, she was exposed to radiation and witnessed the death of many.

“I had hard feelings against Americans at the time but now my feelings have softened,” she said. “But I believe the current generation will never be able to understand our experience.”

Ms Hamada, who witnessed atrocities at a very young age, said she tried her best to continue living a normal life and prayed for world peace.

“Primary school children, whose ages were similar to ours when the bomb dropped, visit us,” she said. “It’s important for them to understand the dangers of nuclear weapons.”

The nursing home, which houses 350 atomic bomb survivors – the eldest turns 105 next week – opened in 1970 to cater to those who required special care.

They constitute the last generation of survivors and are adamant about telling their tale to younger generations through plays.

“The plays also give them a bit of physical exercise,” said Ms Yumiko. “They also allow them to convey their feelings as they were onsite.”

# The 'Dirty' Details About Explosive Devices

**By Courtney Gavitt**

Source:http://www.domesticpreparedness.com/Commentary/Viewpoint/The\_%60Dirty%60\_Details\_About\_Explosive\_Devices/

*One year ago today, 15 April 2013, I was among the many who were stopped by race marshals at mile 25.5 of the Boston Marathon course. The frustration, confusion, and even anger of the growing crowd of runners, halted just moments from Boylston Street, was evident. Having only run a few miles of the race in support of a friend, I was not exhausted nor fueled by adrenaline and, thus, quickly realized the potential gravity of the situation unfolding at the finish line. My hobby of running had suddenly collided with my profession of chemical, biological, radiological, nuclear, and high-yield explosive (CBRNE) preparedness and response.*

As dozens of emergency responders sped through neighborhoods lined with spectators, it was clear that this was not an ordinary medical emergency or traffic incident. Mutterings of “an explosion” began as that worst-case scenario unfolded. Text messages with friends waiting near the finish line confirmed that the explosions were not fireworks, nor planned events gone awry. In the absence of any information or instructions from race officials, these “facts” heightened suspicion that an improvised explosive device (IED) had been detonated near the finish line and there was a potential for additional targets and explosions. Despite the danger, many runners waited less than half a mile from the deadly blasts until law enforcement officials confirmed that the race was over and requested that all runners clear the streets.

Rumors and misinformed reports soon surfaced – including news broadcasts of additional bombs and explosions throughout the city – that continued for days after the event. Of particular concern were reports that erroneously referenced the IEDs as “dirty bombs,” which most commonly describe certain radiological dispersal devices (RDD) and denote a radioactive property that technically and theoretically is more damaging than IEDs. An article published in May 2013, by *Bulletin of the Atomic Scientists* examined how the scenario in Boston would have been significantly different if the IEDs had been dirty bombs.

**Basic Concepts of Complex Devices**

For appropriate emergency response efforts, it is imperative that the media distinguish an IED from a dirty bomb attack and accurately convey that information. Promoting awareness of this topic to media outlets and the public, though, requires that law enforcement officers, emergency response officials, and public health personnel also be familiar with both the common and unique technical characteristics of each type of threat.

In simple terms, RDDs include radioactive material and IEDs employ myriad conventional explosives with no radioactive material; various forms of IEDs are defined in the National Improvised Explosive Device Prevention and Preparedness Act of 2008. Each is notorious in its most popular form – the “explosive-driven dirty bomb” (an RDD) and the “roadside bomb” (an IED, described in detail by *The Washington Post*) – although equally dangerous versions of each device exist. The dispersion of shrapnel – including ball bearings and nails – from the pressure-cooker bombs used in the Boston attacks may have been the reason the IEDs were erroneously labeled as dirty bombs. However, the word “dirty” in this context exclusively identifies radioactive material.

Although all dirty bombs are RDDs, not every RDD is a dirty bomb. In fact, RDDs need not be explosive devices at all, but rather can be any device that disperses radioactive material. In addition to explosion, methods of dispersion include: (a) contamination of large areas using a crop duster; (b) introduction into a food or water supply; or, more rudimentarily, (c) placement of a device in a high-traffic area. Even without the use of a device, according to the Department of Homeland Security’s Protective Action Guides for RDD and IND Incidents, response efforts should treat any dissemination of radioactive material as an RDD.

**Radiological & Nuclear Factors to Consider**

Experts often suggest that, depending on the size and type of device, the greatest harm likely will occur from the blast of an explosive RDD, rather than by exposure to radiation. This comment, however, fails to factor in additional casualties when first responders are unable to immediately triage and treat exposed and contaminated victims.

In Boston, for example, video and photo evidence showed dozens of law enforcement, emergency responders, and even unharmed bystanders rushing to the aid of victims – three people killed and 260 injured by the explosions. Several accounts credit on-scene tourniquets and other immediate – formal and informal – medical attention for saving lives. Had radiation been present and detected, many of these immediate efforts would have been considerably complicated or ceased because of the threat to responders’ health and safety. Although it is likely that the explosion of an RDD poses the greatest risk of immediate injury and death, the presence of radiological material directly increases that risk by limiting lifesaving efforts.

An improvised nuclear device (INDs) is another type of device that is commonly associated and confused with RDDs because they both contain a radioactive element. Radioactivity, though, is perhaps the only technical commonality of the two weapons; the radioactive materials, properties, processes, and impacts differ dramatically. In its “Code of Conduct on the Safety and Security of Radioactive Sources,” the International Atomic Energy Agency (IAEA) identifies **16 radionuclides commonly used in medical, industrial, and research capacities that could pose a threat for radiological dispersal.**

According to a report by the National Research Council**, four of these – cobalt-60, cesium-137, iridium-192, and americium-241 – pose a significant risk** in the United States, where they are widely used in civilian applications. On the other hand, by definition, an IND contains special nuclear, or “fissile,” material – plutonium, uranium-233, or uranium enriched in the isotopes U-233 or U-235 – that do not occur naturally in the environment and are subject to extensive safeguards, making them difficult to acquire and traffic illicitly. For this reason, the threat of an IND attack by a nonstate actor may not be as plausible as the threat of an RDD.

If an adversary state or terrorist group were able to create and detonate an IND, it would likely be far more destructive than an RDD scenario. Unlike an RDD, an IND produces a nuclear explosion, which is characterized by an intense flash of light, extreme heat, a blast wave, and prompt radiation. Such radiation would be acutely lethal for an extended distance, whereas that produced by an RDD would cause concern for chronic risks rather than immediate harm. If, due to poor design, construction, or lack of expertise, the IND fizzles – meaning the weapon does not achieve nuclear yield because fission does not occur – the results then would resemble those of an RDD explosion.

**Emergency Response in a Radiological Event**

Many resources exist to inform emergency planners and responders about radiological and nuclear incidents. In the United States, primary government-issued resources include:

* Environmental Protection Agency’s 1992 Protective Action Guides Manual for both nuclear and radiological incidents and the 2013 revised draft Protective Action Guides Manual;
* Department of Homeland Security, Federal Emergency Management Agency’s 2008 Planning Guidance for Protection and Recovery Following RDD and IND Incidents;
* The White House, National Security Staff and Office of Science and Technology Policy’s 2010 Planning Guidance for Response to a Nuclear Detonation; and
* The Centers for Disease Control and Prevention’s 2007 Population Monitoring in Radiation Emergencies: A Guide for State and Local Public Health Planners.

Although by no means inclusive of all available resources pertaining to emergency response to a radiological event, these resources provide valuable information to aid response efforts for an RDD or IND attack. A coordinated response, with all stakeholders being aware of the differences between IEDs, RDDs, and INDs, would help reduce the risks and consequences to life and property following any radiological, nuclear, and/or explosive incident.

***Courtney Gavitt****, MS, is an analyst at Gryphon Scientific where she focuses on chemical, biological, radiological, nuclear, and high-yield explosive (CBRNE) consequence management in support of the Federal Emergency Management Agency. As a Nonproliferation Graduate Fellow at the Department of Energy (DOE), National Nuclear Security Administration (NNSA), she contributed to U.S. interagency export control and interdiction efforts designed to curb proliferation of CBRNE weapons and dual-use materials. She served as part of the U.S. delegation to the Proliferation Security Initiative and supported DOE’s Australia Group representative. Before working at NNSA, she was a contractor at the U.S. Department of Homeland Security Customs & Border Protection. She holds an MS in biodefense from George Mason University.*

# Floating nuclear plants could ride out tsunamis

### Source: http://newsoffice.mit.edu/2014/floating-nuclear-plants-could-ride-out-tsunamis-0416

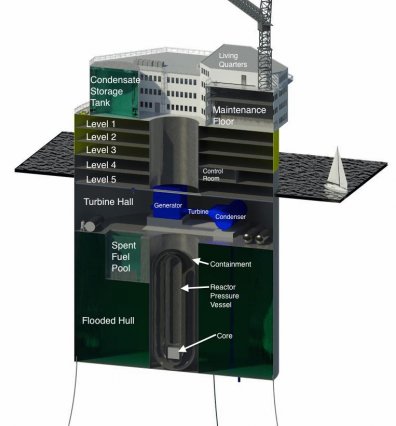
When an earthquake and tsunami struck the Fukushima Daiichi nuclear plant complex in 2011, neither the quake nor the inundation caused the ensuing contamination. Rather, it was the aftereffects — specifically, the lack of cooling for the reactor cores, due to a shutdown of all power at the station — that caused most of the harm.

**A new design for nuclear plants built on floating platforms, modeled after those used for offshore oil drilling, could help avoid such consequences in the future.** Such floating plants would be designed to be automatically cooled by the surrounding seawater in a worst-case scenario, which would indefinitely prevent any melting of fuel rods, or escape of radioactive material.

The concept is being presented this week at the Small Modular Reactors Symposium, hosted by the American Society of Mechanical Engineers, by MIT professors Jacopo Buongiorno, Michael Golay, and Neil Todreas, along with others from MIT, the University of Wisconsin, and Chicago Bridge and Iron, a major nuclear plant and offshore platform construction company.

Such plants, Buongiorno explains, could be built in a shipyard, then towed to their destinations five to seven miles offshore, where they would be moored to the seafloor and connected to land by an underwater electric transmission line. The concept takes advantage of two mature technologies: light-water nuclear reactors and offshore oil and gas drilling platforms. Using established designs minimizes technological risks, says Buongiorno, an associate professor of nuclear science and engineering (NSE) at MIT.

Although the concept of a floating nuclear plant is not unique — **Russia is in the process of building one now, on a barge moored at the shore** — none have been located far enough offshore to be able to ride out a tsunami, Buongiorno says. For this new design, he says, “the biggest selling point is the enhanced safety.”

A floating platform several miles offshore, moored in about 100 meters of water, would be unaffected by the motions of a tsunami; earthquakes would have no direct effect at all. Meanwhile, the biggest issue that faces most nuclear plants under emergency conditions — overheating and potential meltdown, as happened at Fukushima, Chernobyl, and Three Mile Island — would be virtually impossible at sea, Buongiorno says: “It’s very close to the ocean, which is essentially an infinite heat sink, so it’s possible to do cooling passively, with no intervention. The reactor containment itself is essentially underwater.”

Buongiorno lists several other advantages. For one thing, it is increasingly difficult and expensive to find suitable sites for new nuclear plants: They usually need to be next to an ocean, lake, or river to provide cooling water, but shorefront properties are highly desirable. By contrast, sites offshore, but out of sight of land, could be located adjacent to the population centers they would serve. **“The ocean is inexpensive real estate,”** Buongiorno says.

In addition, at the end of a plant’s lifetime, “decommissioning” could be accomplished by simply towing it away to a central facility, as is done now for the Navy’s carrier and submarine reactors. That would rapidly restore the site to pristine conditions.

This design could also help to address practical construction issues that have tended to make new nuclear plants uneconomical: Shipyard construction allows for better standardization, and the all-steel design eliminates the use of concrete, which Buongiorno says is often responsible for construction delays and cost overruns.

**There are no particular limits to the size of such plants,** he says: They could be anywhere from small, 50-megawatt plants to 1,000-megawatt plants matching today’s largest facilities. “It’s a flexible concept,” Buongiorno says.

Most operations would be similar to those of onshore plants, and the plant would be designed to meet all regulatory security requirements for terrestrial plants. “Project work has confirmed the feasibility of achieving this goal, including satisfaction of the extra concern of protection against underwater attack,” says Todreas, the KEPCO Professor of Nuclear Science and Engineering and Mechanical Engineering.

Buongiorno sees a market for such plants in Asia, which has a combination of high tsunami risks and a rapidly growing need for new power sources. “It would make a lot of sense for Japan,” he says, as well as places such as Indonesia, Chile, and Africa.

This is a “very attractive and promising proposal,” says Toru Obara, a professor at the Research Laboratory for Nuclear Reactors at the Tokyo Institute of Technology who was not involved in this research. “I think this is technically very feasible. ... Of course, further study is needed to realize the concept, but the authors have the answers to each question and the answers are realistic.”

|  |
| --- |
| EDITOR’S COMMENT: As you can easily understand these brilliant colleagues do not give a s… about safety but only about how to build new reactors in the “***inexpensive ocean real estate***”! Until now I have not heard or read about plans to improve the ridiculously low wave barriers seen in many nuclear plants. And they are discussing about sea platforms able to withstand natural phenomena such as tsunamis… |

# Australia hopes to lure Emirati students to its institutions while selling uranium to the UAE

Source: http://www.thenational.ae/uae/australia-hopes-to-lure-emirati-students-to-its-institutions-while-selling-uranium-to-the-uae

April 17 – During a visit to the UAE this week by Andrew Robb, Australia’s trade and investment minister, an agreement was signed with Sheikh Hamdan bin Mubarak, the Minister for Higher Education. The countries will collaborate on vocational education, training and research cooperation in higher education.

“It is an all-encompassing memorandum of understanding (MoU) that will provide for increased government-to-government consultation,” said Pablo Kang, Australia’s ambassador to the UAE.

“It also includes the exchange of students, academics and researchers, and sharing of information on issues such as teaching, curriculum materials, standards and accreditation systems.”

Other areas will focus on policy developments, benchmarking of occupational standards and the development of credit transfer arrangements between educational institutions in both countries.

“It is now operational as it does not require ratification,” he said. “We hope it will be the catalyst to increasing numbers of Emirati students travelling to Australia to study, or to study at Australian institutions in the UAE.”

Mr Kang said he hoped more Australian schools would be set up in Dubai and Abu Dhabi.

“There are no student numbers specified in the MoU but the sky is the limit as far as I am concerned.”

Mr Robb said Arabian Gulf countries faced challenges in providing education and skills development for their growing and youthful populations.

Mr Robb said the UAE was investing in infrastructure and restructuring its economy, creating opportunities in sectors where Australia had a proven track record.

He also met senior ministers to advocate for a resumption of negotiations for a free trade agreement with the GCC.

“I [used] my visit to set out the Australian government’s trade and investment agenda, to emphasise that Australia is open for business and that we are committed to deepening our economic engagement with the region,” he said.

Australia will also begin to export uranium to the UAE for its nuclear power plants.

**The Nuclear Cooperation Agreement was signed in July 2012 but was ratified and came into force only on Monday. It could lead to the export to the UAE of up to 800 tonnes of uranium a year by the end of the decade.**

“The agreement should now pave the way for separate commercial agreements between potential Australian uranium suppliers and the Emirates Nuclear Energy Corporation,” said Mr Kang. “The [first exports] are subject to the timeline for the construction of the UAE’s nuclear power plants, but I understand the first of these plants is scheduled for completion in 2017.”

Under the agreement, Australia will supply uranium for use in the UAE’s developing civil nuclear power programme and cooperate in nuclear-related activities, such as safeguards, security, safety and science.

“The agreement has been secured because Australia is a reliable supplier of uranium and the UAE is a responsible user of nuclear energy for civilian purposes,” said Mr Robb, who met Sheikh Abdullah bin Zayed, the Foreign Minister, this week in Abu Dhabi.

“This will open up a new long-term market for Australian uranium producers.”

He said the agreement reinforced Australia’s close and expanding relationship with the UAE, based on mutual political, strategic and economic interests.

**Australia exported almost 8,400 tonnes of uranium in 2012 and last year, worth about AUS$823 million (Dh2.82 billion).** According to the Australian Trade Ministry, the UAE would hope to import about 800 tonnes a year from 2020.

“It is important for the UAE’s civilian nuclear energy programme to have a safe and reliable source of uranium,” Mr Kang said. “Australia holds the world’s largest known uranium reserves – about 40 percent of the world’s total reserves – and, from Australia’s perspective, the agreement opens up a potential new source of exports from Australia to the UAE and hence a considerable diversification in our current terms of trade.”

Sheikh Abdullah said the ratification of the agreement would offer more opportunities for collaboration between the Government and private sectors of both countries. He said this falls in line with the UAE’s policy of developing its peaceful nuclear energy programme in collaboration with other countries that shared the same commitment.

Hamad Alkaabi, the UAE’s permanent representative to the International Atomic Energy Agency, said the agreement constituted a governmental framework for cooperation in nuclear activities between both countries.

“It allows for the transfer of nuclear material from Australian sources to the UAE’s nuclear sector, once the administrative and commercial arrangements are put into place,” he said.

## New detection technology to help combat nuclear trafficking

Source: http://www.homelandsecuritynewswire.com/dr20140418-new-detection-technology-to-help-combat-nuclear-trafficking

According to the International Atomic Energy Agency (IAEA), the greatest danger to nuclear security comes from terrorists acquiring sufficient quantities of plutonium or highly enriched uranium (HEU) to construct a crude nuclear explosive device. **The IAEA also notes that most cases of illicit nuclear trafficking have involved gram-level quantities, which can be challenging to detect with most inspection methods.**

An AIP release reports that according to a new study appearing this week in the Journal of Applied Physics, coupling commercially available spectral X-ray detectors with a specialized algorithm can improve the detection of uranium and plutonium in small, layered objects such as baggage. This approach enhances the detection powers of X-ray imaging and may provide a new tool to impede nuclear trafficking.

The study was conducted by a joint research team from the University of Texas at Austin (UT) and the Department of Energy’s Pacific Northwest National Laboratory (PNNL).

“We first had to develop a computational model for how X-rays move through materials and how they are detected so that we could predict what an image will look like once the radiation passed through an object,” said UT’s Mark Deinert, one of the authors on the paper. “With that in hand, we applied an ‘inverse algorithm,’ varying the composition of the object until the predicted image matched the measured one. We also gave our algorithm additional details about density and other factors — a process called ‘regularization’ — to adaptively enhance its ability to discriminate materials.”

The new system, Deinert said, expands upon techniques originally developed for medical applications such as discerning between bone and iodine contrast agent in an X-ray image. “We wanted to show that spectrally sensitive detectors can be used to discriminate plutonium and other high-atomic-number elements from multiple layers of other materials using a single-view radiograph,” said Andrew Gilbert, the lead author on the paper and a doctoral student of Deinert’s working at PNNL. **“In simulated radiographs, we were able to detect the presence of plutonium with a mass resolution per unit area of at least 0.07 gram/centimeter squared; in other words, we can locate a sample of plutonium with a thickness of only 0.036 millimeters.”**

Now that the inverse algorithm method has been shown to help X-rays detect nuclear materials in luggage and other small objects, Deinert said that his team will next expand the concept to improve detection on a larger scale. “We plan to apply the algorithm to high-energy X-ray systems that could be used for verification of arms-reduction treaties,” he said.

*— Read more in A.J. Gilbert et al, “Non-invasive material discrimination using spectral X-ray radiography,”* Journal of Applied Physics *115, 154901 (15 April 2014)*

►**Full paper available at:** http://scitation.aip.org/content/aip/journal/jap/115/15/10.1063/1.4870043

# Did Israel steal bomb-grade uranium from the United States?

**By Victor Gilinsky and Roger J. Mattson**

Source: http://thebulletin.org/did-israel-steal-bomb-grade-uranium-united-states7056

Last month the Interagency Security Classification Appeals Panel (ISCAP), the nation’s highest classification authority, released a number of top-level government memoranda that shed additional light on the so-called NUMEC affair, "the story that won't go away—the possibility that in the 1960s, Israel stole bomb-grade uranium from a US nuclear fuel-processing plant.”

The evidence available for our 2010 Bulletin article persuaded us that Israel did steal uranium from the Apollo, Pennsylvania, plant of the Nuclear Materials and Equipment Corporation (NUMEC). We urged the US government to declassify CIA and FBI documents to settle the matter. In releasing the current batch—the release being largely due to the persistent appeals of researcher Grant Smith—the government has been careful to excise from all the released documents the CIA’s reasons for fingering Israel. Despite this, the documents are significantly revealing. For one thing, the excisions themselves are a backhanded admission of the persuasiveness of the CIA’s evidence. (Why these excisions are legally justified is not apparent—after nearly 50 years, the “sources and methods” issues have long ago dissipated.)

While we still don’t know exactly what the CIA told high government officials, we do know from the released memoranda that top officials thought the CIA’s case was a strong one. Also, as described in our earlier article, one of us was present at the CIA’s February 1976 briefing of a small group at the Nuclear Regulatory Commission (NRC). At that session Carl Duckett, then-CIA deputy director for science and technology, told the NRC group the CIA believed the missing highly enriched uranium ended up in Israel.

The newly released documents also expose government efforts, notably during the Carter administration, to keep the NUMEC story under wraps, an ironic twist in view of Jimmy Carter’s identification with opposition to nuclear proliferation.

**The context of NUMEC.** A bit of background is in order here. **After a 1965 inventory, NUMEC was found to be missing about 100 kilograms of bomb-grade uranium, even after accounting for all processing losses.** The close personal and commercial ties to Israel of the plant owners and operators raised suspicions that remained unresolved. The affair of the missing bomb-grade uranium was revived in 1976. The newly formed NRC was in the process of writing licensing regulations for commercial fuel firms—of which NUMEC was one—and had heard rumors of possible theft in the 1960s from NUMEC's Apollo facility.

The NRC asked for a CIA briefing. Duckett startled the NRC group with CIA’s conclusion that the missing uranium was in Israeli bombs. The NRC chairman informed the White House, and President Ford took an interest in the case. Ford’s Attorney General, Edward Levi, discovered that the Atomic Energy Commission (AEC), the NRC predecessor nuclear licensing agency, had previously convinced the FBI not to open a criminal investigation into the material’s disappearance. The AEC was concerned that the public revelation of the NUMEC case would draw attention to its lack of control over nuclear bomb materials in the hands of private firms, and thus undermine the commission’s efforts to get nuclear power programs underway. In addition, then-FBI Director J. Edgar Hoover was not eager to get into a technical area with which his agents were unfamiliar. Levi gave the FBI its first instruction to investigate the material’s disappearance, a decade after the 1965 inventory that was the object of concern. In fact, although they attracted little attention, NUMEC inventories through 1968 showed even larger unexplained losses.

After the 1976 election, the Ford White House alerted the incoming Carter administration to the NUMEC affair. In December 1976, according to a July 1977 National Security Council memorandum, then-CIA Director George H.W. Bush briefed President-elect Carter on the case. Congress had been pressing for public disclosure of records of large unexplained losses of bomb-grade material (in government parlance, “material unaccounted for,”or MUF) from the government’s nuclear weapons complex. The White House feared the story was sure to hit the headlines if there were any suggestion of Israeli theft from the NUMEC facility. And any disclosures about Israel’s bomb program would of course have threatened the Carter administration’s Middle East policies.

Carter instructed his national security advisor, Zbigniew Brzezinski, to deal with the NUMEC matter in the context of the impending public release of MUF data. Brzezinski’s staffers John Marcum and Jessica Tuchman posed questions to the CIA about the NUMEC affair. Ted Shackley, then-CIA’s deputy director for covert operations, called Marcum on a secure line on July 28, 1977, to provide answers. Marcum’s entire two-page description of the call in his memorandum to Tuchman is blanked out in the version just released by ISCAP. As noted in our earlier article, other evidence suggests that the next day Shackley briefed senior officials of the Energy Research and Development Administration (ERDA), the principal successor agency to the AEC. He told them that **environmental samples taken by the CIA in Israel in 1968 contained highly enriched uranium, whose enrichment level was so high it pointed to the Portsmouth, Ohio, uranium enrichment plant as the source**. Portsmouth was where NUMEC obtained uranium stock for its naval fuel products. We don’t know whether this information is in the excised portion of Marcum’s memorandum. We do however now have Marcum’s unredacted conclusion: “The CIA case is persuasive, though not conclusive." Marcum preceded his conclusion with the pregnant observation, “At this point, despite the FBI clean bill of health, I do not think the president has plausible deniability.”

**The unusual Brzezinski interlude.** The matter passed up to Brzezinski, who submitted a memorandum to the president on August 2, 1977. (The president’s diary records a discussion on NUMEC the same day.) Brzezinski summarized for President Carter the views of ERDA, the FBI, and the CIA regarding Israeli involvement. His characterization of the CIA's views is excised in the version just released. His descriptions of the other agencies' views omit important evidence. For example, **the memorandum understates by about a factor of six the unexplained amount of missing uranium—more than 330 kilograms by 1968, or enough to make over a dozen Hiroshima-yield bombs**. He reported ERDA’s statements that there was "no evidence" of theft, adding that the agency had no basis for that conclusion. Nevertheless, when it came to his conclusion for the president, he used the same formulation (with our emphasis): “while a diversion might have occurred, there is no evidence—despite an intensive search for some—to prove that one did. For every piece of evidence that implies one conclusion, there is another piece that argues the opposite. One is pretty much left with making a personal judgment—based on instinct—as to whether the diversion did or did not occur.” Leaving aside the contradiction between saying there is no evidence of theft and then saying there is more or less equal evidence on each side of the case, there was in fact a great deal more evidence of Israeli involvement already available in ERDA, FBI, and CIA records that Brzezinski apparently did not take the trouble to look into.

Brzezinski took at face value the AEC's claim that it had investigated the NUMEC affair. As we showed in our 2010 article, however, the commission's inquiries into the NUMEC affair were mainly designed to exculpate NUMEC and the AEC itself from any charges of wrongdoing. In evaluating these past so-called investigations, Attorney General Levi wrote President Ford on April 22, 1976 that federal officials might have violated criminal statutes, including those that cover accessory after the fact and failure to report a felony.

Brzezinski also passed off the FBI’s findings as amounting to no more than confirmation that the president of NUMEC, Zalman Shapiro, had frequent contacts with Israeli officials, including a science attaché “thought to be an intelligence officer,” and received unexplained VIP treatment in Israel. In fact, Shapiro was by then known to have had contacts with Israel’s head of military intelligence and the head of its nuclear weapons program. He later acknowledged knowing Binyamin Blumberg, head of Israel’s “bureau of scientific liaison,” which engaged in high-risk intelligence capers. On one strange occasion in 1968, Shapiro hosted an Israeli intelligence foursome at the Apollo plant. One was the Mossad agent who headed the team that spirited former Nazi leader Adolf Eichmann out of Argentina and who later ran Jonathan Pollard’s spying on the United States for Israel. (Mossad is the Israeli agency that handles foreign intelligence collection and covert action.) Another was that agent’s deputy in the Eichmann kidnap, who went on to become head of Shin Bet, Israel's internal security service. A third was Mossad’s director of technical services. The last was Israel’s science attaché, who had held a senior position in Israel’s nuclear weapons program.

The FBI, Brzezinski told Carter, had just concluded its latest investigation and “was unable to uncover any evidence of theft, although the interviews included many current and former NUMEC employees.” In fact, the FBI investigation continued for two more years, and its interviews of NUMEC employees revealed many suspicious circumstances concerning NUMEC shipments to Israel.

The last part of the Brzezinski August 1977 memorandum to President Carter is the most revealing of the Carter administration’s intentions regarding the NUMEC affair: “We face tough sledding in the next few weeks (particularly in view of [Secretary of State Cyrus Vance's] Mid-East trip) in trying to keep attention focused on ERDA’s technical arguments and, if necessary, on the FBI investigations, and away from the CIA’s information."

**Time for real transparency.**It's fair to ask, in view of the other losses in the US nuclear weapons complex, why the CIA and others singled out NUMEC for grave suspicion as the source for Israeli bomb-grade uranium. In brief, the reasons are these: NUMEC's unexplained losses were a significantly larger proportion of its throughput of highly enriched uranium than was the case for other firms that dealt with nuclear materials. Sloppy accounting and lax security made the plant easy to rob without detection. NUMEC had commercial relationships with Israel’s defense and nuclear establishments and regularly made sizeable nuclear shipments to Israel, which at that time were not checked by the AEC. NUMEC’s owners and executives had extremely close ties to Israel, including to high Israeli intelligence and nuclear officials. Israel had strong motives to obtain the highly enriched uranium before it was producing enough plutonium for weapons. High-level Israeli intelligence operatives visited the NUMEC plant. Israeli intelligence organizations were used to running logistically complicated, risky operations to support nuclear weapons development, and it would have been very much out of character for them to pass up an opportunity like this. On top of all this, records show the CIA believed its 1968 environmental sample taken in Israel evidenced an enrichment level unique to Portsmouth.

Nearly 50 years have passed since the events in question. It is time to level with the public. At this point it is up to the president himself to decide whether to declassify completely the NUMEC documents, all of which are over 30 years old. He should do so. We know that is asking a lot given the president’s sensitivity about anything involving Israel, and especially anything relating to Israeli nuclear weapons. But none of his political concerns outweigh his responsibility to tell the US public the historical truth it deserves to know.

*A physicist,* ***Victor Gilinsky*** *is an independent consultant, and advised Nevada on matters related to the proposed nuclear waste repository at Yucca Mountain. His expertise spans a broad range of energy issues. From 1975 to 1984, he served on the Nuclear Regulatory Commission, having been nominated by President Gerald Ford and renominated by President Jimmy Carter. Earlier in his career he worked at Rand Corporation; he was also an assistant director for policy and program review at the Atomic Energy Commission.*

***Roger J. Mattson*** *is a mechanical engineer who consults on safety matters with NRC licensees and Energy Department contractors. From 1967 to 1974, he was on the Atomic Energy Commission technical staff. In 1976, he led an NRC task force that addressed the Apollo/NUMEC affair. He left government service in 1984.*

## The Science of Detecting and Defeating Radiological Threats

Source: http://www.bnl.gov/newsroom/news.php?a=24728

If you were at the Super Bowl in New Jersey in February, or at the concurrent “NFL Experience” in Manhattan, you may have spotted some elite Brookhaven Lab employees. Not cheering in the stands or even inside the stadium, these members of the Lab’s Radiological Assistance Program (RAP) team were working on Super Bowl Sunday and for several weeks beforehand to monitor the metropolitan area for potential radiological threats.

**The RAP team, one of the National Nuclear Security Administration’s (NNSA) radiological emergency response assets, is comprised of a few permanent staff, augmented by highly trained volunteers from many Lab disciplines. Together, they work to stay ahead of any such threats using a palette of detection tools that have become increasingly sophisticated and user-friendly, driven by the evolving mission of the program.**

“The whole profile of the team has changed,” said Kathleen McIntyre, who is the contractor operations manager for RAP Region 1, which covers the East Coast from Maine to Maryland and inland to the Pennsylvania-Ohio border.  “We used to investigate questionable material found in grandpa’s basement, but since 9/11 the focus has been on search-and-detect missions.”

Working with first responder partners like the Federal Bureau of Investigation, police and fire departments, hazmat units, Weapons of Mass Destruction Civil Support Teams (Air and Army National Guard), and others, the RAP team offers radiological assistance efforts upon the request of federal, state, tribal, and local governments and private groups and individuals for incidents involving radiological materials. In addition to prominent sporting events, the RAP team supports security efforts for high-profile events like the United Nations General Assembly, New Year’s Eve activities in one or multiple locations, the holiday tree lighting ceremony, the Democratic and Republican national conventions, and even Presidential inaugurations.

During a deployment, researchers and technicians with backgrounds in various aspects of radiological controls and analysis conduct field monitoring and environmental sampling, assessment, and documentation activities to help decision makers choose appropriate protective actions for the safety of both the public and first responders. Between deployments, the team examines issues of coordination between agencies, plans, and procedures, and trains and evaluates the proficiency of individuals using the equipment. Initially, all RAP team members are required to take a specialized course in Albuquerque, NM, and then attend training sessions at least quarterly. Team members are periodically evaluated through their participation in drills and exercises.  Occasionally a “No Notice Exercise” is conducted by NNSA that tests the team’s readiness to respond.

### Advances in equipment

Although some of the equipment now being used is commercially developed, other instruments are developed specifically for the use of DOE assets such as RAP teams, with the expertise of scientists and engineers from the DOE and NNSA complexes. Lab staff has participated in the development, testing, and functional evaluation of numerous pieces of equipment in this category. The evolution of this equipment conforms to the change in the program’s mission.

Historically the RAP mission was “consequence management” — events and situations along the lines of responding to a spill from a truck carrying medical radioisotopes, for example.  But as the profile of terrorism has been raised across the country and around the world, the need for a more preemptive approach in radiological screening was recognized, and RAP has been increasingly called upon to support law enforcement groups conducting directed or random screening for illicit movement of radiological materials.

“That screening tends to be correlated with the potential for radiological material to be used to threaten a large mass gathering or other high-profile event,” said Chuck Finfrock, principal engineer for RAP team science. “To assist us in doing what we call low-profile missions, we need to be able to blend into crowds and collect radiological data in the field. Some of the equipment that we originally had was extremely bulky, so scientists have been working on equipment that is easier and less cumbersome to use and allows us to do a quicker assessment of our environment.”

**One of the techniques now being applied to the search and crisis response missions is gamma ray spectroscopy (GRS), largely a laboratory technique used for more than 40 years to identify radiological material.** Like a fingerprint, a particular radiological material has a particular gamma ray spectrum that is unique to that radioisotope. As a result, this technique can be used to not only detect the radioactivity of a sample, but also to give information identifying that particular material.  The instruments can be very large and are delicate items that need very stable temperature control and a constant supply of liquid nitrogen to cool them.

As the RAP program moves to emergency response, more portable equipment allows the team to conduct a search operation with greater focus.  For example, a construction site may report a missing soil density gauge – a commercial product containing some radioactive material that’s used to measure the density of compacted soil.  With a spectroscopic system, the team knows in advance what isotope they’re seeking and can use GRS to search in a more specific way. Also, while the older GRS systems always required a human to take, calibrate, and analyze the data, computer software can now automate some analysis of that gamma ray spectral information.

“The instruments are also, in effect, becoming ‘smarter’ and better able to help first responder partners with limited knowledge collect the initial on-scene information. This improves the quality of the data collected, which in turn helps a team scientist to understand the event more quickly,” said McIntyre. “**Another important technological change that’s taking place is that instruments are being equipped with the ability to communicate by cell phone, satellite or Wi-Fi, allowing us to send data from the field back to a command center in near real time.** Operators in the field working in multiple locations can send data back to the command center to be analyzed by one specialist at the command center.”

Other new, more sophisticated algorithms can generate data products, such as maps, at different stages of an event, so technical information can be conveyed to decision makers at a glance.

### Training, teamwork critical

But McIntyre warns that as sophisticated and user friendly that this gear has become, “we cannot emphasize enough **how important it is to have an individual who has proficiency in the equipment that is being deployed in the field.** **Some of the first responders wear many hats, and while they do receive training, they don’t have the kind of in-depth knowledge and access to scientific expertise that members of the RAP team have.** There are still important issues related to the fact that we live in a sea of radiation from rocks and soil. Also, we live in a community where radiological materials are used in many medical applications. As an example, we often encounter people who have had a thallium stress test or other medical administration. That person will measure as radioactive for days or weeks.”

“Construction materials can also offer challenges,” she added.  “**On the streets of New York City, you’ll see great changes in the background radiation levels as you go from avenue to avenue and street to street.**  Our team has been trained to be cognizant of those changes and those contributing factors as well as being on high alert for something that might contribute additional information that might be of interest.”

The context surrounding a measurement needs to be evaluated by someone with some understanding of the **world’s background radiation footprint**.  The DOE community also has a capability called TRIAGE, where highly trained specialists from the NNSA nuclear weapons laboratories provide a scientific confirmation of the measurements made in the field.  Advances in equipment communication allow that information to be communicated to specialists who can analyze field measurements that may look ambiguous.

“The evolution of our capabilities is a combination of advancements in different areas,” Finfrock said “The advancements in detector engineering have caused them to become more field-usable. The advances in communications electronics and computers have enabled the detectors to more easily send data to the right people quickly.  Most detectors now have global positioning tagged in with the radiological data, so not only are we getting back radiological measurements but we also know very precisely where that measurement was taken. We can correlate multiple measurements in multiple locations to be able to anticipate situations because we have geospatial awareness as well as radiological awareness.”

As the radiological landscape continues to evolve, both in this country and abroad, the RAP team and others will continue to refine their search and detection techniques, and scientists at Brookhaven Lab and elsewhere will be working to stay ahead of the technology curve.

# http://r70.cooltext.com/rendered/cooltext1333426779.pngCar bomb explodes in Bahrain capital, F1 race unaffected

Source: http://www.reuters.com/article/2014/04/06/us-bahrain-blast-idUSBREA350HA20140406

**A home-made bomb exploded in a car in the center of the Bahraini capital Manama on Sunday, the interior ministry said, as the kingdom hosted a Formula One motor racing Grand Prix.**

Earlier, three witnesses had reported hearing a blast in the bustling Adliya district, where many foreigners live. The interior ministry confirmed the incident on its Twitter account, saying the car had burnt as a result of the explosion.

**There were no reports of casualties.** Police blocked off the road where the incident took place near a government security building.

Small bomb blasts occur sporadically in the **U.S.-allied kingdom, which has witnessed low-level political unrest since 2011, when protests mainly by the Shi'ite Muslim community erupted to demand democratic reforms in the Sunni-led government.**

But unrest in the run-up to the race, staged about 30 km (20 miles) south of Manama at the Sakhir desert circuit, was markedly lower than in the past two years, apparently due to a more effective security clampdown on Shi'ite villages.

The government sees the Bahrain Grand Prix as a way to raise Bahrain's international profile and attract tourists and foreign investment.

In 2011, when the unrest first broke out as part of the Arab Spring, the race had to be canceled.

Many Bahraini Shi'ites complain of discrimination, especially in employment and housing, a charge that the government denies.

Political reconciliation talks between the government and opposition have made little progress.

Earlier on Sunday, a small crowd of youths in the Shi'ite village of al-Eker, south of Manama, burned tires and threw stones at police who responded by firing tear gas, Reuters witnesses said. The youths quickly dispersed.

Bahraini activists reported similar sporadic unrest in other areas where dozens of protesters marched inside villages and others threw stones at police who seemed to effectively block off the main entrances to the villages. Reuters could not immediately verify these accounts.

On Friday, tens of thousands of mainly Shi'ite protesters had marched for democratic reforms and on Thursday, anti-government demonstrators throwing petrol bombs clashed with police who fired tear gas and birdshot following a funeral procession in al-Eker.

Meanwhile, police have increasingly come under attack in recent months from home-made bombs and dozens of Bahrainis have been sentenced to prison terms ranging up to life in prison for attacking police stations and attempting to kill policemen.

One of three blasts last month killed three policemen, including one from the UAE. Bahrain quelled the uprising in 2011 with help from forces from its Sunni Gulf Arab allies, Saudi Arabia and the United Arab Emirates.

**Greece – VBIED detonated in Athens downtown**

Source: Greek media

April 10 – At 05:55 a stolen Nisan Sunny packed with explosives (75kg TNT according to the person who called 45 min before the explosion) detonated downtown Athens causing extensive material damages in surrounding buildings (banks, shopping mall, offices). No injuries caused.



|  |
| --- |
| EDITOR’S COMMENT: Alleged 75kg of TNT but NO crater on the road? Amazing! |

# Terrorist attack at Nigerian bus station kills at least 71

Source: http://nypost.com/2014/04/14/terrorist-attack-at-nigerian-bus-station-kills-at-least-71/

**April 14 – A massive explosion ripped through a bus station during the morning rush hour in Nigeria’s capital, killing at least 71 people and wounding 124 in a bombing that marked the bloodiest terrorist attack ever in Abuja.**

President Goodluck Jonathan visited the scene and blamed Boko Haram, an Islamic extremist group which operates in the northeast of Nigeria and which has been threatening to attack Nigeria’s capital. One official said he believed the bomb was buried in the earth, while the emergency management agency said the explosives apparently were hidden in a vehicle.

The blast destroyed 16 luxury buses and 24 minibuses and cars, said police spokesman Frank Mba, who gave the death toll.

Survivors screamed in anguish and the stench of burning fuel and flesh hung over the site, where billows of black smoke rose as firefighters worked to put out the fires. Reporters saw rescue workers and police gathering body parts as ambulances rushed the wounded to hospitals. State television has broadcast calls for blood donations.

Security personnel battled to cordon off the area as a bomb detonation team was combing it for secondary explosives, a common occurrence here. Thousands of bystanders gathered, ignoring warnings to stay away. While violence has torn the northeast, where Boko Haram has killed thousands, the capital in the middle of Africa’s most populous country has been relatively peaceful.

**Two notable exceptions occurred when Boko Haram members rammed two explosives-laden cars into the lobby of the United Nations office building in 2011, killing at least 21 people and wounded 60, and when militants from the southern oil-producing Niger Delta in October 2010 exploded two car bombs at an Independence Day celebration, leaving at least 12 people dead and 17 injured**. The Movement for the Emancipation of the Niger Delta, which carried out that attack, has been largely dormant since then, except for some sabotage of oil pipelines.

There was no immediate claim for Monday’s bombing, though bus stations are a favored Boko Haram target. In March 2013, the extremists drove a car bomb into the main bus station in Kano, Nigeria’s second-biggest city, killing at least 25 people.

Nigeria’s 170 million people are divided almost equally between Muslims living mainly in the north and Christians in the south. Boko Haram’s campaign to make Nigeria an Islamic state with Sharia, or Islamic law, enforced throughout the country poses the greatest threat to its cohesion and security and threatens nearby countries, where the fighters have gone to train and fight.

“The issue of Boko Haram is quite an ugly history within this period of our own development,” said Jonathan. “Government is doing everything to make sure that we move our country forward … But the issue of Boko Haram is temporary. Surely, we will get over it.”

In May 2013, Jonathan declared a state of emergency and deployed thousands of troops to curb the violence in northeast Nigeria after the extremists took control of entire towns and villages. Security forces quickly forced the Islamic insurgents out of urban areas but have been battling to dislodge them from hideouts, despite near-daily air bombardments and ground assaults this year on forests and mountain caves along the border with Cameroon.

The military has claimed it has the upper hand in the war, but the extremists have fought back with more frequent and ever-deadlier attacks.

Governors and traditional leaders in the northeast have demanded that Jonathan end the state of emergency, saying it is causing suffering and has not been effective. **Some 750,000 people have been forced from towns and villages, including tens of thousands of farmers who had to abandon their farms, risking a food shortage this year.**

There was believed to be only one bomb detonation Monday, with secondary explosions as vehicle fuel tanks ignited and burned. It appeared the explosives were buried in the ground at the bus station, said John Ahwen, counter-terrorism chief of the National Security and Defense Corps. But the National Emergency Management Agency said it thought the explosives were hidden in a vehicle.

“I can’t count the number of people that died. They took them in open vehicles. People were running and there was confusion,” said civil servant Ben Nwachukwu.

**The blast left a hole 4 feet (1.2 meters) deep in the ground of Nyanya Motor Park, about 10 miles (16 kilometers) from the city center. It happened at 6:45 a.m. local time, as people were traveling to work.**

**The deadliest toll in the nearly five-year-old Islamic uprising came March 14 when Boko Haram attacked the main military barracks in the northeast, Giwa Barracks in Maiduguri, and freed hundreds of detainees. Amnesty International said more than 600 people were killed, most of them unarmed detainees gunned down by soldiers.**

Last week, Boko Haram suspects detained at the State Security Service headquarters in Abuja, next door to the residence and office of Jonathan, staged a failed jailbreak in which it is suspected that they had outside help. The agency said 21 detainees were shot and killed and two agents wounded in a shootout that lasted more than two hours.

The militants are blamed for attacks in northeast Nigeria that have killed more than 64 people in the past week, including eight teachers living at a boarding school that had been closed because of frequent attacks on schools in which hundreds of students have died.

**Boko Haram — the nickname means “Western education is forbidden” — has been attacking schools, villages, marketplaces and military barracks and checkpoints this year in increasingly frequent and deadly attacks.**

# Canada Invests in Explosives Detection

Source: http://i-hls.com/2014/04/canada-invests-explosives-detection/

The Canadian Air Transport Security Authority (CATSA) contracted L-3 Security & Detection Systems to supply its high-speed eXaminer XLB explosives detection systems.

The total value of the contract, including service, is approximately $60 million.

L-3’s eXaminer XLB is the first certified dual-energy EDS specifically for screening checked baggage in high-throughput airport environments. Capable of scanning over 1,200 bags per hour in-line, it is designed to keep baggage moving continuously through a meter-wide scanner.

The eXaminer XLB generates high-resolution 3D image data for explosives detection by combining helical computed tomography (CT) with dual-energy imaging. Using 3D continuous flow CT technology, the system generates high-resolution, medical-quality images in real time. Features include 360-degree rotational views of entire bags and individual threat objects.

More than 1,000 eXaminer systems have been deployed at airports domestically and internationally.

# Gulf War and Health, Volume 9: Long-Term Effects of Blast Exposures (2014)

#### Source:http://www.nap.edu/catalog.php?record\_id=18253&utm\_medium=etmail&utm\_source=The%20National%20Academies%20Press&utm\_campaign=Final+Book+2014.04.17+-+Gulf+War+and+Health+9&utm\_content=&utm\_term=

#### Authors

Committee on Gulf War and Health: Long-Term Effects of Blast Exposures; Board on the Health of Select Populations; Institute of Medicine

#### Description

Since the United States began combat operations in Afghanistan in October 2001 and then in Iraq in March 2003, the **numbers of US soldiers killed exceed 6,700 and of US soldiers wounded 50,500.** Although all wars since World War I have involved the use of explosives by the enemy, the wars in Afghanistan and Iraq differ from previous wars in which the United States has been involved because of the enemy's use of improvised explosive devices (IEDs). The use of IEDs has led to an injury landscape different from that in prior US wars. The signature injury of the Afghanistan and Iraq wars is blast injury. Numerous US soldiers have returned home with with devastating blast injuries and they continue to experience many challenges in readjusting to civilian life.

Gulf War and Health, Volume 9 is an assessment of the relevant scientific information and draws conclusions regarding the strength of the evidence of an association between exposure to blast and health effects. The report also includes recommendations for research most likely to provide VA with knowledge that can be used to inform decisions on how to prevent blast injuries, how to diagnose them effectively, and how to manage, treat, and rehabilitate victims of battlefield traumas in the immediate aftermath of a blast and in the long term.

**Contents**

#### Front Matter i-xviii

#### Summary 1-12

#### Introduction 13-20

#### Methods 21-32

#### Pathophysiology of Blast Injury and Overview of Experimental Data 33-84

#### Human Health Outcomes 85-184

#### Recommendations 185-200

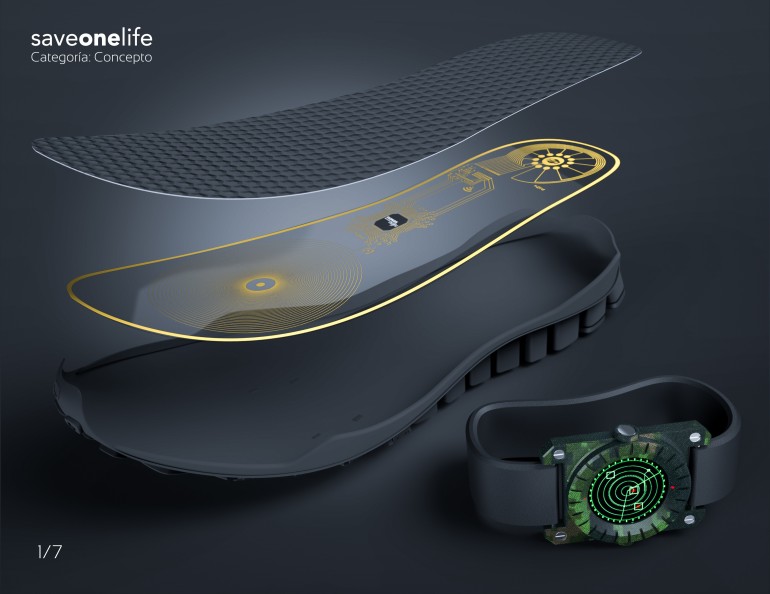
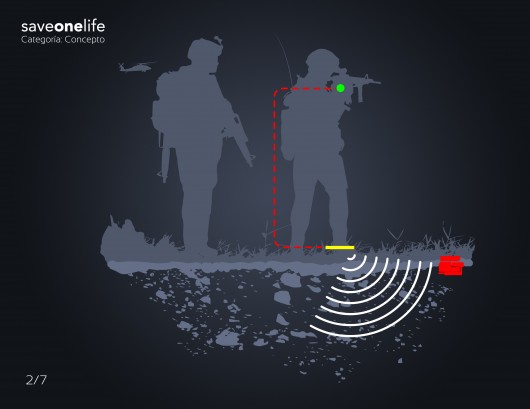
#### Appendix: Committee Biographic Information

# Lemur Studio Design develops mine detector in a shoe

Source: http://www.gizmag.com/lemur-studio-saveonelife/30569/

Boot insoles can turn a pair of really uncomfortable brogues into podiatric clouds that can take a long hike and remove the foot ache. Now, Lemur Studio Design based in Bogota, Colombia, has come up with a concept for insoles that won’t just save your instep, but could save your life. A submission to the World Design Impact Prize 2013-2014 competition, SaveOneLife is a wearable mine detector that fits in a shoe and warns the wearer if and where a potentially deadly landmine might lurk nearby.

Colombia has a major landmine problem. According to the International Campaign to ban Landmines (ICBL), the country is the second most mined in the world after Afghanistan, with over 10,000 casualties since 1990, including about 2,000 killed. Anti-government rebel groups have strewn antipersonnel and antivehicle mines along roads and foot trails, near government bases, in rural areas, around schools, houses, national parks, and indigenous communities’ land. The problem is made worse by drug gangs using mines to protect their coca farms from intruders.

This widespread, often indiscriminate mining combined with the mountainous jungle terrain of the region make detecting and clearing landmines extremely difficult. The notoriously dangerous job requires money, special equipment, and expert crews. It’s a long, slow task that even under the best conditions can take decades to complete. Meanwhile, soldiers, coca eradication teams, farmers, and people in general are at daily risk of being maimed or killed.

According to the designers, SaveOneLife isn’t a solution to the problem, but more of a stopgap technology to reduce the danger from antipersonnel mines. It works on the principle of a metal detector. The insole is made of a conductive material and has a planar coil printed on it. This produces an electromagnetic field. When the wearer walks within two meters (6.5 ft) of a mine containing metal parts, this disrupts the field and is detected by a microprocessor, which is also printed on the insole, as is a radio transmitter. The transmitter sends a signal to a wristwatch-like readout that sounds an alarm and displays the location of the mine on a small screen.

SaveOneLife was designed by Iván Pérez under project leader Lorena Cárdenas. It’s currently at a conceptual stage due to economic reasons, but is designed to be as realistic as possible with the aim of providing a template for eventually coming up with a practical, life-saving device based on nanotechnology.

****Why Ukraine Hasn’t Sparked a Big Cyberwar, So Far

Source: http://www.newsweek.com/why-ukraine-hasnt-sparked-big-cyber-war-so-far-232175

**Cyberwar, we have been warned on countless occasions, will be a major part of the next global conflict. So how is it playing out in Ukraine? The answer is: so far, not so bad.**

A best-case scenario sees the low-level cyberconflict between the United States and Russia remaining unchanged. This means that hacking attacks aimed at collecting information from government and corporate sources continues, quietly and without serious confrontation.

On the scarier side of the spectrum is a full cyberwar, something the world has never seen. This could involve Russian hackers taking down U.S. civilian infrastructure, like power plants and public transport or going after American banks. American and other anti-Russian cyberwarriors would respond in kind.

Cybersecurity experts say the first scenario is much more likely than the second. So far the conflict in Ukraine has seen only limited cyberconfrontation, with some small attacks from Russia on Ukrainian communications and media targets. But cyberspace is a new front in conflicts between world powers and tensions are escalating following Russia’s annexation of Crimea.

As Crimeans went to the polls on Sunday to vote in a referendum on secession from Ukraine, cyberattacks escalated. Hackers struck several NATO websites, including a nonsecure email server.

What would further cyberconflict look like? The entire world of cyberwarfare is opaque. Hackers operate in the shadows. Governments keep their cyberprograms secret.

“Attribution is extremely difficult in cyberspace,” says John Bumgarner, a former U.S. intelligence officer who now works at the U.S. Cyber Consequences Unit, a research institution. “If you have to have attribution where you can trace back a cyberattack, you have to have better monitoring capabilities than the NSA does.”

The U.S. military has Cyber Command (CyberCom), which shares its headquarters with the National Security Agency in Fort Meade, Md., and has an independent budget of $447 million. CyberCom has been growing exponentially in recent years and is set to get even bigger. But most of the details of its activities are highly classified.

Russia is even more secretive. “All of the offensive cyber activities taking place from Russia are under the purview of the security services, which are in deep secrecy,” says Keir Giles, an expert on Russia’s cybercapabilities.

Russia also subcontracts much of its cyberwarfare to nonstate actors, according to Giles. Often “patriotic hackers” will join in on attacking Russia’s enemies. Sunday's attacks on NATO were attributed to a group that calls itself “cyber berkut” and which many believe is affiliated with Russian intelligence agencies.

“You have a very large population of hackers in Eastern Europe in general and Russia especially,” says Dmitri Alperovitch, co-founder of CrowdStrike, a cybersecurity firm. “A lot of them consider themselves patriotic individuals and will take broad direction from government policies. We don’t know how closely they take orders from the government.”

Nonstate actors tend to be less sophisticated than government-orchestrated hacking, relying on simpler operations like denial-of-service attacks, which bombard a website or computer in order to stop it from connecting to the Internet.

**But the Russian government is one of the most sophisticated in the world when it comes to hacking. “They are top-tier actors,” says Alperovitch. “Their capabilities can rival our own. They’ve been spending tremendous resources on this for the last 30 years.”**

The fruits of this spending are usually invisible. Much of the hacking that goes on regularly goes unreported, and people outside this shadowy world usually only know about cyberattacks once they have occurred. Ukrainians are getting some experience these days.

The communications channels of Ukraine’s National Security Council and Defense Council suffered a denial-of-service attack last week, as did the state news agency. Russians were also accused of disrupting Ukrainian phone networks.

Malware detections in Ukraine have “maintained a heightened level on a weekly basis” since early 2014 when the crisis in Ukraine erupted, according to Kurt Baumgartner, the principal security researcher at Kaspersky Lab, a cybersecurity firm. News sites, government communications and organizations and activists communications have also been affected, Baumgartner says.

Russian hacking in Ukraine didn’t begin with the current conflict, though.

**A very sophisticated Russian malware has been infecting Ukrainian computer systems for years,** according to a recent report from BAE Systems, a British defense firm. The malware, known as Snake, allows the attackers to lift data from infected computers and send it back to its point of origin.

While indisputable links to Russian intelligence are hard to draw, the BAE Systems report says **Snake operates on Moscow’s time zone and some of the code is in Russian.**

Still, experts say, Russia has been fairly restrained in its use of cyberweapons so far.

“Russia didn’t have to launch cyberattacks against media outlets in Ukraine. They didn’t have to launch attacks against military websites. Their objective was to seize [Crimea], and they did that,” says Bumgarner. “They didn’t need cyber to seize the territory.”

Russian cyberattacks were more aggressive in previous conflicts. Russian hackers shut down most of the Georgian government’s communications systems during the conflict there in 2008.

Giles remembers sitting in a meeting room with the U.K. military at the time. A dusty fax machine started buzzing. It was the Georgian government. “It was the only way they could get the message out,” he says.

In 2007 Russia unleashed on Estonia one of the biggest cyberattacks in history. Following the quashing of protests by ethnic Russians in the tiny Baltic state, hackers took down government, bank and newspaper websites. Estonia is one of Europe’s most wired countries, leaving it particularly vulnerable. It was impossible to pinpoint the perpetrators, but Moscow was widely blamed for the attacks.

But serious attacks on the United States seem unlikely at this point, experts say.

Instead, Russia and the U.S. engage in mutual espionage. As government and corporate secrets have moved online, the need for a KGB agent in Washington making surreptitious photocopies has diminished and the role of hacking has increased. Hackers directed by Washington and Moscow collect government emails and private communications and release malware to exfiltrate state secrets.

That’s mostly harmless, says Giles, but “the lines are blurred. At what point does breaking into a computer become sabotage?” Some espionage attacks are designed to steal secrets and at the same time render computers and systems nonfunctional. When Saudi Arabia’s national oil company was hit with malware in 2012, the virus did more than just steal secrets. It shut down nearly 30,000 computers.

For now, though, all is quiet on the cyber front between the U.S. and Russia. The level of cyberespionage that is ongoing has not accelerated in any noted way since the conflict over Ukraine began, experts say. But if the conflict gets worse, so will events online.

In October 2011, then-Defense Secretary Leon Panetta warned of the potential for a “digital Pearl Harbor,” a massive cyberattack on U.S. infrastructure or military installations that could cause serious death and destruction.

Some cybersecurity experts say they could foresee something like that happening in the case of a serious escalation in the Ukraine conflict.

“If a shooting war starts, there will be cyberattacks to go along with that,” says Bumgarner. “It could be basic [distributed denial-of-service] attacks or sabotage stuff. But really, I’d be more worried about a 500-pound bomb falling on my head.”

Others are less sanguine. “I think ultimately if this does turn into cyberwarfare, there could be attacks on critical infrastructure,” says Darren Hayes, a professor at Pace University and an expert in digital forensics and cybersecurity. “If you think about someone hacking into the subway system, that’s a pretty serious blow.”

Then again, that might be counterproductive for everyone. Despite tensions, a serious blow to the U.S. economy would harm Russia and a massive attack on the U.S. could precipitate serious retaliation.

“Imagine Russia had the capability to create a small blackout in the U.S. Escalating a cyberattack would be counterproductive,” says Thomas Rid, a professor of war studies at King’s College in London. “Yes, some of them seem to be quite stupid. But I don’t know if they’re that stupid.”

# thumbs up.jpg.pngKaspersky's Real Time Cyber Threat Map Is One Part Cool, Two Parts Terrifying

Source: http://hothardware.com/News/Kasperskys-Real-Time-Cyber-Threat-Map-Is-One-Part-Cool-Two-Parts-Terrifying/

Sometimes it's helpful to have a visual aid to better understand something, and with that in mind, security vendor Kaspersky Labs has launched **an interactive cyber threat map that lets viewers see cyber security incidents as they occur around the world in real time.** It includes malicious objects detected during on-access and on-demand scans, email and web antivirus detections, and objects identified by vulnerability and intrusion detection sub-systems. In other words, you have a front row seat to the attempted carnage that's constantly taking place on the web.

"Every day Kaspersky Lab handles more than 300,000 malicious objects. Three years ago the figure was just 70,000 but antivirus technologies have also changed with the times and we have no problem coping with this huge stream of traffic,” commented Denis Zenkin, Head of Corporate Communications at Kaspersky Lab. "Where do the attacks come from? Where do users click on malicious links most often? Which types of malware are the most prevalent? These are the sort of questions being asked by lots of users. Our new map of the cyberworld threat landscape allows everyone to see the scale of cyber activity in real time and to get a taste of what it feels like to be one of our experts."

This is a nifty thing Kaspersky has put together. Using your mouse (or touch input), you can rotate the globe and zoom into any part of the world to see what the local threat landscape looks like. The various types of threats are color coded to make it easier to tell what you're looking at.

You can also bring up a description of each threat, as well as customize the map by changing the background color, language interface, and display mode from a rotating globe to a flat map. **And while you're there, you can click on a link to see if your PC is infected.**

►**Visit map at:** http://cybermap.kaspersky.com/

# Developments in Iranian Cyber Warfare, 2013-2014

Source: http://i-hls.com/2014/04/developments-iranian-cyber-warfare-2013-2014/

“This website was hacked by the Iranian cyber army.” Photo: INSS

In early 2013, a senior official from the cyber security company CrowdStrike described Iran as a “third tier” country in terms of its cyber capabilities, and estimated that they lagged significantly behind the capabilities of leading countries such as the United States, Russia, Great Britain, and China. The perception was that Iran had the ability to be a nuisance to Western information security systems, but that it lacked the knowledge and means to carry out a strategic cyber attack. **These assumptions largely dissolved over the course of 2013, when Iran became one of the most active players in the international cyber arena.** **Iran’s progress can be attributed to a combination of two elements: a certain easing of the restraints on offensive activity in cyberspace by Iranian decision makers, and a qualitative leap by the Iranian cyber warfare system.** **This major advance by Iran has surprised many Western experts in terms of its scope, its professional sophistication, and the ambitious choice of targets.**

**The Defense Concept: Cutting Iran Off from the World**

From its past experience with events such as the Stuxnet virus and the post-election riots in June 2009, Iran learned the importance of an effective cyber defense system and effective control of the internet. **To this end, Iran has worked on three main tracks to create a multi-dimensional cyber-defense system: (**1) creating a defense envelope against cyber attacks on critical infrastructures and sensitive information; (2) neutralizing cyber operations by opposition elements and regime opponents; (3) keeping Western ideas and content, which could contribute to the development of a “soft revolution” that would harm the stability of the regime, out of Iranian cyberspace.

Each of these three tracks in the Iranian cyber defense system underwent a significant upgrade during 2013, mainly as a result of the maturation of organizational technologies and systems. **First,** Iran has introduced an isolated domestic intranet that gives it close control over content in cyberspace within the country. **Second,** Iran has invested in developing technologies and cyber defense mechanisms locally in order to reduce its dependence on foreign products that could be Trojan horses**. In addition,** the Iranian regime has increased physical enforcement against regime opponents who are active online, mainly through aggressive use of the cyber police. **Furthermore,** the Iranian cyber authorities have instituted a routine of training, exercises, and inspections among the country’s security and civilian institutions. The impact of these measures was reflected during the elections in June 2013, when the Iranian cyber system worked efficiently and largely succeeded in controlling the discourse on the domestic internet and monitoring subversive activity.

It appears that as of today, the Iranian cyber defense system still has a long way to go in coping effectively and consistently with highly sophisticated cyber attacks such as Stuxnet. But Iran’s technological and organizational leap in the past year indicates that the Iranians could formulate a comprehensive and effective defense system sooner than anticipated.

**The Offense Dimension: Seeking “High Quality” Attacks**

The Islamic Republic sees the cyber arena as an effective offensive platform enabling it to cause harm to adversaries with clear military superiority, and at the same time, maintain a margin of denial that will prevent international censure or even sanctions and a counter attack. During 2013, cyber warfare became a key tool used by Iran to attack Western targets in response to the sanctions and as a means of deterring escalation by Western countries against Iran. The scope, targets, and relative success of those cyber attacks of the past year ascribed to Iran show its improved capabilities. Western sources attribute the progress in Iran’s cyber warfare program to its success in combining the capabilities, knowledge, and manpower in Iranian computer science departments with the experience and capabilities of the Iranian hacker community, much of which identifies with the regime and its goals. Furthermore, the increasingly close ties between the Iranian cyber system and cyber criminals, hackers, and information security experts, mainly Russians, who are prepared to sell their services for money, contribute to the rapid progress in Iran’s cyber warfare program. In addition to reinforcing its own cyber system, Iran is working to expand and strengthen the cyber warfare capabilities of its allies. It appears that the Iranians are seeking to create an effective system of proxies that work for them in cyberspace. One of the centers of this Iranian activity is in Syria, where Iran is supporting the Syrian Electronic Army (SEA), a hackers organization that is an increasingly important player in cyberspace.

The progress in Iranian cyber warfare capabilities can be seen in a number of attacks that occurred in the second half of 2012 and during 2013. These attacks made use of sophisticated techniques, had high quality targets, and were wider in scope than previous Iranian attacks. **Among the most prominent of these was the large scale attack on websites of major banks and financial institutions in the United States, which one information security expert described as unprecedented in scope and effectiveness.** Another wave of attacks blamed on Iran focused on **US energy and infrastructure companies** and involved attacks on control systems that could have harmed their physical operation or the safety measures for critical infrastructures such as gas and oil conducting systems and electrical systems. In the past year, Iranian-affiliated elements have also taken responsibility for cyber attacks against Israeli institutions, and in June 2013 Prime Minister Benjamin Netanyahu announced that there had been a significant increase in Iranian cyber attacks against important computer infrastructures in Israel.

The rapid development of Iran’s cyber warfare capability and that of its proxies and allies means that Israel and other Western countries must work decisively and systematically to maintain qualitative and operational superiority in cyberspace. The importance of cyberspace for Israel’s security concept and the urgency of creating a “digital Iron Dome” were well expressed by IDF Chief of Staff Lt. Gen. Benny Gantz: “Israel must be on a superpower level in cyberspace…we must not wait with this.”

# Exclamation_red.png'Heartbleed' computer bug threat spreads to firewalls and beyond

Source: http://www.reuters.com/article/2014/04/10/us-cybersecurity-internet-bug-idUSBREA3804U2014 0410

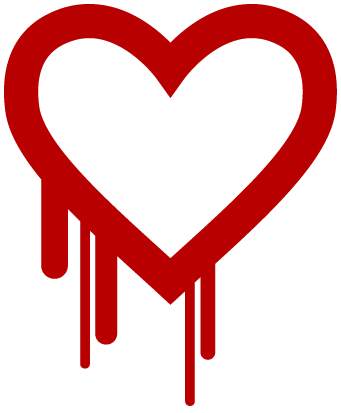
April 10 – Hackers could crack email systems, security firewalls and possibly mobile phones through the **"Heartbleed" computer bug**, according to security experts who warned on Thursday that the risks extended beyond just Internet Web servers.

The widespread bug surfaced late on Monday, when it was disclosed that a pernicious flaw in a widely used Web encryption program known as OpenSSL opened hundreds of thousands of websites to data theft. **Developers rushed out patches to fix affected web servers when they disclosed the problem, which affected companies from Amazon.com Inc and Google Inc to Yahoo Inc.**

Yet pieces of vulnerable OpenSSL code can be found inside plenty of other places, including email servers, ordinary PCs, phones and even security products such as firewalls. Developers of those products are scrambling to figure out whether they are vulnerable and patch them to keep their users safe.

"I am waiting for a patch," said Jeff Moss, a security adviser to the U.S. Department of Homeland Security and founder of the Def Con hacking conference. Def Con's network uses an enterprise firewall from McAfee, which is owned by Intel Corp's security division.

He said he was frustrated because people had figured out that his email and Web traffic is vulnerable and posted about it on the Internet - but he can't take steps to remedy the problem until Intel releases a patch.

"Everybody is going through the exact same thing I'm going through, if you are going through a vendor fix," he said.

An Intel spokesman declined comment, referring Reuters to a company blog that said: "We understand this is a difficult time for businesses as they scramble to update multiple products from multiple vendors in the coming weeks. The McAfee products that use affected versions of OpenSSL are vulnerable and need to be updated."

It did not say when they would be released.

The Heartbleed vulnerability went undetected for about two years and can be exploited without leaving a trace, so experts and consumers fear attackers may have compromised large numbers of networks without their knowledge.

Companies and government agencies are now rushing to understand which products are vulnerable, then set priorities for fixing them. They are anxious because researchers have observed sophisticated hacking groups conducting scans of the Internet this week in search of vulnerable servers.

"Every security person is talking about this," said Chris Morales, practice manager with the cybersecurity services firm NSS Labs.

**Cisco Systems Inc,** the world's biggest telecommunications equipment provider, said on its website that it is reviewing dozens of products to see if they are safe. It uncovered about a dozen that are vulnerable, including a TelePresence video conferencing server, a version of the IOS software for managing routers. A company spokesman declined to comment on how those issues might affect users, saying Cisco would provide more information as it became available.

**Oracle Corp** has not posted such an advisory on its support site. Company spokeswoman Deborah Hellinger declined to comment on Heartbleed.

**Microsoft Corp,** which runs a cloud computing and storage service, the Xbox platform and has hundreds of millions of Windows and Officer users, said in a statement that "a few services continue to be reviewed and updated with further protections." It did not identify them.

Officials with technology giants IBM and Hewlett-Packard Co could not be reached. EMC Corp and Dell said they had no immediate comment.

Security experts said the vulnerable code is also found in some widely used email server software, the online browser anonymizing tool Tor and OpenVPN, as well as some online games and software that runs Internet-connected devices such as webcams and mobile phones.

Jeff Forristal, chief technology officer of Bluebox Security, said that version 4.1.1 of Google's Android operating system, known as Jelly Bean, is also vulnerable. Google officials declined comment on his finding.

Other security experts said that they would avoid using any device with the vulnerable software in it, but that it would take a lot of effort for a hacker to extract useful data from a vulnerable Android phone.

## How computer worms are spreading among smartphones

Source: http://www.homelandsecuritynewswire.com/dr20140411-how-computer-worms-are-spreading-among-smartphones

Professor Kevin Du and a team of researchers from the College of Engineering and Computer Science at Syracuse University have recently discovered that **some of the most common activities among smartphone users — scanning 2D barcodes, finding free Wi-Fi access points, sending SMS messages, listening to MP3 music, and watching MP4 videos — can leave devices vulnerable to harmful “computer worms.”**

These worms can infiltrate smartphones through apps designed in a specific computer language/code — and they can do more harm than just steal the device owner’s personal information, researchers warn. They can also spread to the owner’s friends and personal contacts.

“These attacks target an increasingly popular type of app known as HTML5-based app,” says Du who worked on the research with students Xing Jin, Tongbo Luo, and Derek G. Tsui.

**“Traditionally, apps are developed using a platform’s native technologies, such as Java in Android and Object C in iOS. HTML5-based apps do not use platform-dependent native technologies, but use JavaScript instead, which is universally supported by all platforms.**

“The advantage for developers is clear: write an app once and it can run on all major platforms,” Du explains.

A Syracuse University release reports that the team has so far identified fourteen vulnerable HTML5-based apps from three types of mobile systems, including Android, iOS, and Blackberry. Developers of those vulnerable apps have been informed and in an effort to give them time to fix the problem, researchers have decided not to disclose the names of the vulnerable apps.

“Imagine you’re at the airport and you want to find the free Wi-Fi. When you scan, your phone is going to display the Wi-Fi access points. That could be an easy channel for a hacker to inject malicious worm code into your smartphone,” Du says. “Once the worm takes control, it can duplicate itself, and send copies to your friends via SMS messages, multimedia file sharing, and other methods.”

Researchers are currently working to develop solutions to help users and app developers detect and prevent such attacks.

Details of how attacks can occur this attack are described in a paper titled “XDS: Cross-Device Scripting Attacks on Smartphones through HTML5-based Apps” that the team will present at the Mobile Security Technologies workshop in May.

Du and his team are continuing their research to see what other apps might be at risk.

“We are launching a large scale search in the Google Play market and expect to find more vulnerable apps,” says Du. “By 2016, it’s estimated that more than fifty percent of the mobile apps will be produced using HTML-5 technology. This is just a disaster waiting to happen,” he adds.

*— Read more in “Injecting Malicious Code Into HTML5-Based Apps” (Syracuse University, 2014)*

****Physical Security of Electric Grid on FERC’s Radar

Source: http://www.energymanagertoday.com/physical-security-of-electric-grid-on-fercs-radar-099493/

Energy Regulatory Commission (FERC) has directed the North American Electric Reliability Corporation (NERC) to develop standards that address physical security risks and vulnerabilities of the nation’s power grid.

FERC’s directive comes after Jon Wellinghoff, a former FERC chairman, told the Wall Street Journal he was concerned that the nation’s electric-grid isn’t adequately protected against attacks.

**“Because the grid is so critical to all aspects of our society and economy, protecting its reliability and resilience is a core responsibility of everyone who works in the electric industry,”** said FERC Acting Chairman Cheryl LaFleur. “Today’s order enhances the grid’s resilience by requiring physical security for the facilities most critical to the reliable operation of the Bulk-Power System. The reliability standards directed by today’s order require owners and operators of the Bulk-Power System to take at least three steps to protect physical security. **First,** owners and operators must perform a risk assessment of their system to identify facilities that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation, or cascading failures of the Bulk-Power System. **Second,** owners and operators of critical facilities must evaluate potential threats and vulnerabilities to those facilities. **Finally,** owners and operators must develop and implement a security plan to address potential threats and vulnerabilities.”

**NERC has 90 days to submit the proposed standards.**

U.S. Army Corps Eases Up on its Stance Against Trees on Levees

Source: http://www.emergencymgmt.com/disaster/US-Army-Corps-Stance-Trees-on-Levees.html

**The U.S. Army Corps of Engineers has decided it will no longer force local levee agencies to choose between keeping trees on their levees and losing federal money for disaster assistance.**

On Monday, the Army Corps announced in a new "interim" policy that it will not disqualify levees that fail to meet its maintenance criteria from receiving disaster relief funding, essentially granting a reprieve to thousands of miles of California riverside habitat. The move appears to resolve, for now, a long-running policy dispute that pitted the state of California against the powerful federal flood-control agency.

"This is really quite a substantial change," said Tammy Conforti, levee safety program manager at the Army Corps. "That specific vegetation criteria won't be one of the criteria that has to be met."

**Until now, the agency has said that trees threaten levee safety and must be removed.** It argued that tree roots could serve as a path for seepage through a levee, or that trees could topple over in a storm and tear out chunks of a levee. Its vegetation standards allow nothing but short grass, not even small shrubs or trees.

Levees with too many trees risked being disqualified from a federal program that provides millions of dollars in levee repair grants in the event of a flood. Such a disqualification also put communities at risk of displeasing the Federal Emergency Management Agency, which sets flood insurance rates.

The policy pushed California levee districts to make a tough choice: Spend millions of dollars cutting down trees essential to habitat and risk violating other environmental laws, or risk going without federal flood relief money.

There has been little scientific proof that trees actually threaten levee stability. Officials at the California Department of Water Resources and the Department of Fish and Wildlife both oppose the policy, warning it could bankrupt local levee districts and destroy the last of the state's riverside habitat.

In the new "interim" policy, the Army Corps is now saying it will still inspect levees according to the same vegetation standards, but will no longer use that particular rating to decide whether a "local sponsor" agency is eligible for financial assistance. The vegetation rating will be informational only.

"We want to make sure we're not incentivizing local sponsors to do something with the vegetation without taking into account endangered species," Conforti said. "We heard the public feedback and take that very seriously that we need to better take into account local objections, local constraints."

George Qualley, a flood management policy adviser at the California Department of Water Resources, praised the Army Corps move and said it would allow levee districts to spend their limited funds on more pressing issues, such as erosion and encroachment by buildings and utilities. He said the emphasis on vegetation was a potentially costly distraction.

"I never could figure out why they were making such a focus on it," Qualley said. "My initial impression is it's a step in the right direction and they are cognizant of what's really important as far as keeping the levees safe. I would just say good for them; they've finally put something out there with logic to it."

So far, only one Central Valley levee agency -- serving part of the city of Marysville -- has been disqualified because of vegetation problems. Army Corps officials said that agency can now request a new inspection and have its eligibility for disaster relief reinstated if no new problems are found.

Conforti said the Army Corps is working to permanently revise its maintenance standards and will likely complete that process a year from now. It will include an opportunity for public comment. She said the details are uncertain, but hinted that the new approach to inspecting vegetation will become permanent.

"We're moving away from a strict black-and-white, 'Here's all your deficiencies and we're going to tell you what to fix and when' approach," Conforti said. "We're going to be focusing on more sponsor-led activities that are focused on reducing risk."

**Bob Wright, attorney at Friends of the River in Sacramento, said the change marks a victory but not the end of his battle. Wright's group, along with the Center for Biological Diversity and Defenders of Wildlife, sued the Army Corps in 2011 over its vegetation policy. They argue it violates the Endangered Species Act and National Environmental Policy Act.**

A federal judge in 2012 struck down a motion by the Army Corps to dismiss that case. Wright speculated this may have led to the new interim policy announced Monday. He now intends to submit his own motion to dismiss the case, probably next month.

"They're trying to publicly avoid admitting they were wrong," Wright said. "We can all feel pretty good that we're going to be keeping the trees and shrubs on the levees in California's Central Valley."

# New Emergency Warning System Launched In Belgium

Source: http://i-hls.com/2014/03/new-emergency-warning-system-launched-belgium/

Belgium’s Minister of the Interior, Joëlle Milquet has announced the pilot launch of an emergency population warning and information system in Belgium.



Illustration. Photo: Superbass / CC-BY-SA-3.0 (via Wikimedia Commons)

Thales was selected in November 2013 by the CRISIS Center of the Federal Public Service (FPS) Internal Affairs to provide Belgium with the **new system called BE-ALERT.**

According to HS Today in response to various incidents in Belgium in recent years, the ability to alert the population rapidly, selectively and effectively is a central component of the CRISIS Center’s policy to upgrade and extend its channels of communication.

Thales and program partner Unified Messaging Systems (UMS) of Norway, specialists in early warning and mass notification solutions, designed and implemented the BE-ALERT national warning system, incorporating proprietary technology from UMS for the Belgian authorities responsible for CRISIS management at the local, provincial and national level.

Thales provided the CRISIS Center with additional support for the rollout of the pilot, including local assistance, training operators and adapting the system to the customer’s exact requirements.

BE-ALERT takes the form of a secure platform that is accessed via the Internet. Beginning March 17, every citizen has been able to register with the system online at so that they can receive alerts directly.

After the test and analysis period, the BE-ALERT system will be rolled out nationally and made available to all governors and local authorities across the country.

►**BE-ALERT:** http://be-alert.be/

## New York will issue red license plates for government emergency response vehicles

Source: http://www.homelandsecuritynewswire.com/dr20140410-new-york-will-issue-red-license-plates-for-government-emergency-response-vehicles

Governor Andrew Cuomo last week announced that the Department of Motor Vehicles will begin issuing the first **New York State emergency management red license plates for vehicles registered to state agencies and political subdivisions such as counties, cities, towns, and villages.** Vehicles that serve a critical role will be given the new emergency license plates to assure they have immediate access to locations impacted during a state emergency as well as prioritized access for assets such as emergency fuel supplies. The red plates will carry a new Emergency Management (EM) indicator for quick identification.

“New York has lived through the new reality of repeated extreme weather and natural disasters and we are reimagining every part of how our state responds so that when the next storm comes, we are ready,” Cuomo said. “We are distributing the new red emergency license plates to local governments and agencies free of charge to help prioritize response efforts statewide. This will help law enforcement and first responders respond faster and keep New Yorkers safe when the worst happens.”

**The new plates will have a white background and a red banner with the “EM” designation appearing in the upper left hand corner.** The name of the state agency or the political subdivision and its county of primary use will also be displayed on the plate. “State” will appear at the bottom of state agency plates. Sample images of the new plates can be viewed here and here.

The New York State Department of Homeland Security and Emergency Services will determine how many red license plates will be available to the various agencies and localities. Initially most localities will be entitled to register for a minimum number of red plates. The vehicle must either be owned or controlled and registered in the name of the state agency or locality in order to be eligible for the new red license plate. Additionally, the highest ranking government official in each locality will certify that the identified vehicles are eligible for this program.

Letters were sent recently to the heads of eligible state agencies and political subdivisions to advise them of the availability of these plates and to provide them information on how to apply. The new plates will begin to be distributed to the agencies and political subdivisions as applications are received and processed. There is no charge for the new plates.

A political subdivision is defined as a subdivision of New York State that has been delegated certain official functions of state or local government including a government entity created by, or under the authority of, State law. Volunteer organizations are not political subdivisions.

Barbara Fiala, commissioner of the Department of Motor Vehicles said, “We are sure that providing these emergency plates to the various state and local entities will benefit all New Yorkers in time of emergency or significant storms. We will be working with DHSES and the various localities to make sure that these plates are distributed in a timely manner.”

Jerome Hauer, commissioner of the New York State Division of Homeland Security and Emergency Services said, “This is another component of the Governor’s plan to ensure New York is the best prepared state in the nation. These plates will aid in quickly identifying people with the critical need to enter areas that have restricted access and who should be on the road during times of emergency. It is another step forward in better preparing our state.”

New Multimedia Communications Platform Links Schools, First Responders for Security, Safety

Source: http://www.hstoday.us/single-article/new-multimedia-communications-platform-links-schools-first-responders-for-security-safety/baecbf77fff98c0e2c1370ac4940f56e.html

**Tailored for schools, a new multimedia communications platform developed by Mutualink provides K-12 schools with the capability to establish a direct link with police, fire, EMS and other first responders in emergency situations.**

The all-in-one device acts as a gateway for real-time voice, video, data and text communications, giving first responders increased situational awareness and rapid response time, the company said.

**The new Mutualink K12 communications system also includes a panic button which enables teachers or administrators to alert first responders to an emergency with the push of a button.**

“Mutualink’s K12 program includes an all-in-one gateway device to bridge radio, video, telephone and public address/intercom systems while addressing the limited budgets of school systems,” the firm said in an announcement. “The program is designed and licensed exclusively for public, private and parochial K-12 schools.

“While many school districts are increasing their investment in security measures, such as video surveillance systems or Radio over IP (RoIP) solutions, these systems operate in a single media form with first responders in crisis situations,” the company said. “Mutualink K12 bridges a full complement of the school devices and media and enables real-time multimedia resource sharing with police and other agencies, even bridging communications between disparate communications systems including legacy and forward-looking equipment.”

“The ability to instantly and securely share multimedia information in an emergency situation – including live video feeds, school building blueprints and police and fire radio to school radio and public address audio -- is a potentially life-saving asset to first responders and the students and teachers they are protecting,” said Patrick V. Fiel, Sr., former executive director of security for Washington, DC public schools.

“Our goal with Mutualink K12 is to provide schools with an affordable, effective means to communicate and share critical information with first responders in the face of an emergency, but equally important, it is a solution to plan and practice response,” said Mutualink CEO Mark Hatten. “Also significant is the peace of mind that comes from knowing that everyone is working together, with the most advanced technology, to protect students, teachers and school officials on a daily basis.”

“The fact that Mutualink K12 ensures that all parties maintain control over their resources cuts down on time-wasting red-tape while protecting the privacy of everyone involved,” Fiel said, adding that Mutualink’s invitation-based platform, no memorandum of understanding between the schools and public safety agencies is required because each agency maintains sovereign control over their communication resources.

“The Mutualink system also includes panic buttons. One type is wired and similar to those found in banks,” the company explained. “Activating it instantly creates a multimedia sharing session and alerts first responders in the event of an emergency, automatically engaging radio and/or video communications. The other panic button is an app that installs on school staff and teachers’ smartphones. Both methods create an instant connection of the Mutualink system to law enforcement that activates communications and enables a quicker, more fully informed response.”

“Security and sovereignty” are also key features of Mutualink’s communications platform, which is utilized by hundreds of public safety, emergency management, private security and defense agencies worldwide,” the company said. “Schools using Mutualink K12 share video, audio and other information, sharing their communications assets only as necessary, and only with trusted parties of their choosing. All participants maintain sovereign control of their communication resources. Mutualink’s platform is IP-based, with multi-level encryption and a distributed architecture.”

**Key Benefits of Mutualink K12 includes:**

* Video and audio sharing capabilities to enable police to “see into the school” before entering;
* Security, privacy and sovereignty are all designed into the Mutualink system;
* Panic button initiates emergency response with the touch of a button; and
* Very low recurring costs are an important consideration for taxpayer-funded procurements.

Understanding the Gaps in Cybersecurity of Emergency Management

**By Anthony Kimery** (Executive Editor HSToday.com)

Source: http://www.hstoday.us/single-article/understanding-the-gaps-in-cybersecurity-of-emergency-management/d44df780114f9fb12f28a1d2a90116fb.html

Additional work is needed at all levels of government to address the myriad capability gaps in cybersecurity preparedness and response among the first responder and emergency management community, according to a new Federal Emergency Management Agency (FEMA) Lessons Learned Information Sharing (LLIS) research team trend analysis.

The LLIS team arrived at this conclusion after reviewing the 2012 State Preparedness Reports (SPRs) and 16 After Action Reports (AARs) related to cybersecurity.

In an effort to explore and understand key gaps in the cybersecurity capability of the emergency management community, the LLIS.gov team conducted research and analysis to examine the challenges confronting cybersecurity efforts and to identify overall trends within cybersecurity.

“The goal of the analysis was to identify recurring issues to help emergency managers address challenges in cybersecurity efforts and establish a framework for further research into specific cybersecurity issues,” the LLIS trend analysis said.

The following are key trends identified as a result of the analysis.

**Planning**

Many states and localities lack effective plans to manage cybersecurity efforts and ensure the availability of necessary resources.

**Key topics, gaps and areas of interest within planning in cybersecurity:**

* Developing a cybersecurity plan at a state or local level;
* Establishing pre-defined support agreements; and
* Establishing or including resource acquisition plans.

**Coordination**

The LLIS trend analysis said that “Proper coordination to ensure all entities are working in unison to prevent and respond to cyber incidents is an integral element of cybersecurity. It is essential that entities at all levels of government work together, including working with the private sector, to overcome the broad scope and rapid spread of cyber incidents. This includes facilitating information sharing about threats and attacks and leveraging resources to reduce risk and mitigate damage.”

**Key topics, gaps and areas of interest within coordination in cybersecurity:**

* Handling incident coordination;
* Improving information sharing & information gathering;
* Forming public-private partnerships; and
* Enabling coordination between state and federal resources.

**Incident response**

“Understanding roles and responsibilities of federal and state authorities, as well as use of response tools, can help effectiveness of response efforts to cyber incidents,” the FEMA LLIS trend analysis report said. “Issues with communication and outreach about cybersecurity threats and the impact of ongoing cyber incidents can further impede response capacity.”

**Key topics, gaps and areas of interest within incident response in cybersecurity:**

* Agency response tools and tactics (including, but not limited to, electronic tactical response, and response from law enforcement, firefighting, medical/public health, and public works personnel);
* Determining the role and decision-making process of federal entities;
* Determining the role and decision-making process of state entities; and
* Maintaining and improving communications and outreach.

**Prevention**

The LLIS research team said “Authorities can help prevent the occurrence of cyber incidents and mitigate risks by performing assessments of system’s capacity to handle incidents and by taking steps to limit potential opportunities for unauthorized access to systems.”

**Key topics, gaps, and areas of interest within planning in cybersecurity:**

* Preventing unauthorized access to systems;
* Situational awareness & threat detection;
* Identifying new threats and innovations in the cyber field; and
* Evaluating continuity of service capability & establishing redundancies in essential systems.

**Training & exercises**

Authorities at all levels could benefit from improvements in training and exercise programs to increase awareness of cybersecurity issues, identify potential threats to systems, and evaluate the effectiveness of existing plans and response capability.

Key topics, gaps, and areas of interest within training and exercises in cybersecurity:

* Developing and executing programs to improve awareness & recognition of issues;
* Creating and conducting cybersecurity exercises; and
* Cybersecurity training programs and educational materials.

FEMA’s LLIS team also noted that “insufficient funding and personnel shortages create capability gaps by impeding employee training, the development of institutional knowledge and response capacity.



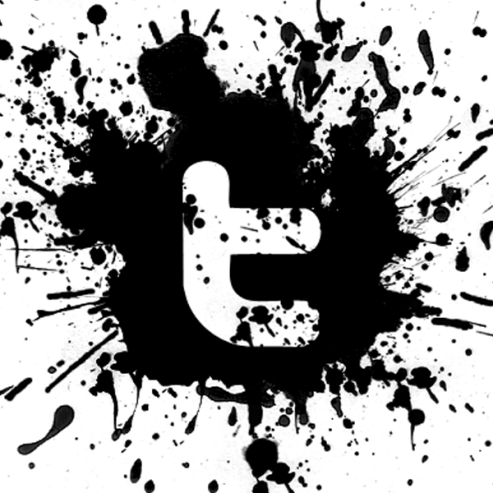


Controlling Rumors on Social Media Crucial During a Disaster, Terrorist Attack

Source: http://www.hstoday.us/single-article/controlling-rumors-on-social-media-crucial-during-a-disaster-terrorist-attack/d5c5b86c2bcfcacc424de4b9d7d9166f.html

Authorities around the world should set up emergency communication teams to manage the amount of misinformation that is circulated on social media websites during disasters, terrorist attacks and other social crises, a new study published in *MIS Quarterly* said.

**The new study, “Community Intelligence and Social Media Services: A Rumor Theoretic Analysis of Tweets During Social Crisis,” by Onook Oh of the Warwick Business School; Manish Agrawal of the University of South Florida; and Raghav Rao of the State University of New York at Buffalo, examined the use of social media in three major incidents, including the terrorist attacks in Mumbai, India in 2008.**

The study revealed that **Twitter is emerging as the dominant social reporting tool to report eye-witness accounts** and to share information on disasters, terrorist attacks and social crises as a collective effort to make sense of what is happening.

However, the study noted, when it’s the online community that creates and exchanges news about a crisis situation rather than official news media, the facts and perceptions about unfolding events can be exaggerated. It also unintentionally turns this information into mis-information, diverting attention from the real problems.

Oh, who is assistant professor of information systems, believes authorities and organizations involved in responding to a disaster or terrorist attack need to set up an emergency communication center to provide speedy, relevant information on an unfolding crisis and to confirm or dispel misinformation circulated on social media.

**The study by Oh and his colleagues, which is the first application of rumor theory to social media and community intelligence, analyizes three large Twitter data sets:** the 2008 Mumbai terrorist attacks, where a group of gunmen killed 165 and injured 304 people; the May 2012 shooting of five people by a gunman in Seattle; and the recall of four million cars by Toyota in 2009 and 2010 because of a faulty accelerator pedal.

Within minutes of the initial terrorist attack in Mumbai, a local resident posted a stream of pictures on the photo sharing website Flickr. Almost concurrently, a group of people voluntarily formed a Twitter page with a link to the Flickr site and spread eyewitness accounts of the terrorist attacks with texts, photos and links to other sources.

While the flurry of social media activity had many positive outcomes -- enabling people to contact family members, encouraging blood donations and providing eyewitness accounts -- it also caused many rumors to circulate.

**In total, they analyzed 20,920 tweets on the Mumbai attacks from the moment the attacks occurred on November 26 through November 30.**

“Natural disasters and crises such as terrorist attacks provide the optimum conditions for rumors to spread which can exacerbate the situation for emergency response operations and cause panic amongst the public,” Oh said. “For example, during the Mumbai terrorist attacks, the police control room was flooded with incorrect reports of explosions at leading hotels.

“**Misinformation on the internet** was also influencing what was being reported on official news channels,” Oh said, noting that “the **BBC was forced to admit they had made a mistake after using Twitter coverage of the Mumbai terror attacks as a source of their official news**.”

Oh believes the main motivation for people turning to Twitter in a crisis is to find out what is happening in their immediate area or to acquaintances. But in order to control the flow of misinformation, emergency communication centers need to be set up quickly to respond to misinformation through social media channels.

“People use mainstream media to try to make sense of the situation but it usually provides general information or repeatedly broadcasts a few sensational scenes over and over again,” Oh said, citing the **Federal Emergency Management Agency’s Rumor Control Center website during Hurricane Sandy in 2012 as an example of one way of using emergency communication centers.**

“What people involved in the crisis really want is very localized information in real time to aid their decision-making,” Oh said. “Hence, they rapidly realize that mainstream media do not provide them with local information that they desperately need to overcome the extreme situation.” Consequently, “they turn to social media such as Facebook and Twitter,” he said.

“Emergency response teams need to put in place prompt emergency communication systems to refute the misinformation and provide citizens with timely, localized and correct information through multiple communication channels such as website links, social network websites, RSS, email, text message, radio, TV or retweets,” Oh explained.

“In cases of community disasters,” Oh continued, “emergency responders need to make extra effort to distribute reliable information and, at the same time, control collective anxiety in the community to suppress the spreading of unintended rumor information. This includes the setting up of an ‘emergency communication center’ in the local community who would monitor social media very closely and respond rapidly to unverified and incorrect rumor information.”

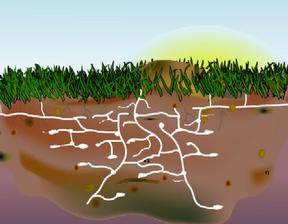
**“Given that the motivation of rumoring is fundamentally to make sense of uncertain situations such that people can deal with a possible threat, the provision of timely and certain information may lead to successful crisis management in partnership with voluntary online citizens,”** Oh said.

## Learning from ant colonies how to evacuate disaster zones

Source: http://www.homelandsecuritynewswire.com/dr20140417-learning-from-ant-colonies-how-to-evacuate-disaster-zones

An escape route mapping system based on the behavior of ant colonies could give evacuees a better chance of reaching safe harbor after a natural disaster or terrorist attack by building a map of showing the shortest routes to shelters and providing regular updates of current situations such as fires, blocked roads, or other damage via the smart phones of emergency workers and those caught up in the disaster.

An Inderscience Publishers release reports that Koichi Asakura of Daido University in Nagoya and Toyohide Watanabe of the Nagoya Industrial Science Research Institute in Japan have carried out successful simulations of the construction of navigational maps using this approach and report details in the International Journal of Knowledge and Web Intelligence.

Following a major earthquake, tsunami, typhoon, or other disaster it is crucial for those affected, including emergency workers, to obtain and share accurate and timely information about the situation as it unfolds. Lives can only be saved if evacuation to safe areas and shelters is not stymied by blocked roads, fires, and other problems.

The team’s new system has two key features: First, it utilizes the smart phones which are now ubiquitous across cities as networked, mobile sensors that can feed information back to emergency centers. The second feature exploits our understanding of the behavior of an ant colony. This provides a way to determine whether or not particular problems are recent or not, just as individual ants use pheromone trails, and the concentration changes in those pheromones to assess how recently a colony member left a particular signal and so find the optimal routes to and from the nest via food supplies. By using this approach to analyze the data from myriad smart phones as evacuees head for shelter, it is possible to build an active navigational map using the phones’ GPS and other tools.

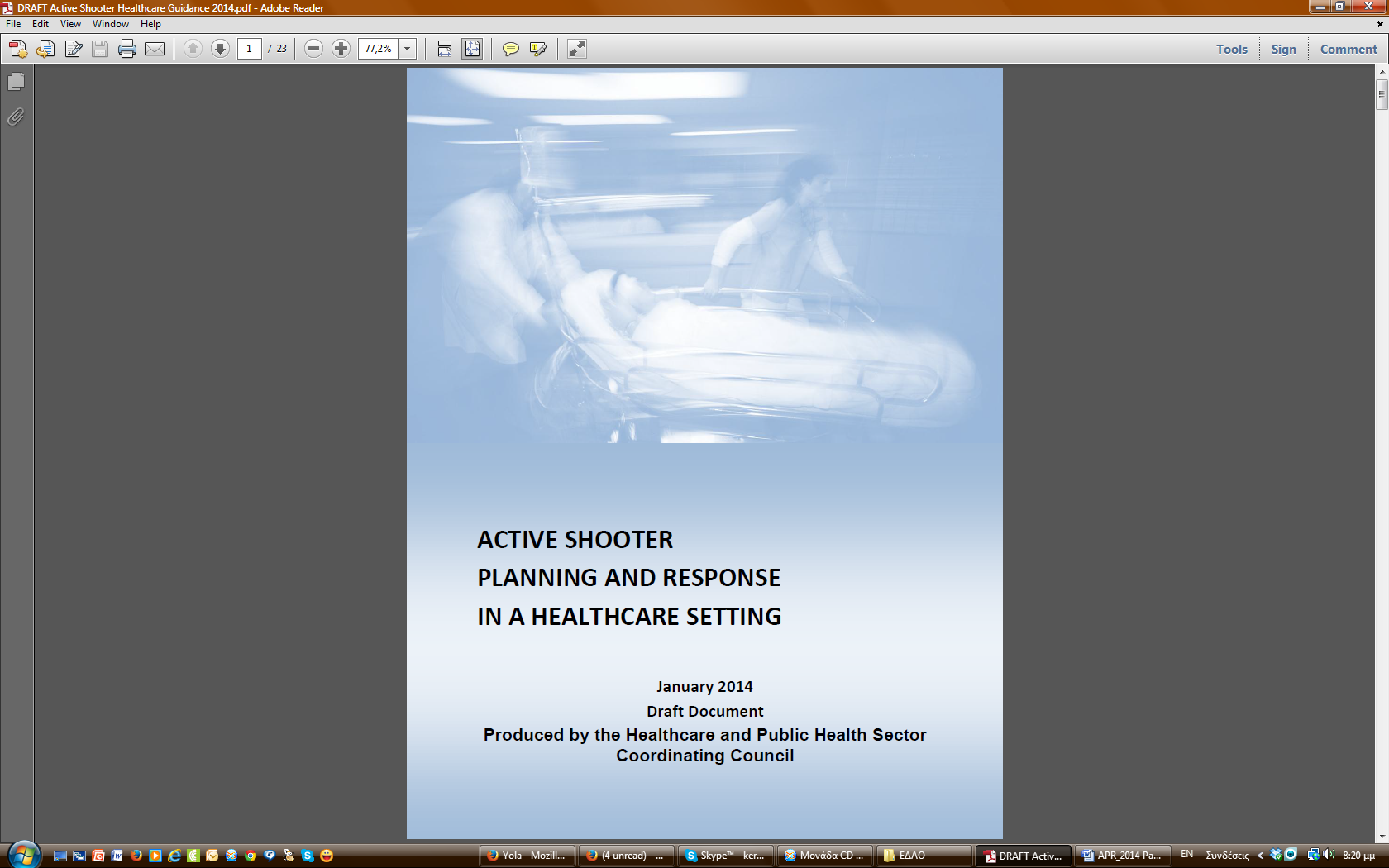
The system circumvents the problem that would be almost inevitable during a disaster that closed circuit television (CCTV) cameras would be unreliable whereas sufficient numbers of wireless communication devices might remain active for sufficient time given a large enough number of service providers and communication towers spread widely across the disaster area.

The next step will be to develop an ad hoc mobile networking system so that evacuees can themselves access these active maps rather than the present system that provides advice to emergency services for guiding evacuees. Such a network might also circumvent the problem of service provider outages by allowing individual smart phones to create a local network.

*— Read more in Koichi Asakura and Toyohide Watanabe, “Construction of navigational maps for evacuees in disaster areas based on ant colony systems,”* International Journal of Knowledge and Web Intelligence *4 (2014): 300-13*

**Active shooter planning and response in a healthcare setting**

Source:https://programs.gha.org/Portals/5/documents/DRL/2014/Headlines/DRAFT%20Active%20Shooter%20Healthcare%20Guidance%202014.pdf

**The key message of this document is that hospitals and academic health centers represent a very unique set of challenges for active shooter planning**. The individual uniqueness of healthcare facilities and the limitations as a result of size, location, critical care access versus acute care, rural versus urban versus suburban, the presence of students, whether you have security, law enforcement availability and response times are just a few of the many challenges when developing a response to Active Shooter. For this reason, we recommend that as you develop your plan, you consider the planning guidance listed below and determine what works best in your particular circumstances. You will notice however that all of the guidance below shares a common set of principles. The first of these principles is that your plan should seek to maximize the protection of life. If possible, evacuation away from the incident will reduce the number of people in harm’s way, and facilitate the police response. Another principle is that in the end, individuals will have to make decisions based on their assessment of the situation in how best to maximize the protection of life and what tactics to employ. When all other options have been exhausted, an individual decision to engage or fight the shooter may be the only tactic available. Another important principle for healthcare is that individuals may have a duty of care for patients – in your planning, you should determine any specific requirements that your organization may have and include this in staff training so that they may include this aspect in determining the best course of action to take in maximizing the protection of life.

The primary purpose of your response plan shall be to prevent, reduce or limit access to potential victims and to mitigate the loss of life. Options for consideration in developing your response plan are:

**Alice Active Shooter Response**

“ALICE” is an acronym for five steps the proponents say can be used to increase your chances of surviving a surprise attack by an Active Shooter. ALICE stands for:

**A**lert – Can be anything

**L**ockdown – This is a semi-secure starting point from which to make survival decisions. If you decide not to evacuate, secure the room.

**I**nform – Using any means necessary to pass on real time information

**C**ounter – This is the use of simple, proactive techniques should you be confronted by the Active Shooter.

**E**vacuate – Remove yourself from the danger zone as quickly as possible

**R**un, **H**ide, or **F**ight

**Is a three step process to prevent or reduce loss of life in an active shooter event.**

**R**un – is to immediately evacuate the area

**H**ide – seek a secure place where you can hide and/or deny the shooter access

**F**ight – where your life or the lives of others are at risk, you may make the personal decision to try to attack and incapacitate the shooter to survive

**Window of Life**

**Window of Life is an emergency response method authored by Safe Havens International. It says a person who is in a crisis has four responsibilities:**

1. A person’s first responsibility is for his or her safety. You are an important asset in a crisis, not one to throw away lightly. If you are lost, that loss is felt in successive areas around you, much like the ripples in a pond.

2. A second responsibility is to those in the immediate vicinity, those who are within line-of-sight or ear shot of where you are. Recognizing your importance as an asset involves using that asset to help others.

3. A third responsibility is to those in your place. Having protected yourself and alerted those near you, it is important to alert those who will also be affected by the crisis but may have a bit more time to react.

4. A fourth responsibility is to notify public safety. For more information on Window of Life, listen to Campus Safety’s interview with Mike Dorn called “Should School Teachers, Administrators Attack Active Shooters?” at http://www.campussafetymagazine.com/WindowOfLife

**The 4 As**

**The 4As is a 4 step process to prevent or reduce loss of life in an active shooter event. They stand for:**

1. Accept that an emergency is occurring.

2. Assess what to do next so that you can save as many lives as possible, which depends on your location.

3. Act: Lockdown (lock and barricade the doors, turn off the lights, have patients get on the floor and hide) or evacuate or fight back (last resort).

4. Alert law enforcement and security

►**Read full draft document at source’s URL.**

Door Security System from Smarter Security Helps University Keep Students Safe

Source: http://www.hstoday.us/single-article/door-security-system-from-smarter-security-helps-univer sity-keep-students-safe/0c395dc00b95900ea387180f2df7f4a4.html

Austin, Texas-based Smarter Security, Inc., a provider of premium, innovative entrance control and outdoor security solutions, announced that a university in the Midwest ordered more than fifteen **Door Detective CL** units to help stop unauthorized access through dormitory exit doors.

The company said that “prior experience and success with Fastlane optical turnstiles led to the university trusting Smarter Security with helping to solve this door security challenge as well.”

“It is a high compliment when customers come back and buy different products from a company, and we are pleased to be working with this university again,” said Jeff Brown, CEO of Smarter Security. “University campuses are at greater risk of tailgating and piggybacking than corporate offices because young adults are less likely to confront a tailgater or to follow access rules. Locked doors are wonderful security devices … until they are opened. In Door Detective, universities finally have a solution that helps keep things honest once a door has been opened, which is when the access control system is essentially blind.”

The university ordered seventeen Door Detective CL units from Smarter Security to place on perimeter doors used by students for free egress from several residence halls.

Some students were violating rules and opening these doors for friends to come in, and it was possible for someone to enter a door unnoticed as it was closing.

With Door Detective, students can still exit the doors as before, but any entrance through the door sounds an alarm. The university installed Fastlane optical turnstiles several years ago which greatly improved entry control in dormitory lobbies. Appreciation for Smarter Security’s technology advantages and responsive service and support convinced the customer to stay with the company, and it chose the CL model because of the status lights that provide users feedback.

Door Detective is a tailgate detection system available from Smarter Security that works on an access-controlled door and forces everyone who enters to present authorized credentials, even if the door is held open. In cases such as at this university, where no access control system is in place, Door Detective can be used to stop direction violations.

**In either situation, an alarm sounds when there is a violation, and this can trigger a CCTV camera or another door to lock.** The company offers three models to meet different needs, budgets, and aesthetic preferences.

# New technology predicts upcoming sandstorms in UAE

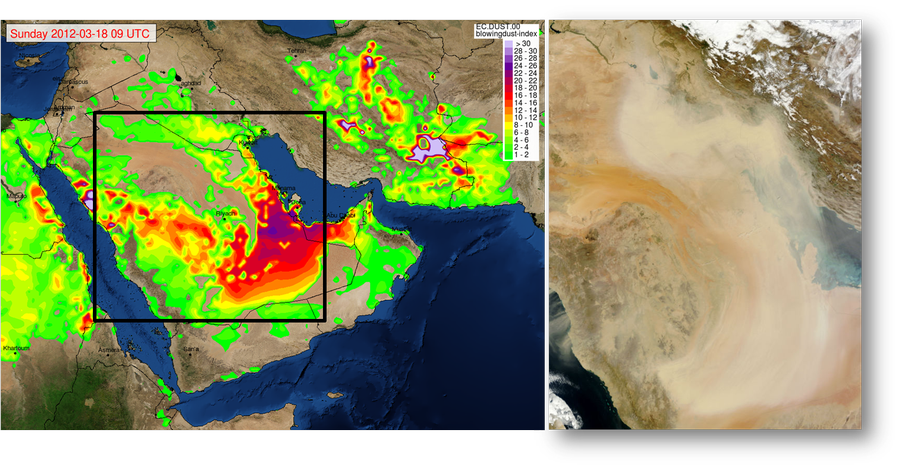
Source: http://www.thenational.ae/uae/environment/new-technology-predicts-upcoming-sandstorms-in-uae

Officials can now predict when a sandstorm will sweep across the country thanks to new technology unveiled in Dubai.

The **Sandstorm Forecasting/Prediction system**, the first of its kind in the UAE, was launched on Sunday (April 20) as part of Gitex Technology Week. It is based on a 3D weather prediction model that uses satellite imagery to forecast storms.

“First results of the dust storm prediction system are very promising and indicate that the system will help prepare the public for dust storm events,” said Eman Al Falasi, head of Dubai Municipality’s Geodesy and Hydrographic Survey section.

The project is a joint venture between the Geodesy and Hydrographic Survey Section of the Dubai Municipality and Unique System FZE, a maritime group company.

The system uses geostationary and orbiting satellites, lidar and aerodrome reports to present real-time satellite images of upcoming dust storms, Ms Al Falasi said.

Previously, Dubai had five coastal stations. **In 2010, eight inland stations, a 3D weather model and 1D fog model were launched. Satellite imagery and remote meteorologist services were added in 2012. New buoys, cameras, rain gauges and sandstorm monitoring systems will be available soon.**

Iraq, Kuwait and Saudi Arabia are significant sources of dust affecting the UAE, according to a Dubai Government news release.

“We are very proud with the results of this project which is useful to the whole nation and for the people living here,” said Eng Mohammed Mashroom, director of the survey department of the municipality.

# Trinity portable wind turbine takes a breezy approach to charging-on-the-go

Source: http://www.gizmag.com/trinity-portable-wind-turbine/31749/?utm\_source=Gizmag+Subscribers &utm\_campaign=141712c3ba-UA-2235360-4&utm\_medium=email&utm\_term=0\_65b67362bd-141712c3ba-90124985

There are already plenty of solar-powered phone chargers out there, but they won't do you much good at night, when it's cloudy, or even if you live too far north. Chances are, however, that in any one of those situations, there will be at least a slight breeze ... and that's where the Trinity portable wind turbine comes into play.

The plastic-bodied Trinity is carried as a 12-inch (30.5-cm) cylinder when not in use. When you want to juice it up, you pull out the turbine's three aluminum legs, and prop it up to catch the wind. The legs can be laid flat to form a pedestal, or partially extended to form a tripod base. And yes, it is waterproof (rated to IPX6), should the wind be accompanied by rain.

As the blades turn, they spin an internal 15-watt generator that in turn charges a 15,000-mAh lithium-polymer battery pack. Using one of two USB ports on the bottom of the unit, you can then plug in your phone (or other device) and charge it. According to Skajaquoda, the Minnesota-based company that's developing the Trinity, one full charge of the battery should allow for four to six phone charges – you can also forgo the battery, and charge your phone directly from the generator.

Skajaquoda hasn't stated how long it takes to fully charge the battery, although it obviously depends very much on wind speed. The company plans on providing that information on its Kickstarter page soon – important information to know, for sure.

That said, if you just want to bring the Trinity along as an extra power source and don't have the time or inclination to set it out in the breeze, you can also just charge it from an outlet via an integrated mini-USB port.

The suggested retail price of the Trinity is US$399, although you can preorder one now for a pledge of $279. Delivery is estimated for January, assuming it reaches production. Should you feel like shopping around, you might also want to check out offerings such as the Orange Wind Charger, the HYmini or the Powertraveller.

# Emergency crews could start getting messages from their jackets

Source: http://www.gizmag.com/wi-fi-firefighter-message-jacket/31748/?utm\_source=Gizmag+Sub scribers&utm\_campaign=141712c3ba-UA-2235360-4&utm\_medium=email&utm\_term=0\_65b67362bd-141712c3ba-90124985

It's important for firefighters or members of disaster response crews to stay in touch with one another during operations, which is of course why they carry two-way radios. Researchers from Norway's SINTEF group, however, are developing a system that could help even more. It allows users to receive and read text messages hands-free, via their jackets.

The prototype jacket, developed in a collaboration with students from the Norwegian University of Science and Technology, has electronics sewn into it, including a narrow LCD screen on the sleeve. **The idea is that all members of a rescue crew will be wearing the jackets, which will be in wireless contact with one another, and with the team leader.**

When that leader sends a message out from their phone or computer, the jackets receive it, and alert the wearers by activating a buzzer in the collar. The users then look down at the screen, where they can read the message as it scrolls across.

While a smartphone could serve the same purpose to a limited extent, firefighters likely wouldn't want to dig out their phone and hold it up every time they received a message. Additionally, particularly in the case of disaster sites, mobile networks might not always be available.

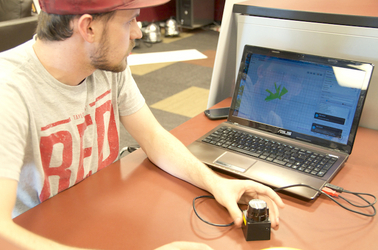
The **SINTEF jacket** instead utilizes a private Wi-Fi Direct system, in which a single message is relayed from jacket to jacket, as long as they're no more than 50 meters (164 ft) apart. The technology was originally developed using web-based social media platforms such as Facebook to share the messages, which could still prove practical for other applications.

**So far, however, it's still not possible for jacket-wearers to respond to messages, or to send them to one another.**

# Robot scouts rooms people can't enter

Source: https://asunews.asu.edu/20140422-robot-room-mapping-project

Firefighters, police officers and military personnel are often required to enter rooms with little information about what dangers might lie behind the door. A group of engineering students at Arizona State University is working on a project that would help alleviate that uncertainty.

 “**We’re creating a room-mapping system that can be used to map rooms in three-dimensional space,”** says Travis Marshall, a student in the College of Technology and Innovation. With guidance from two faculty mentors, Marshall and four other ASU students are working with Sandia National Laboratories to come up with a way to scan a room and produce a 3-D rendering of what’s inside.

**The product they’re building consists of a laser sensor attached to a motor that sweeps all the way around a room, taking 700-800 individual scans, each one with about 680 unique data points.** This information is transmitted to a computer program that creates a picture of the room and all its contents. Whoever is controlling the sensor remotely can see and analyze the data in real-time, as it’s being collected.

“The ultimate goal is for this to be very much separated from the user,” Marshall says. “It could be useful for surveillance, or pretty much anywhere a person couldn’t go, or wouldn’t want to go.”

**The technology offers incredible potential.** A firefighter might be able to avoid entering a room engulfed in flames by mapping it beforehand to determine if there is a need to go inside. A soldier could scan a building and identify potential threats so that he or she is not blindsided.

“Also, if there has been some sort of emergency in a building where rescue workers can’t go inside for fear of it collapsing, this would be a system that could go in and survey damage, possibly survey invisible physical damage to the building’s infrastructure, without people having to go in and risk their lives to do it,” Marshall says.

The students are building the system for Sandia National Laboratories, a U.S. Department of Energy research facility that focuses on security issues. While Sandia has challenged the team to create the most accurate sensor possible, they are also interested in learning about its limitations. For example, the current prototype can’t scan reflective surfaces or see around objects in the room. But these challenges provide helpful insight and are part of the learning process for both parties.

“After we get a blank room mapped, they want us to progressively be able to map more and more complex rooms,” Marshall says. He and his teammates – Matt Bodington, Preston Yeschick, Jeffrey Rojo and Steven Sanchez – are all engineering students who began working together through ASU’s iProjects program. The program matches student groups with industry partners that need help solving real-world challenges.

Each team also benefits from the help of faculty mentors. Angela Sodemann and Tom Sugar are both engineering professors at CTI with experience working on technology similar to what Marshall’s team is developing. They volunteered to be mentors, and have worked closely with the team since the project began.

Sodemann says the students were faced with a unique challenge in that no one was quite sure what the final product would look like.

“This project is pretty open-ended. They don’t have a definite task that they’re trying to accomplish in the end. They kind of have a series of increasingly difficult challenges that they’re trying to meet,” Sodemann says. But that’s what makes the process so valuable. The experience of tackling a problem that’s not clearly defined will prepare the team for their future careers.

“Having to decide for themselves what steps they need to take along the way is good practice for the way that problems really are out there in the real world,” Sodemann says.

For Marshall, who is also using the project to fulfill his senior capstone requirement, the opportunity to work closely, one-on-one with Sugar and Sodemann has been a highlight of the project. He also appreciates the exercise in problem-solving with students from different engineering backgrounds to accomplish a common goal.

“This team has been awesome for getting that experience of working with people that are like-minded, that are interested in the project, that want to do well on it,” Marshall says.

The project will wrap up at the end of the semester, when Marshall and his teammates will present Sandia with the culmination of their work, as well as participate in the Innovation Showcase on the Polytechnic Campus.

****Risk of a Catastrophic Quake, Tsunami in CA Greater than Once Believed

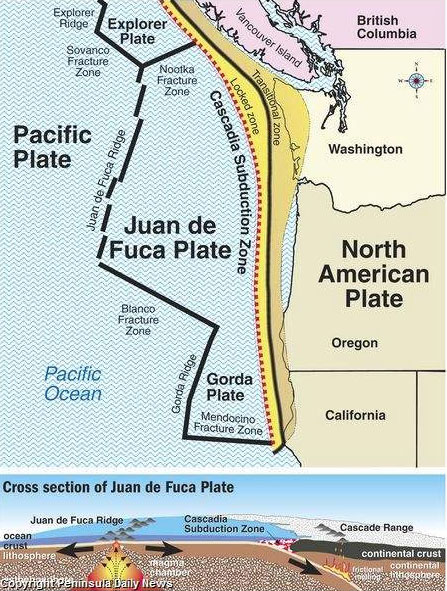
Source: http://www.emergencymgmt.com/disaster/Risk-Catastrophic-Quake-Tsunami-in-CA.html

**If a 9.0 earthquake were to strike along California's sparsely populated North Coast, it would have a catastrophic ripple effect.**

**A giant tsunami created by the quake would wash away coastal towns, destroy U.S. 101 and cause $70 billion in damage over a large swath of the Pacific coast. More than 100 bridges would be lost, power lines toppled and coastal towns isolated. Residents would have as few as 15 minutes notice to flee to higher ground, and as many as 10,000 would perish.**

Scientists last year published this grim scenario for a massive rupture along the Cascadia fault system, which runs 700 miles off shore from Northern California to Vancouver Island.

**The Cascadia subduction zone is less known than the San Andreas fault,** which scientists have long predicted will produce The Big One. But in recent years, scientists have come to believe that the **Cascadia is far more dangerous than originally believed** and have been giving the system more attention.  
The Cascadia begins at a geologically treacherous area where three tectonic plates are pushing against each other. The intersection has produced the two largest earthquakes in California in the last decade -- Sunday's 6.8 temblor off Eureka and a 7.2 quake off Crescent City in 2005. The area has produced six quakes of magnitude 7.0 or greater in the last 100 years, the California Geological Survey said.

Officials in Northern California as well as Oregon and Washington are beginning to address the dangers.

National Oceanic and Atmospheric Administration tsunami researchers are testing a new generation of tsunami detectors off the Oregon coast, which could provide earlier warnings about the incoming wave's size.

During the 2011 Japan tsunami, some of the first detailed alerts underestimated the size of the tsunami to be lower than the sea walls — and then communications were cut off.

"So some people had a false sense of security," said Vasily Titov, director of NOAA's Center for Tsunami Research. "You want to have this information as accurate as possible."

Installing tsunami sensors on the deep ocean floor would provide better information on the tsunami's size in as little as five minutes. It now takes about half an hour.

Titov said two underwater test sensors off the Oregon coast seemed to perform well in Sunday's earthquake, though the quake did not produce a tsunami.

In Grays Harbor County in Washington State, crews will begin building an elementary school gym this summer to double as a "vertical evacuation center" — built so that 1,000 people can flee to the roof during a tsunami, protected by a high wall.

**"We have no natural high ground,"** said Ocosta School District Supt. Paula Akerlund. **"So we have to evacuate vertically."**

Washington state and federal officials have also been discussing building about 50 "tsunami safe havens," such as artificial hills that could hold as many as 800 people.

The 2011 Japan tsunami as well as other natural disasters like Hurricane Katrina have fueled efforts to better prepare for a major quake on the Cascadia fault.

"Katrina was a worst case scenario for hurricanes in the gulf. And a Cascadia would be the worst case scenario for tsunamis on the West Coast," said Paul Whitmore, director of the National Tsunami Warning Center in Alaska.

**For years, scientists believed the largest earthquake the area could produce was magnitude 7.5. But scientists now say the Cascadia was the site of a magnitude 9 earthquake more than 300 years ago.**

Ripping over a fault that stretches in the Pacific Ocean from the coast of Vancouver Island to Cape Mendocino, the quake on the evening of Jan. 26, 1700, was so powerful, entire sections of the Pacific coastline dropped by as much as 5 feet, allowing the ocean to rush in and leave behind dead trees by the shore.

The tsunami reached Japan, destroying homes and rice paddies along the eastern shore.  
In the Pacific Northwest, Native American stories told of "how the prairie became ocean," and how canoes were flung into trees. Whitmore of the National Tsunami Warning Center said similar waves, up to 100 feet above sea level, could again inundate many areas of the U.S. West Coast.

Scientists in the 1980s began piecing together the evidence of the ancient tsunami.

They analyzed the rings of the trees that had suddenly died, and carbon dating narrowed the date of an earthquake to between 1695 to 1720. Then, Japanese researchers pored over ancient records and found a mystery "orphan" tsunami that arrived with no parent earthquake in 1700.

**The Cascadia fault is powerful for two reasons:** It is both extremely long and it is a "megathrust" fault, in which two tectonic plates — slabs of rock roughly the size of New Mexico floating atop the Earth's molten core — are being forced underneath the gigantic North American plate.

As the smaller plates — the Juan de Fuca and Gorda plates — jam underneath the North American plate, friction builds, and the edge of the North American plate is temporarily dragged down as well.

But the North American plate is old and strong, and won't be pulled down forever.

Every several hundred years or so, the North American plate violently snaps back like a rubber band -- thrusting upward with horrific power.

Sunday's quake, which erupted 50 miles off the coast, caused light to moderate shaking. No injuries or damage was reported.

But the North Coast has not always been so lucky.

On April 25, 1992, a magnitude-7.2 earthquake hit on shore near the village of Petrolia — about 30 miles southwest of Eureka — injuring 95 people, and triggering landslides and rockfalls, according to the U.S. Geological Survey.

That quake was so powerful that a 15-mile stretch of beach was pushed up as much as 4 feet — leaving behind rows of dead sea urchins, mussels and sea snails.

The 1992 earthquake pushed Victorian-era homes from foundations and took down chimneys.

An aftershock sparked an electrical fire that engulfed the lone shopping center in the town of Scotia. Firefighters stood by helplessly as a ruptured water main cut off water to the hydrants.

Fires also destroyed the only general store and post office in Petrolia.

**As for the next 9.0 quake, U.S. Geological Survey seismologist David Oppenheimer said: "It could be today. It could be 100 years from now."**

‘Asymmetric’ Helps Define Disaster Resilience

**By Eric Holdeman**

Source: http://www.emergencymgmt.com/disaster/Asymmetric-Define-Disaster-Resilience.html

The word “asymmetric” is most typically associated with “asymmetric terrorism” in today’s emergency management vocabulary. However, I see the word “asymmetric” as being helpful in defining what we mean by disaster resilience.

Resilience is a fairly new word that’s become almost as popular as “paradigm” was years ago. People drop it into their conversations and writings regularly. My day job even has the title “director of regional disaster resilience.” Sounds good, but what does it really mean to obtain disaster resilience and what does resilience look and feel like?

Resilience isn’t easily defined or executed. It’s the combination of many factors and actions by multiple individuals and groups. Typically it’s not the No. 1 priority for any institution or government, yet taken as a whole, the investments in resilience pay huge dividends when disasters do strike.

Resilience has most frequently been used for the disaster recovery phase of emergency management. Well trained and exercised people make better decisions faster, thus speeding up the response and recovery process. Mitigation measures, when implemented before the disaster, can eliminate or minimize damages from natural and technological disasters, thus providing resilience.

Disasters are becoming almost routine from a news perspective. In the last three years, the federal government has spent an average of $85 billion each year. The number of annual billion-dollar disasters is escalating. While severe weather accounts for most disaster costs, there are other human-caused disasters lurking. Consider that one estimate of the physical damage and economic impacts from the 9/11 terrorist attacks is $178 billion.

You can’t pin the disaster resilience responsibility on just one function of society. Responsibility for resilience is also asymmetric. Governments at all levels, the private sector, nonprofits, tribes, neighborhoods, families and individuals all have responsibility for achieving a measure of resilience.

Ever since 9/11, the burden of government funding of preparedness and disaster resilience has shifted to the federal level. While extensive federal grant funding wasn’t supposed to   
supplant state and local funding, you only have to look at the budgets of many states and local communities to see that it has replaced state and local dollars that were there before. Now with the drawdown of federal grants, the pinch in emergency management budgets is being felt severely. From a funding standpoint, disaster resilience will suffer until all parties share the funding burden.

Public-private partnerships are also critical if a community and region are to become truly resilient. The significant concentration of critical infrastructure in the private sector begs us to have closer working relationships and plans. The interdependencies between infrastructures and a functioning economy require us to work more harmoniously and to put aside jurisdictional rivalries to achieve stronger regional collaboration.

While individual deeds are appreciated and single-discipline actions that work to build capabilities enhance resilience, group action that’s multi-jurisdictional and multi-disciplinary becomes a force multiplier when it comes to disaster resilience. To achieve resilience will require “bending” the stovepipes to allow for better coordination and eliminate duplicate efforts.

Lastly, resilience is asymmetric because the path to resilience isn’t predefined. It has many shapes and sizes, all defined by the actions taken, or not taken, by people and institutions as they make their choices in building and designing for the future.

***Eric Holdeman*** *is a contributing writer for Emergency Management magazine and is the former director of the King County, Wash., Office of Emergency Management.*

Building 21st-Century Cities Means Taking the Long View

**By Colin Wood**

Source: http://www.emergencymgmt.com/disaster/Building-21st-Century-Cities.html



Following the devastating tornado in 2007, Greensburg, Kan., seized the opportunity to not just rebuild infrastructure, but improve it, making the city an example for many other communities that have endured similar disasters.

Sustainability is like dieting. It’s not something you do once and then forget about — it’s a lifestyle change. Like a healthy diet, sustainability is also something that’s good for everyone. The environmental movement is rooted in hippie culture of the 1960s and 1970s and still suffers today from an image that confuses some and stratifies adoption along political lines. But in recent years, government leaders have begun to create programs and institute concrete changes that go beyond rhetoric and align not necessarily with any one political interest, but with universally human ones.

Sustainability seems a nebulous concept because it entails so much at once, and to each community it means something slightly different. Leaders in Vietnam found sustainability in learning to live with nature. Dubuque, Iowa, found sustainability in the human capital of its citizenry. And the inhabitants of rural, tornado-ravaged Greensburg, Kan., found that sustainability was the hope they needed to rebuild and not to give up.

The position of chief innovation officer is a recognition by government that IT is no longer peripheral, but an integral tool meant to assist all business needs. That idea is now giving way to new titles. Governments are hiring officers of performance, innovation and sustainability. Technology remains crucial, but leaders are setting their sights on broader goals and taking a more holistic approach.

Pittsburgh is among the cities undergoing such a change. When Mayor Bill Peduto took office in January, he brought in new cabinet members like Chief Innovation and Performance Officer Debra Lam. Though Pittsburgh is still at the earliest stages of sustainable thinking, it’s starting with people who have experience and know what it takes to position a community for a sustainable future.

Working for consulting and design firm Arup, Lam has managed projects and consulted with communities around the world to show them what sustainability means, how it can enhance lives, and help ensure that life will continue to be enjoyable as the environment presents new challenges.

Sustainability is a controversial word, Lam said, but the one thing that most everyone agrees on is that government should continually strive to improve everyone’s quality of life, and that’s what a sustainable approach does.

And sustainability is not just intended to mitigate climate change, Lam said. Even if civilization meets its most ambitious goals, the effects of climate change will continue to manifest in ways that can’t always be anticipated. Sustainability is also about finding ways to be resilient and live alongside the environment. “It’s really understanding what the risks are climate-wise, and then putting up the necessary measurements to be prepared for that,” she said. “We can’t predict and prevent everything. There’s an inherent underlying unpredictability. But that doesn’t mean we can’t be prepared.”

Lam managed a project in Ho Chi Minh City, Vietnam, where leaders sought guidance on how to handle their water management problems. Alongside the Mekong Delta, Ho Chi Minh City has seen centuries of flooding, but today there are new factors to consider. The growing population and rising affluence means a new class of people will draw more resources, depleting groundwater supplies and increasing soil salinity. Furthermore, climate change and rising sea levels are expected to cause even more soil salinity, not to mention flooding. Some researchers predict that many provinces in the delta region will be flooded as soon as 2030.

After studying the area, Arup issued a report to Ho Chi Minh City that recommended the city work to reduce water leakage and theft, and adopt more effective irrigation methods. The company also recommended infrastructure upgrades to improve water logistics, and encouraged leaders to think about how their infrastructure will need to adapt as conditions in the environment change. Getting all the stakeholders talking with one another, Lam explained, was key to making the other recommendations attainable.  
When faced with a specific problem like flooding in Vietnam, the prevailing pragmatic mentality can fall short, Lam said. Typical solutions proposed are walls, ducts or dams. “That only goes so far,” Lam said. “It’s very costly, it’s very resource-intensive, very time-intensive, and it’s not necessarily the most effective way. If you’re assuming a sea level rise of 5 feet, but then sea level rise comes to 6 feet, it’s not going to work.”

Instead, she said, they should be looking at solutions that let the water in, and use green architecture and infrastructure to filter and absorb it. That’s sustainability. “It’s the realization that man can’t just block out or control nature,” Lam said. “There are a lot of good things working with nature.”

After Hurricane Katrina damaged or destroyed more than 200,000 New Orleans homes in 2005, people began rebuilding, although they understood that a similar situation could and probably would happen again. Sustainable architecture has become important in the region, but the concept is far from perfected. While the enthusiasm is there, sufficient knowledge and competent project management doesn’t necessarily follow. Dozens of homes built by actor Brad Pitt’s award-winning charity, the Make It Right Foundation, began rotting soon after construction in 2007 because of faulty wood products. Cities interested in sustainability need competent role models and reliable information.

Dubuque, Iowa, is a city that people look to when they want things done right. For sustainability initiatives to be impactful, they need grass-roots support from the people and leadership from government, said Cori Burbach, sustainability community coordinator for the city.

Dubuque has received awards and acclaim for its sustainability initiatives, including Smarter Sustainable Dubuque, a private-public research partnership with the IBM Watson Research Center. The city’s work is viewed as a model of sustainability for similarly sized local governments.

Dubuque partnered with private utility companies to help educate the public and boost energy conservation. The city encourages businesses to go green, while also searching for ways to spur local economic growth. In 2012, Dubuque was identified by the Martin Prosperity Institute as having the fourth largest average annual salary increase in the nation among metropolitan regions. Much of the region’s economic growth is thought to come from programs like Green and Healthy Homes, savings gained by smart metering and the use of data analytics to optimize the city’s bus schedule.

You can’t become sustainable by directive, Burbach said. Success requires support from the people and guidance from the top down, both of which Dubuque has had. Stakeholders in the community decided together to make sustainability a priority, and that sort of cooperation is crucial to make such initiatives work.

“That’s not just because there are more hands at the table, but because we’re all sharing data,” Burbach explained. “So often, even the way we collect data is siloed, and so we’re not getting the whole picture. We’re looking at, for instance, literacy scores, not understanding how family, economic status, health, activity, or access to services impacts those literacy scores.” Being a sustainable city means considering data on a communitywide basis so that decisions are based on all the available information, she said. “It’s really addressing the needs that are unique to Dubuque in a very coordinated, collaborative way.”

When people hear “sustainability,” they think it only means environmentalism, but that’s not the case, Burbach said — sustainability is environmental integrity, economic prosperity, and social and cultural vibrancy. It’s hard to make a business case for sustainability if all the plan consists of is changing a few light bulbs or installing a solar panel. When people realize that it’s about making communities resilient on all levels and building toward a better future, they start to see the value in it.

Through initiatives like Bridges Out of Poverty and Circles, community leaders in Dubuque are looking to forge a sustainable populace. Rather than just giving people money to pay the rent, the city wants to empower families and reduce dependence on the government, because everyone in society has something to contribute.

“It’s recognizing those assets in those families that have come out of our programs and connecting them to nonprofits, church groups or neighborhood associations so they can then be engaged in the community as well,” she said. “When you look at what our communities are going through in terms of changing economies, in terms of a changing federal funding world, all of the things that are impacting communities, I think it’s challenging us to think differently about the way we provide services. Sustainability, to me, gives us the framework to analyze what’s truly a priority and then to revise those services.”  
On the evening of May 4, 2007, a tornado nearly two miles wide brushed through the small rural city of Greensburg, Kan. The tornado was later rated an EF5, the most powerful tornado on the scale, with wind speeds up to 240 mph. The tornado killed 13 people, hurt another 60 and leveled the city, destroying 95 percent of the buildings. Immediately, about half of the city’s 1,500 residents relocated, and the rest stood by, not sure what to do next.

The city was declared a disaster area, and the Federal Emergency Management Agency (FEMA) stepped in with food, water, shelter and supplies. FEMA and design firm BNIM also helped the city create a plan to rebuild. Eight months later, the Greensburg City Council adopted a resolution committing it to sustainability. **All buildings larger than 4,000 square feet were to meet LEED-platinum standards, and all energy was to come from renewable sources.**

Over the next four years, the city rebuilt. It built a new courthouse, school, medical center, arts building, city hall and energy-efficient homes. It built wind and solar farms, and geo-thermal wells. Many thought the tornado was going to be the end of Greensburg, but today the city is revered as a living laboratory of advanced building materials and sustainable living. Other cities hit with tornadoes visit Greensburg to attend peer-to-peer workshops to learn how to rebuild and how not to despair.

Starting from scratch allowed Greensburg an opportunity to build things right, and fix some of the problems it had before, Mayor Bob Dixson said. “We were able to consolidate school buildings all on one campus instead of several centers all across town,” he said. “That maximized resources available and allowed us to have a lot more shared spaces.”

At first, the remaining population of Greensburg was not sold on the idea of sustainability, Dixson said, but they’ve since come around. People now see that the “crunchy” connotation of the word is just a distraction from the value it truly represents. “For us here on the high plains of the western Kansas rural area, it’s about those conservation values that our parents and grandparents and past generations taught us — to just take care of what you’ve got. If you take care of the land, it will take care of you.”

In April and May of 2011, a string of tornadoes passed through the Midwest and the South, killing about 500 people and causing billions in damages. Community leaders from Alabama, Mississippi, Missouri and others came to Greensburg to learn from people who had already been there.

“The one thing we shared with other communities is: Don’t make life decisions rapidly, because you’re in a very emotional state of mind anyway. Not only are you trying to rebuild your homes, and your lives, you’re trying to rebuild a city. So take time to make sure you think through the processes and involve the community and you get a whole lot better results,” Dixson said. “The other thing that is highly critical, especially in rural communities, and it is true in major metropolitan areas, too, is that in order to be long-term sustainable as a community, you have to have a vibrant economy.”

Sustainability means a holistic approach, Dixson said. Each community’s specific goals and industries will vary, but when it’s time to plan, he said, communities should look carefully at their resources and decide how they’re going to rebuild not just their structures, but their economy and their lives. “The economic infrastructure can’t take a back seat,” he said. “It all has to come together.”

“Sustainability to me means have we learned from our past? Our heritage and our ancestors taught us how to survive and how to thrive,” Dixson said, adding that communities should take advantage of today’s technologies and advanced materials to build on that foundation. “Each one of us is just trying to make our communities a better place for us to live and work. And if you’re really striving for that, then you’re a true sustainable community.”

***Colin Wood*** *is a Seattle-based writer who covers various technology topics.*

## Bangladesh tops list of countries at risk from sea level rise

Source: http://www.homelandsecuritynewswire.com/dr20140407-bangladesh-tops-list-of-countries-at-risk-from-sea-level-rise

Scientists say that see levels may rise by up to the feet by 2100.The implications of this would have drastic consequences for nearly all coastal nations, but the consensus is that Bangladesh will be the hardest hit by the change. Leading Bangladeshis say that since Bangladesh produces less than 0.3 percent of the emissions driving climate change, it would unjust for Bangladesh to rely on its own meager resources to solve this problem. **One solution they offer: fifty million Bangladeshis (out of a population of 163 million) should be allowed to move to and resettle in the countries which produce the bulk of greenhouse gasses.**

Many of the world’s top scientists met in Yokohama, Japan last week to discuss the prediction that sea levels around the world could rise three feet by 2100. The implications of this would have drastic consequences for nearly all coastal nations, but the consensus is largely that Bangladesh will be the hardest hit by the change.

**Coastal Bangladeshis, especially those within the Ganges Delta, live in such dire circumstances that they often face difficulty growing vegetables and maintaining drinking water due to salt water influx from flooding, and are forced to subsist in sub-quality housing on muddy, treeless plains.**

As theNew York Times reports, that country has already been racked by the combination of heavy storms and poor infrastructure, with millions of citizens living in zones that could be seriously affected by the slightest sea level rise.

Rafael Reuveny, a professor at the School of Public and Environmental Affairs at Indiana University at Bloomington, told the paper, “There are a lot places in the world at risk from rising sea levels, but Bangladesh is at the top of everybody’s list…And the world is not ready to cope with the problems.”

**Despite the threat to Bangladesh, the country only produces “0.3 percent of the emissions driving climate change” — leading to the idea that the problems facing the country are also becoming an issue of justice.**

Atiq Rahman, executive director of the Bangladesh Center for Advance Studies, said, “These migrants should have the right to move to countries from which all these greenhouse gases are coming. Millions should be able to go to the United States.”

More importantly, as Tariq A. Karim, the Bangladeshi ambassador to India, warns, “We need a regional, and, better yet, a global solution. And if we don’t get one soon, the Bangladeshi people will soon become the world’s problem, because we will not be able to keep them.”

**Karim estimates that up to fifty million Bangladeshis would be forced to exit the country by 2050 if sea rise predictions turn out to be true.**

# Climate change report outlines threats to UAE’s coastline

Source: http://www.thenational.ae/uae/environment/climate-change-report-outlines-threats-to-uaes-coastline

Environment experts say they have made provisions for the possible harm that climate change could cause to the coastline.

**The Intergovernmental Panel on Climate Change said last week global warming could pose risks to marine habitats such as mangrove swamps and coral reefs in the UAE and the wider Arabian Gulf.**

Dr Thabit Al Abdessalaam, a senior adviser on biodiversiy at the Environment Agency Abu Dhabi, said that rather than presenting new information the panel’s warning had reinforced the significance of climate change.

“It also emphasises the need for joint and concerted efforts to address and implement priorities aimed at mitigating climate change and adapting to its impacts,” he said.

“The Government is cognisant of the potential of climate change to pose serious adverse impacts on Abu Dhabi emirate and the UAE’s environment, its people and their safety and livelihood.

“The development of joint plans at the emirate of Abu Dhabi and federal levels, which are striving to take into account local, regional and international drivers and agreements, is a testimony to the government’s understanding of the significance of the matter and the need to ensure that climate change issues are addressed as a matter of national priority.”

The environment agency has made climate change a high priority in its five-year strategic plan, he said. Last year the agency established a greenhouse gas inventory for Abu Dhabi and it is undertaking studies into the possibility for the emirate’s ecosystems and sensitive land areas to adapt to changes in climate.

“Climate change mitigation requires broad cross-sector coordination instead of isolated interventions of individual organisations. As the leading public agency for protecting and conserving the environment in Abu Dhabi, EAD has a key role to play in managing a concerted response to mitigate climate change at the local level through a combination of supply and demand side management initiatives,” he said.

The latest report from the intergovernmental panel details the current and future impact of climate change on different global regions.

**Coastal and marine eco-systems in Asia are already under pressure from different factors and the stress is likely to increase as the amount of heat-trapping greenhouse gases in the atmosphere increases.**

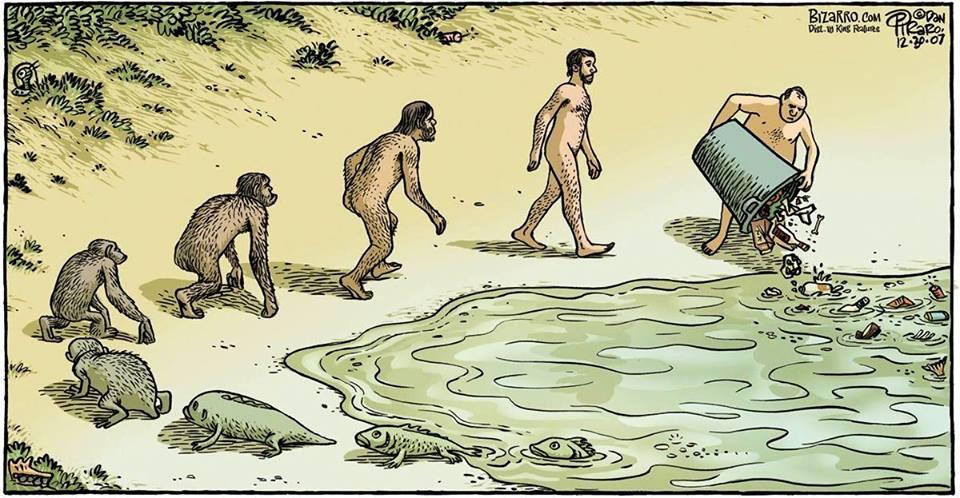
“Mangroves, salt marshes and seagrass beds may decline unless they can move inland, while coastal freshwater swamps and marshes will be vulnerable to saltwater intrusion with rising sea-levels,” said the report.

“Widespread damage to coral reefs correlated with episodes of high sea-surface temperature has been reported in recent decades and there is high confidence that damage to reefs will increase during the 21st century as a result of both warming and ocean acidification.”

Besides warning over warmer subtropical and tropical waters that will likely be less rich in terms of biodiversity, the report is also urging for more studies into how climate change will affect rain patterns and the availability of water in many parts of Asia.

“Improved projections for precipitation, and thus water supply, are most urgently needed,” it said. “Another priority is developing water management strategies for adaptation to changes in demand and supply.”

Another area where knowledge is lacking is in understanding the effects of climate change on biodiversity. In many countries in the region, scientific baseline information is either lacking or limited, the report warned.



# http://r70.cooltext.com/rendered/cooltext1333431858.png

# U.S. corporations aware of current, future water risks

Source: http://www.homelandsecuritynewswire.com/dr20140402-u-s-corporations-aware-of-current-future-water-risks

A new survey of major U.S. corporations released yesterday (Apr 1) by the Pacific Institute and VOX Global, titled **Bridging Concern with Action: Are US Companies Prepared for Looming Water Challenges?**, reveals that most companies believe water challenges will significantly worsen in the next five years. The majority of companies surveyed, however, do not appear to be planning corollary increases in the breadth and scale of their water risk management practices. In fact, nearly 70 percent of responding companies said their current level of investment in water management is sufficient.

A Pacific Institute release reports that in an attempt to gain insight on corporate perceptions of risks associated with water issues and plans to address these challenges, the Institute and VOX Global surveyed over fifty companies, the majority Fortune 500 and publically traded, representing virtually every industry sector. In addition to an online survey, in-depth interviews were conducted with senior officials who have direct responsibility for water issues from companies including: AT&T, Cummins, Inc., The Hershey Company, MillerCoors, and Union Pacific Railroad.

**Nearly 60 percent of responding companies indicated that water is poised negatively to affect business growth and profitability within five years, while more than 80 percent said it will affect their decision on where to locate facilities. This is a stark increase from only five years ago, when water issues affected business growth and profitability for less than 20 percent of responding companies.**

“Water challenges are not just for developing countries; they are happening here in the United States,” said Jason Morrison, program director of the Pacific Institute. “While the current California drought gets considerable attention, many regions face a chronic imbalance between water supply and demand.”

The acknowledgement among major U.S. corporations that water is becoming major business issue is a significant finding. There is growing recognition that in addition to being a considerable societal problem, water also creates critical challenges for businesses specifically. Insufficient or contaminated water supply, or a lack of infrastructure to reliably deliver that supply, can mean companies may not be able to maintain the volume and quality of their production.

“As more and more corporate boards discuss the impact of social and environmental issues on their profitability and growth, topics such as water risk will emerge as central to company strategy,” said Tony Calandro, senior partner and leader of the VOX Corporate Sustainability and Social Responsibility Practice Group. “This new economic reality necessitates that companies better understand the many ways that water affects their reputation and bottom line and the multitude of communication and management strategies they may need to adequately address these business challenges.”

**While survey respondents indicated that water challenges are worsening and will affect their business more significantly in years to come, most did not indicate any plans to expand their water risk mitigation measures in the future.** “It is for this reason that we question whether many companies are adequately prepared for the growing number of water risks and challenges they face,” Morrison said.

Calandro noted that internal obstacles are often to blame for slow action. “Business leaders we surveyed pointed to two significant internal obstacles that hinder companywide buy-in to water: lack of time to raise awareness and buy-in and other risks ranking as a higher, more immediate priority.”

The study found that companies use a variety of ways to build internal support in order to fully understand the impact water has throughout the business. “Since we were not necessarily seeing water stress or scarcity issues within our primary manufacturing footprint, we didn’t have the focus that was expected of the food processing industry sector,” said Todd Camp, senior director, Corporate Social Responsibility & Community Relations for The Hershey Company. “Participation in the reporting initiatives and an evaluation of our peer group’s efforts provided the incentive to be proactive.”

Additionally, some companies find that relatively small investments can produce a significant return on investment in mitigating water risks.  John Schulz, assistant vice president, Sustainability Operations, AT&T, said, **“We’re beginning to see that relatively small capital investments can bring about nearly ten times the amount of savings in annual water and energy costs.”**

*— Reading more in Bridging Concern with Action: Are U.S. Companies Prepared for Looming Water Challenges? (Pacific Institute, April 2014)*

### Work Area Recovery: WAR – What is it Good for?

Source: http://blueyedbc.blogspot.gr/2014/04/work-area-recovery-war-what-is-it-good.html

I was sitting in the office the other week when all of a sudden a deafeningly high-pitch fire alarm started ringing in my ear and it continued to ring out for much longer than the usual 30 second-test. Is this a drill?  
As I look to my colleagues for a response, the teams around me began to stand up from their desks and without question form a steady line out through the fire escape. A majority of these people had clearly done this before as they calmly migrate their way to allocated rendezvous points and without a single hint of panic. I suppose in the absence of a raging inferno or a sudden onset of thick smoke, they think it’s safe to assume a colleague has foolishly burnt their toast or something. Anyway, as I’m stood in the distant car park awaiting my queue to get back to work, I can’t help but wonder how relaxed we actually might be if the bell continued to ring, the flames started to rise and we lost the entire building…and what then? Ultimately, with everyone safe and well, the show really must go on. We all have clients to serve and we need to get back to work as soon as possible. I’m fairly certain you won’t be able to meet any Service Level Agreements (SLAs) or a Key Performance Indicators (KPIs) from the car park!

Historically, all types continuity plans (in whatever shape or design you create them) will typically identify a relocation strategy to another building or premises if something like the above should ever occur. In my experience, the cost effective options are usually deployed first:

**1)** Send home the other non-critical staff and services from office space you might have from another location and use that space short-term to relocate.

**2)** Set up a mutual agreement with a neighbouring organisation perhaps with shared interests i.e. you can use their space and they can use yours when things get bad.

In the private sector today, many organisations now take advantage of a more sophisticated solution (at cost) which is commonly known as a **Work Area Recovery (WAR)**. From what I can see, this is becoming a rapid growth area as organisations reach agreements with dedicated providers of alternative space and technology.

I recently worked with a small project team to develop one of these WAR site solutions and was heavily involved in how it might actually work in reality with operations. As a junior professional in this industry it was completely new territory for me and so true to form I’ve decided to share my experience.

**Disclaimer:** There are stacks and stacks of information leaflets on the basics of WAR sites so I won’t bore you with too many specifics. Also, I’m sure there are people who will quickly try to point out my inaccuracies but I am viewing this from a first time approach and I’m certain I won’t be the only one with these views. If you want some wider more useful detail on this I would recommend Mr Paul Kirvan online posts.

**Overcomplicated Complacency**

I recently spoke to a colleague who confidently suggested to me that setting up and invoking an alternative workspace is a relatively simple process. I really couldn’t disagree more having spent a number of months working on a solution for a number sites in multiple countries.

As with every industry, there are those who needlessly over-complicate the process and those who over simplify (such as Sales Teams from WAR site Providers in my opinion). So the rest of this post will give you what I’ve learned in the last few months.

**Basic Jargon-Busting**

In my very first planning meeting I was surprised by the sheer range of terminology being used even on the basic stuff. Here are a few examples:

**Cold Site:**

This is basically an open space you’ve secured (usually an empty office floor or building). It usually has no equipment or furniture installed. But if you needed to you could urgently kit it out and move staff in but as you will appreciate will take some time to do this.

**Hot Site:**

This is the term used to describe alternative premises that are set up and ready to go with all the access, data, facilities, software and hardware to carry on working as if you’ve always worked there. As you can imagine having a completely mirrored site just sat there is the most expensive solution.

**Warm Site:** After the last two descriptions, it doesn’t take a rocket scientist to figure out what this term means. Essentially it is a happy medium between a cold and hot site. You have the space; hardware and connectivity installed, ready to go but things like back-up data might not be instantly available involving a short delay in readiness.

**Desk:** I have to admit this one confused me briefly because when you discuss “desks” in this context, it also appears to mean desk, drawers, telephone, monitor, hard drive, chair etc. No one told me this for quite a while.  
  
**Syndicated Desks:** This is where basically you hire a space that is shared between clients (presumably at a reduced cost) on the assumption that not all of you will need it at the same time. Nevertheless the process appears to work on a first come first serve basis meaning if an incident affects a wide area and the other business gets there first you miss out.

**Dedicated Desks:** This is where all the kit is exclusively yours to use and is sat there waiting for you. Naturally you pay a premium for exclusivity.

**Thin Client:** For me this was temporarily confusing. Clients are basically PCs that employees will use when they arrive at the alternative site. A thin client doesn’t have all the stand-alone technology to work without the applications being piped through from the main server. It is essentially a portal working off the server from what I can tell.

  
**Rich Client:** This is where the PC that has some applications/software installed locally but also depends on other resources distributed over the network from the server. For us this is typically when some departments rely on unique or specific software that other departments don’t need.

The above terms are just the initial ones that what I would consider to be the basics you encounter first. If you’re non-tech like me you will probably find that as you delve deeper in to the physical and technological arrangements of a full relocation it can sometimes feel like the IT crowd are talking a different language. Terms such as “DHCP Server”, “ACD Switch” and “LAN” that you don’t typically use every day start to rear their ugly head. Also, IT Departments tend to fall in to the habit of using lots of acronyms. In fact during a recent meeting there were so many I actually stopped to ask the technical architect what one of these acronyms meant to which the highly experienced individual replied “ I don’t know what it fully spells out but I know what it does”…My point being try not to be scared off by the black magic that is IT as they don’t appear to fully know either.

**It’s not just a Lift and Shift**

I have recently spoken to a number of professionals about the concept of Work Area Recovery and generally speaking there are quite a few that claim to not only know a lot about it (even as a non-tech professional) but also suggest the process is particularly easy. It’s almost as if they assume you simply move to another site and plug in but it really doesn’t work like that. In fact, it never works like that so if someone tries to pull the same ego-based stunt on you then don’t believe it. This is a project of significant size and don’t underestimate it.

**Resources Requirement Overdrive**

As part of planning arrangements for a potential relocation, managers are asked to state their resource requirements. However, in my experience, this is basically where operational managers will tell you they need every desk and every pc available with every possible software package ever installed and if they don’t get it then it will surely result in a major business catastrophe!! I exaggerate of course but that’s the sort of impression I got when arranging ours. Although, this is a very typical response to get in business continuity anyway so it will come as no surprise to my people in the industry. It’s a real balancing act between making a realistic assessment of genuine business resource requirements against the hefty demands from a panic-stricken department manager.

**The Bigger they are the harder they failover**

A larger organisation will often have multiple sites across a number of locations and sometimes being supported by different servers. If you do have to move to another site, the work required to make it happen urgently from both a physical and technological perspective is relative to the size of the business. One WAR site provider once told me that the bigger organisation, the more complex the move is as you would rightly expect. Try not to compare the apparently seamless transition of a small single-site business to an alternative site when planning yours. I gather it’s a great deal easier.

**Practice Makes Perfect**

The amount of tests and rehearsals involved can also be a bit misleading. If you decided to sign up to a WAR site agreement you will typically think that maybe 1 or 2 practice events should nail it but it can be more complicated than that. These are the things I personally think you need to prepare:

**1)** Engage with BAU staff. There is a difference between the tech guys designing the technical solution for the move to those who will help the staff move on the day and this sometimes gets overlooked. Try to maintain a high level of engagement with the onsite desktop support engineers. Agree on and test a process with the BAU resources before you even touch the wider operations. It’s all well and good having a solution but once the technical architects finish their work and move on you will be left with a solution and no one to support it. Operational staff won’t know how to troubleshoot anything technical.

**2)** Gain permission to access your own network in advance of any connectivity testing from your internal change management board or whatever red tape exists in your organisation to slow the process down – ahem I mean ensure the process if safe and low-risk.

**3)** Try to pre-train or brief key staff who can confidently support an office move at a service level. This could include taking them across to the site so they can familiarise themselves with the facilities, where to park, fire exits, room layout, desk space etc. It’s really valuable to have a few people who are visibly more calm and familiar with the surroundings.

**4)** The pre-planning and assessments need to be thorough. It’s not just about the IT but also the other supplementary equipment including stationary and any other specialist equipment. You also need to think about the simple logistics like transport of staff from fixed points, refreshments and lunch facilities. It’s amazing how quickly you can forget the basics when you get lost in the tech detail.

For those not in the industry or even those that consider this as a simple task, all I will say is…Did you honestly think it was that simple to urgently move a business from one location to another? It takes serious planning.

For those just generally interested in what happens if your fire alarm continues to ring and you end up losing your building, at least you now you have an idea of what might happen behind the scenes to get you off the Car Park and back to work.

|  |
| --- |
| EDITOR’S COMMENT: I liked this article because it is realistic and simple – the two basic qualities that each planner should pocess. But in real life things are a bit different. Take for example CBRN drills: usually they end-up at the hospital’s gate or inside the ambulances assuming that good doctors know what to do if the ambulance with contaminated victims arrives at the ED entrance. How wrong they are! Same with fire drills – participated in a few of them during my active duty years: you follow the plan, you evacuate in an organized manner but you never take your “emergency box” with you. Once upon a time in a major NATO table-top exercise high rank officers were asked to remove their glasses and use their second pair. Almost none had a second pair of glasses with him and so they were not able to read the screens or documents during a supposed high emergency situation. Those who have visited Newsletter’s website you will notice a link named “666-kit”. It contains some basic CBRN documents that you must print and store (your own “emergency box”) in case there is no electricity, no computers, no Internet, nothing! I always kept my own box aside – unless you can remember everything by heart! |

