January 2016

CBRNE NEWSLETTERTERRORISM

E-Journal for CBRNE & CT First Responders

Sex Terrorism

PART B

Europe's Shame

Failing to Protect its Female Citizens

www.cbrne-terrorism-newsletter.com

North Korea has secured 88 pounds of plutonium

Source: http://www.upi.com/Top_News/World-News/2015/12/25/North-Korea-has-secured-88-pounds-of-plutonium-Seoul-official-says/6001451022429/

Dec 25 – **South Korea's Defense Ministry said North Korea is capable of producing a nuclear weapon, using less than 13 pounds of plutonium.**

A government official in Seoul who spoke to South Korea press on the condition of anonymity said North Korea has secured 88 pounds of plutonium, and capable of producing one weapon of mass destruction, South Korean outlet Newsis reported Friday, local time.

Yonhap reported a minimum of 13 pounds of plutonium is required to manufacture a nuclear weapon, and North Korea can manufacture 6-7 weapons.

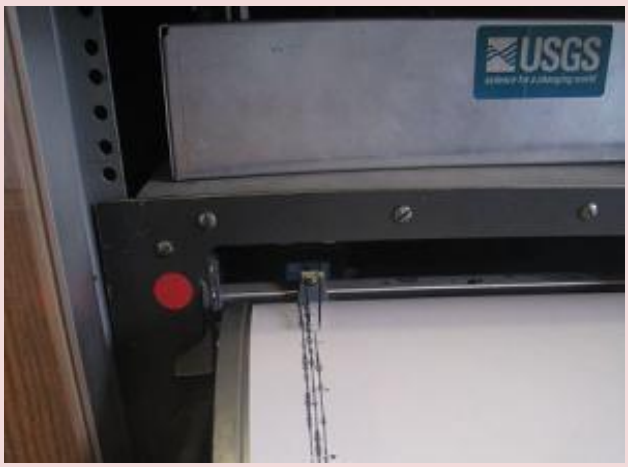
In August, North Korea reportedly restarted its Yongbyon Reactor 2 to resume plutonium production, South Korea press reported. In early 2013, Pyongyang had already begun building light water reactors at Yongbyon.

North Korea's nuclear arsenal continues to grow, even as the country has come under attack from the international community for its weapons program. **The Institute for Science and International Security issued a report in October stating Pyongyang has enough nuclear material to build 22 nuclear weapons, and more specifically, between 66 and 88 pounds of separated plutonium in late 2014.**

The report had stated activities captured in commercial satellite imagery at the Yongbyon nuclear site indicated spent fuel has been removed for chemical processing, and the fuel could have been used for nuclear tests. North Korea could produce weapons from plutonium or weapons-grade uranium, the report said, and could make a median of 22 nuclear weapons, but more information is needed on the size of North Korea's centrifuge program.

Forensic seismology tested on 2006 munitions depot explosion in Baghdad

Source: http://www.homelandsecuritynewswire.com/dr20151228-forensic-seismology-tested-on-2006-munitions-depot-explosion-in-baghdad



Dec 28 – On 10 October 2006, a mortar round hit the ammunition supply depot at the U.S. Forward Operating Base Falcon south of Baghdad. The round started a smoldering fire punctuated by whizzing skyrockets, a rain of incandescent fragments, and massive explosions that bloomed into mushroom clouds. Soldiers who videotaped the “cook-off” can be heard wondering what exactly was in the dump and how much longer the explosions would continue.

But the soldiers were not the only ones recording the cook-off: a

seismometer just four miles away was also registering every boom and shock. The seismometer was one of ten installed in 2005 and 2006 in northern and northeastern Iraq to study the seismic properties of the Earth's crust in that area so that it would be possible to quantify the yield of nearby earthquakes or nuclear tests.

The principal investigator on the team that deployed the seismometers was Ghassan I. Aleqabi, a seismic deployment coordinator in the Department of Earth and Planetary Sciences in Arts & Sciences at Washington University in St. Louis. Iraqi in origin, Aleqabi had obtained his Ph.D. in seismology at Saint Louis University and settled in Saint Louis.

WUSTL reports that installing and maintaining instruments in war-torn Iraq was sometimes a hair-raising business. Installation of the seismometer that recorded the cook-off had to be delayed until April 2006 because it was dangerous even to enter the city. And, once deployed, the seismometers, which recorded 100 samples per second, filled their hard drives in a few months, so someone had to return to the sites to bring out the data.

Then the ammunition dump went up. Aleqabi and his colleague Michael Wysession, professor of earth and planetary sciences in Arts & Sciences, were curious and decided to see if the seismometer had recorded the cook-off. "Sure enough, you could see a whole sequence of explosions," Wysession said.

They report what they found online in the 22 December issue of the *Bulletin of the Seismological Society of America*. "It was an accident that we got such a rich recording," Wysession said. "But sometimes science works that way; you get lucky."

Shock and awe

Analyzing the record in various ways, they found that some types of weapons jumped right out at them. "Mortar fire has a very specific signature that is always the same," Wysession said. "If you make a spectrogram, which breaks out the signal into different frequencies, you see that the firing of the mortar produces one set of frequencies and the case splintering around the explosive produces another. When you see those signals you know that's a mortar firing. You can begin to pick out what's going on."

Passing helicopters produced lovely swooping S-curves in the seismograms as they moved toward and away from the seismometer and their dominant frequency dropped (the same effect that makes the siren on an emergency vehicle drop in pitch). "You can look at how much the frequency drops and over what length of time and determine how far away the helicopter is, and how fast it's going, which is really fascinating," Wysession said.

But they also discovered some limitations. It was not possible to read every little rumble and report. The seismometer, for example, picked up two different car bombs, but their seismic records looked very different. By checking with counterterrorism intelligence sources, Aleqabi learned more about the bombs. One had detonated in a fairly open space at a university and the other had gone up at a checkpoint in a narrow street lined with tall buildings. The checkpoint explosion reverberated in the small spaces, creating a more complex sound pattern that made it harder to figure out the explosive type and yield.

But looking at the seismic recording before and during the cook-off, the seismologists could reconstruct the sequence of events that led to the catastrophe. About 7:22 local time they could see the signatures of mortar fire in the record. At 7:31, a helicopter flew by. An explosion at 7:36 was the one that probably ignited the cook-off, but it was followed by a series of small explosions that gave the soldiers on the base time to take cover. Then, at 7:40, there was a huge explosion and all hell broke loose.

Seismic sleuthing

Seismometers were developed to record earthquakes, Wysession said, but then they turned out to be useful for monitoring nuclear tests, and now people are using them in all kinds of creative ways. "We can independently verify with seismometers the occurrence of global warming because we can track the decadal increase in the storm intensity globally," he said.

Seismology is also used as a forensic tool, he said, to help investigative agencies and insurance companies piece together what happened during terrorist attacks or industrial accidents. One of the leaders in this field is Keith Koper, a Washington University alumnus who is now a professor of seismology at the University of Utah.

Unfortunately, given recent terrorist attacks in Paris and elsewhere around

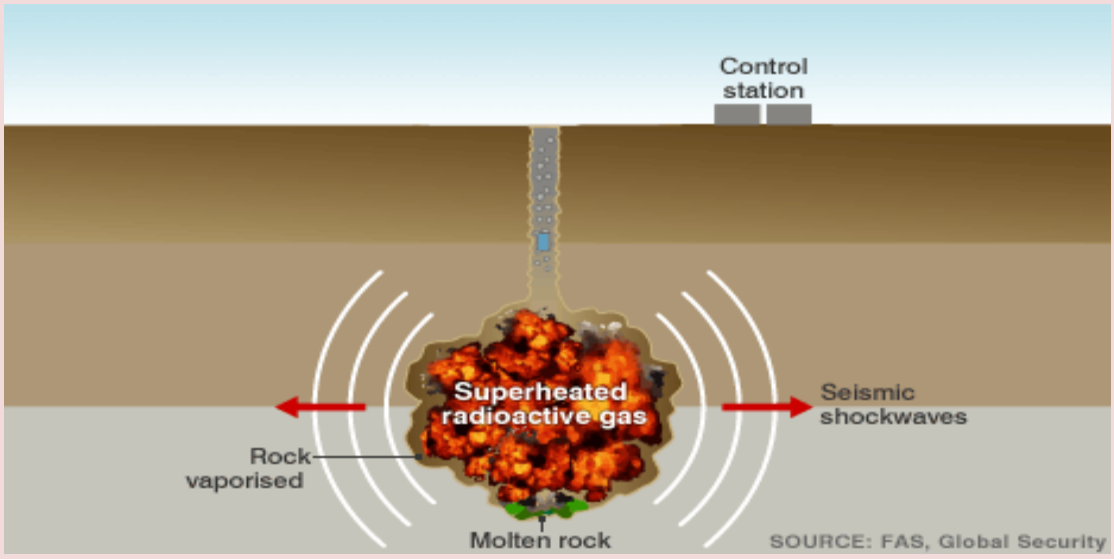
the world, this paper may be timelier than the authors ever expected it to be, Wysession said. "A network of seismometers in an urban area could tell you a lot about a terror attack." A real time-array, he points out, might have prevented the ammo "cook-off." Because the "cook-off" was preceded by a volley of mortar fire — and mortar firings have a unique seismic signature — it might have been possible to pinpoint the source of the rounds before the round that destroyed the ammo depot was fired.

"I think we'll hear more about forensic seismology as time goes on," Wysession said.

— Read more in Ghassan I. Aleqabi et al., "Characterization of Seismic Sources from Military Operations on Urban Terrain (MOUT): Examples from Baghdad," Bulletin of the Seismological Society of America (forthcoming, December 2015).

Pairing seismic data, radionuclide fluid-flow models to detect underground nuclear tests

Source: http://www.homelandsecuritynewswire.com/dr20151228-pairing-seismic-data-radionuclide-fluidflow-models-to-detect-underground-nuclear-tests



Dec 28 – Scientists at Los Alamos National Laboratory have developed a new, more thorough method for detecting underground nuclear explosions (UNEs) by coupling two fundamental elements — seismic models with gas-flow models — to create a more complete picture of how an explosion's evidence (radionuclide gases) seep to the surface. Their findings appear in the journal *Nature's Scientific Reports*.

"The research is novel because it represents an integrated science approach," said Dale Anderson, the project lead and co-author of the paper. "Our field has never integrated seismology and the seismic processes that create fracture pathways with our nuclear-waste-remediation experts that know how radionuclides get through to the rock. You can't do gas seepage unless you understand the pipes and the size of the pipes that go to the surface of the earth. The solution to the problem could not have been advanced without the significant integration of these two sciences."

On September 19th 1957, the United States detonated a 1.7 kiloton nuclear weapon in an underground tunnel at the Nevada Test Site (NTS)

LANL notes that underground nuclear weapon testing produces radionuclide gases that may seep to the surface, which is affected by many factors. These include fractures in the rock caused by the explosion's shock waves that create pathways for the gas to escape plus the effect of changes in atmospheric pressure that affect the gases' movement.

Atmospheric pumping of gas through explosion-fractured rock is investigated using a new, sequentially coupled hydrodynamic rock damage/gas transport model. Previous models used a simplified approach, modeling how the gas flows but not coupling that with the explosion rock fracture models through which the gases escape: the seismology and damage. There are major differences between predictions using a realistic fracture network and prior results that did not couple models. For example, simplified fracture models produced some predictive information about the gas movement, but they did not provide the directionally dependent information — that is, whether the gas moved horizontally or upwards through the rock. **Thus the new calculations are able to give a better idea of how much gas may be migrating horizontally away from the location of underground explosions using knowledge about atmospheric conditions (for example, the barometric pressure that creates a vacuum) and seasonal variabilities in different regions.**

This team's research investigated the effects of the fracture network on late-time seepage (weeks to months) of radionuclide gases that migrate through explosion-enhanced fracture networks. The simulations were created for one kiloton UNEs in granite and tuff at burial depths of 125, 250, and 390 meters. Rock damage was simulated in a two-dimensional axisymmetric model using the CASH (CAmpell-SHashkov) hydrocode, a computer code for modeling shock propagation. Barometric data, of great importance to the accuracy of the models and simulations, were selected from the varied climates of Colorado, Alaska, and Hawaii across different seasons and modeled with FEHM (Finite Element Heat and Mass transfer code) developed at LANL. Rather than a generic mathematical model, this research included first-principle seismology, chemistry and experimental data to improve the ensemble model.

Predicting the travel time, window of opportunity for detection, and concentration of radionuclide gases from UNEs is of considerable importance to explosion monitoring.

In addition to nuclear explosion monitoring, this team's coupled model could be applied to other geophysical systems that produce fractures with subsequent flow, such as hydraulic fracturing for fossil fuels, wastewater injection, mine explosions and damaged rock zones around excavations. The gas transport results are relevant to other applications, such as radon and methane migration, soil vapor extraction for cleanup of contaminated sites and landfill gas migration.

— Read more in Amy B. Jordan et al., "Radionuclide Gas Transport through Nuclear Explosion-Generated Fracture Networks," Scientific Reports 5, Article number: 18383 (17 December 2015).

Iran ships 25,000lb of low-enriched uranium to Russia as part of nuclear deal

Source: http://www.theguardian.com/world/2015/dec/28/iran-ships-uranium-russia-nuclear-deal

Dec 28 – **A ship carrying 25,000lb (11,000kg) of low-enriched uranium left Iran for Russia on Monday, marking one of the most vital steps yet in a high-stakes deal to deny Iran a nuclear weapon.**

"I am pleased to report that we have seen important indications of significant progress towards Iran completing its key nuclear commitments under the deal," the US secretary of state, John Kerry, said.

The July accord has been trumpeted as one of the banner foreign policy achievements of Barack Obama's presidency but proved divisive in Washington, with Republicans refusing to support it and several of the party's presidential candidates vowing to scrap it.

Under the deal between Iran and the P5+1 group of world powers, Tehran agreed to scale back its nuclear programme so that Washington and its allies were assured it would no longer be on the threshold of being able to produce an atomic weapon. In return, Tehran will have access to about $100bn of previously frozen assets and fully return to the oil market.

Iran had until the end of 2015 to ship out all but 660lb (300kg) of the low-enriched uranium it has stockpiled. Low-enriched uranium is suited to power generation but can be further enriched to yield fissile material for nuclear warheads.

Welcoming Monday's shipment, Kerry said that by divesting itself of this low-enriched material, Iran had already trebled the amount of time it would take to produce enough fuel for a bomb from two or three months up to nine.

"The shipment included the removal of all of Iran's nuclear material enriched to 20% that was not already in the form of fabricated fuel plates for the Tehran Research Reactor," he said.

"This removal of all this enriched material out of Iran is a significant step toward Iran meeting its commitment to have no more than 300 kilograms of low-enriched uranium by Implementation Day."

Kerry praised Russia, "a country with significant experience in transporting and securing nuclear material", for taking the material out of Iran and providing natural uranium in exchange.

The July agreement also commits Iran to sharply reduce the number of centrifuges, which are used to enrich uranium, as well as to re-engineer a reactor to cut its output of plutonium – another pathway to nuclear weapons.

The International Atomic Energy Agency, the UN nuclear watchdog, will decide when Tehran has complied with its obligations, after which the US, Russia, China, Britain, France and Germany will remove some economic sanctions that targeted the programme.

Ben Cardin, the top Democrat on the Senate foreign relations committee, said recently that "implementation day" could come earlier than expected, perhaps even next month, and not in the spring as initially expected.

But the deal has suffered a potential threat in a different area. Earlier this month the US Congress passed a law restricting visa-free travel rights for people who have visited Iran or hold dual Iranian nationality. The measure, which affects citizens of the 38 mostly European countries that have visa waiver arrangements with the US, is framed as a counter-terrorism measure and also targets Iraq, Syria and Sudan.

Asked about the US law on Monday, the Iranian foreign ministry spokesman, Hossein Jaberi Ansari, told a press conference: "Any steps taken outside the agreement are unacceptable to Iran, and Iran will take its own steps in response where necessary."

Tehran recently test-fired two ballistic missiles capable of carrying a nuclear warhead in breach of a UN Security Council resolution, in what some analysts say is part of a backlash aimed at showing a domestic audience that it has not caved in to the US.

North Korea claims to have tested miniaturized hydrogen bomb

Source: http://www.homelandsecuritynewswire.com/dr20160106-north-korea-claims-to-have-tested-miniaturized-hydrogen-bomb

Jan 06 – **North Korea has conducted its fourth nuclear test in ten years – the previous tests took place in 2006, 2009 and 2013 – indicating that the country is further along in developing nuclear warheads which could be miniaturized and placed on a missile capable of reaching the U.S. mainland.**

Pyongyang pubic media outlets have claimed that what was tested was hydrogen bomb, but some experts who talked with the *Telegraph* say initial evidence suggests the test involved a uranium or plutonium device which was not as powerful as a hydrogen bomb.

North Korean television announced the country had successfully tested a "miniaturized hydrogen bomb" underground on Wednesday morning, describing it as an "act of self-defense" against the United States. North Kore's claim about the type and size of device tested could not be verified independently.

Analysts note, though, that if North Korea's claims are true, it would be the first time the North has successfully tested a hydrogen bomb and could also enable the isolated country to launch long-range nuclear missiles.

"If it's true, it means they've made something smaller scale, capable of being put onto a missile, said John Carlson, the former head of the Australian Safeguards and Non-Proliferation Office. "I think we can assume the previous tests they've carried out have been devices too large to fit onto a missile."

South Korea's intelligence agency said the seismic wave the agency's sensors picked up was more likely caused by an atomic bomb, Lee Cheol Woo, a South Korean politician, told the *Telegraph*.

Yang Uk, a senior research fellow at the Korea Defense and Security Forum, said: "Given the scale it is hard to believe this is a real hydrogen bomb. They could have tested some middle stage kind (of device) between an A-bomb and H-bomb, but unless they come up with any clear evidence, it is difficult to trust their claim."

North Korea's previous nuclear tests triggered condemnations and rounds of UN sanctions banning trade and financing activities which aid its weapons program.

North Korea, believed to have between six and ten crude nuclear bombs in its arsenal, is now facing deepening isolation and more sanctions imposed by the UN Security Council.

Canada: Nuclear transport accident

Source: http://www.nuclearsafety.gc.ca/eng/acts-and-regulations/event-reports-for-major-nuclear-facilities/index.cfm#sec8

Date of event/disclosure: January 11, 2016

Cameco notified the CNSC of a transport accident involving uranium yellowcake that took place on Highway 4 near Swift Current, SK. Cameco activated its approved Emergency Response Assistance Plan, as per procedures, and sent specialists onsite to assess the situation. CNSC inspectors were also dispatched to the accident site to oversee the licensee's response.

The cleanup activities were completed on January 13, 2016, and the highway reopened. Cameco's assessment revealed a minimal and contained spill of uranium yellowcake onsite. The spill was cleaned up, and a survey following the cleanup confirmed that there is no residual contamination. There was no impact to members of the public, the environment or first responders as a result of the spill.

The container that had suffered a breach was sealed and safely placed inside an overpack. It is now being transported to one of Cameco's licensed facilities in Saskatchewan for repackaging before the shipment continues to Cameco's Blind River Refinery in Ontario. A CNSC inspector oversaw all actions taken at the site, and the CNSC is satisfied that Cameco's Emergency Response Assistance Plan was implemented properly and successfully. This accident will be discussed at the next Commission meeting to be held on January 28.

Could North-Korea's Bomb Be a Super-EMP Weapon?

Source: http://i-hls.com/2016/01/could-north-koreas-bomb-be-a-super-emp-weapon/

Jan 13 – Although North Korea was rather braggingly telling the world that it had managed to explode a test hydrogen bomb, several nuclear exprts remain sceptic.

The White House itself said that results from the explosion weren't consistent with a hydrogen bomb which has the potential to be even more powerful than an atomic bomb.

Among the experts' downlplaying North Korea's boastful achievement, **one specialist claims that results actually indicate that this explosions was "another kind of H-Bomb" and is in fact a neutron bomb or an enhanced radiation weapon such as a super-EMP (electromagnetic pulse) weapon.**

Peter Pry, an expert on EMP weapons, says that North Korea's claims align with the scenario of a device which produces enhanced amount of devastating gamma rays despite its low yield.

Pry said the latest North Korean weapons test followed three others each in the range of 10 kilotons or less, adding that Pyongyang has been conducting underground nuclear tests since February 2013, all of which have been of low-kiloton yield.

Pry – who is the executive director of the Task Force on National and Homeland Security, and served on the Congressional EMP Commission, the House Armed Services Committee, and the CIA – as well as other EMP experts said North Korea has the capability to launch a satellite carrying a super-EMP weapon into space that could be triggered to explode on command at a high altitude over a highly populated area in the United States.

The neutron bomb is designed to generate enhanced gamma rays which in turn cause the super-EMP effect. An H-bomb of identical explosive yield of a fission, or atomic, bomb is a neutron bomb that will emit some 10 times the amount of neutron radiation. In an atomic device, the total radiation pulse energy composed of gamma rays and neutrons is only 5 percent of the entire energy released. In a neutron bomb, it is closer to 40 percent. In addition, the neutrons emitted by a

neutron bomb have a much higher average energy level than those released during a fission reaction.

Pry had told WND that North Korea was working on such a device as early as last year. The US government, however, denied it had developed miniaturized nuclear warheads and missiles to deliver them. This denial, Pry said, came despite an assessment by both the Defense Intelligence Agency and the Central Intelligence Agency that such do indeed exist.

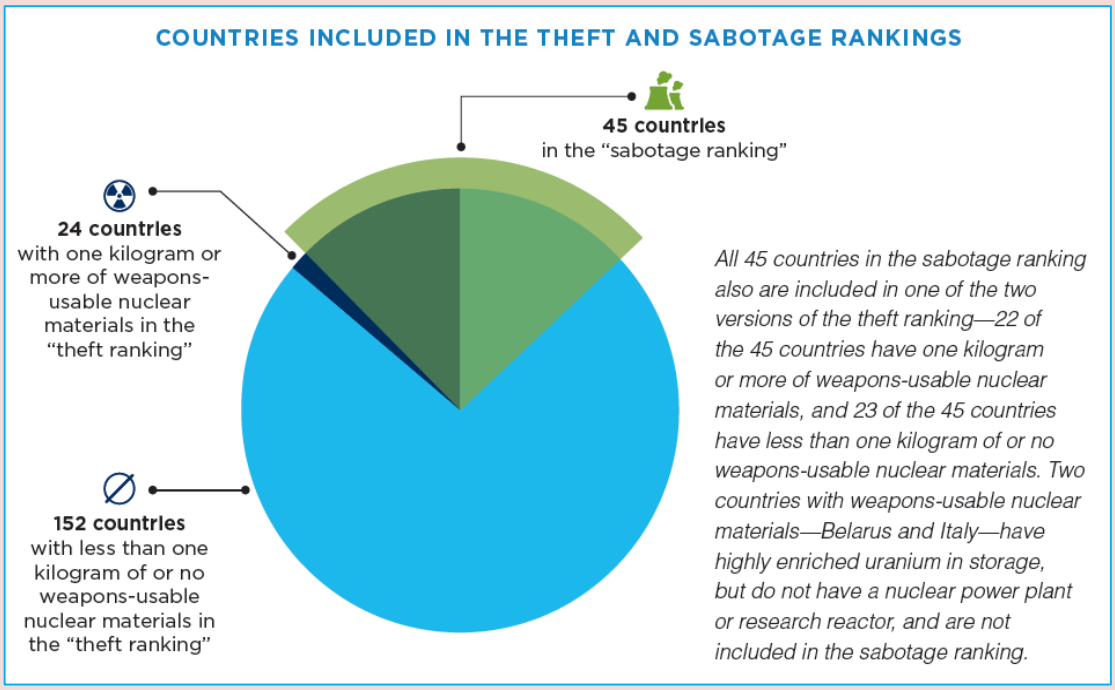
Slowed Momentum on Nuclear Security

Source: http://www.ntiindex.org/wp-content/uploads/2013/12/NTI_2016-Index_FINAL.pdf

Six years ago, world leaders gathered for the first time to collectively address the growing threat of catastrophic nuclear terrorism. At that first Nuclear Security Summit in 2010, the leaders launched a major initiative to lock down the more than 2,000 metric tons of weapons-usable nuclear materials then spread across the globe and to reduce stocks of plutonium and highly enriched uranium, which are the key ingredients needed to build a nuclear weapon.

Today, as leaders prepare to gather in Washington, D.C., for their fourth and final summit, they can cite progress on their pledge to protect vulnerable nuclear materials from theft by terrorists seeking weapons of mass destruction and to build a robust nuclear security system involving all states in the ongoing protection of dangerous nuclear materials. Since early 2010, a dozen countries have eliminated weapons-usable nuclear materials from their territories, dozens more have strengthened their nuclear security practices and policies, and a key international treaty is closer to entry into force.

However, the global threat environment has worsened. At the same time, progress on goals set during the first three summits has slowed, according to the results of the 2016 NTI Nuclear Security Index (NTI Index). It's a troubling development at a time of escalating and evolving threats from sophisticated and well-financed terrorist organizations, from nuclear smugglers, and from hackers capable of launching devastating cyber attacks at nuclear facilities.



In addition, the current global nuclear security system still has major gaps that prevent it from being truly comprehensive and effective. For instance, no common set of international

standards and best practices exists, there is no mechanism for holding states with lax security accountable, and the legal foundation for securing materials is neither complete nor universally observed.

Without a comprehensive and effective global system in place, states' approaches to nuclear security continue to vary widely, thereby creating dangerous weak links that terrorists could exploit as they seek the easiest path to weapons-usable nuclear materials.

▶ **You can read the full report at source's URL.**

America's Nuclear Power Plants Vulnerabilities

By David J. Stuckenberg and Hershel C. Campbell

Source: http://acdemocracy.org/americas-nuclear-power-plants-vulnerabilities/

Jan 18 – A year-long study found that the present legal and regulatory approach to EMP/Space weather threat to America's nuclear power plants are inadequate and dangerous. This sorry state is anchored in the industry efforts to maintain safety regulations dating back to the 1980s, and a national security mentality relevant at the end of the Cold War.

This has been successful, in part, due to a campaign to brand nuclear power as a clean, safe source of energy. To their credit, the NRC and industry have demonstrated a commitment to safety where design basis events are concerned. However, EMP and GMD are beyond design basis events. Once these occur, there are no guarantees and few strategies with which to cope.

There has only been a handful of nuclear disasters in history, and only one in the U.S. – TMI. It is, therefore, understandable from an economic standpoint that industry is resistant to change. However, this inertia has given rise to a complacent regulatory climate absent adaptive and progressive analysis. More than 30 years have elapsed since this topic was last openly addressed. Unfortunately, the assumptions borne of the highly controversial 1982 report continue to misinform decision makers even as recent as 2015. Despite these challenges and an NRC and industry galvanized to maintain the status quo, there are signs of progress. Some push for increased standards and regulations has occurred since Fukushima.

However, these efforts have been met with a tepid response from the nuclear industry. To stave off costly infrastructure updates, the industry responded by holding out the FLEX, a plan that is both impractical and dangerous due to an over-reliance on a functioning national infrastructure. Congress recently found, "The current strategy for recovery leaves the United States ill-prepared to respond effectively to an EMP attack that would potentially result in damage to vast numbers of components nearly simultaneously over an unprecedented geographic scale."

As a result, 31 (bi-partisan) members of the House sponsored the Secure High-voltage Infrastructure for Electricity from Lethal Damage Act (or the SHIELD Act), to create a mechanism to address the nationwide EMP risk. The Act sought to establish a mechanism whereby the President of the United States (POTUS) along with a specialized commission could designate certain areas and nodes critical to the U.S. infrastructure and security. The Act also provided the POTUS the authority to compel enterprises both public and private to protect key elements of the grid.

Most importantly, the SHIELD Act would have conferred upon the U.S. Federal Energy Regulatory Commission legal authorities, which it currently lacks, to require the North American Electric Reliability Corporation and the electric power industry to protect EHV transformers, SCADAS, and other critical components of the bulk power system from natural and manmade EMP. Moreover, if SHIELD were enacted and implemented, by protecting the bulk power system, nuclear reactors would have been protected from the scenario of a protracted nationwide blackout.

The Congressional EMP Commission estimated that the national electric grid could be protected from natural and manmade EMP for about $2 billion and that implementation, on a nonemergency basis, would require 3-5 years. However, lobbying by the electric power industry kept SHIELD from coming to a vote before the House

Energy and Commerce Committee for years, until the bill died.

In November 2015, the House passed by unanimous consent the Critical Infrastructure Protection Act (CIPA–HR 1037), which bill requires the Department of Homeland Security to establish a new National Planning Scenario focused on EMP. All federal, state, and local emergency planning, training, and resource allocation is based on the National Planning Scenarios—so CIPA will for the first time require emergency planners and first responders at all levels of government to be EMP educated and begin preparing to survive and recover the nation from an EMP catastrophe. CIPA further requires DHS to develop plans to protect the electric grid and other critical infrastructures from natural and manmade EMP, to evaluate existing technologies and help develop new technologies for EMP protection, and to launch pilot projects to encourage the protection of the electric grid and other critical infrastructures. CIPA currently awaits action by the Senate.

Conclusion

The U.S. must address 21st Century problems with 21st Century prevention-based mitigation strategies that are part of a holistic and common sense approach.

This study contends that although the threat to EMP/GMD and its likely impacts on nuclear power stations have been known for some time, both internal and external political pressures have ensured the regulatory and technological status quo for more than three decades.

However, some steps could be implemented to significantly reduce our vulnerability to EMP and GMD including the addition of requirements to sustain stations, hardening, filters and development of better early warning and detection systems that would allow for grid isolation and shutdown before impact. However, hardening the nation against an EMP or major GMD event will require a total effort directed not only toward critical infrastructure and national resources, but also those that beckon to greater individual and community responsibility relating to issues of sustainment.

With that in mind, we recommend a holistic approach that strengthens both our nuclear infrastructure and individual communities until a total solution is realized. In a world where America's adversaries are increasingly innovating, developing, adapting, and accessing conventional and asymmetric weapons capabilities, our nation must make grid protection a top priority. However, the theoretical dichotomy between America's grid and nuclear power stations and research reactors must be expunged. Our power grid is part of a total system – a system that is required to ensure a safe and prosperous United States, and all of it must be safeguarded if we take our national security seriously

David Stuckenberg *is Chairman of the American Leadership & Policy Foundation and a USAF veteran pilot with experience in the intelligence and strategic arms control communities.*

Hershel Campbell *is Ronald Reagan Research Fellow at the American Leadership & Policy Foundation and a USAF veteran where he served as an intelligence analyst.*

New X-ray method could detect nuclear materials

Source: http://www.homelandsecuritynewswire.com/dr20160119-new-xray-method-could-detect-nuclear-materials

Jan 19 – Physicists at the Diocles Extreme Light Laboratory at the University of Nebraska-Lincoln have demonstrated that their unconventional laser-based X-ray machine could provide a new defense against nuclear terrorism.

In proof-of-principle experiments, the UNL scientists used the laser-driven X-ray source to produce an image of a uranium disk no bigger than a stack of three nickels and hidden between 3-inch steel panels.

"For the first time, we have used our new X-ray source to detect a nuclear material inside a shielded container," said Donald Umstadter, director of the Diocles Laboratory and leader of the project.

UNL notes that the Domestic Nuclear Detection Office of the Department of

Homeland Security funds the research, through a contract with the National Strategic Research Institute. The government is evaluating the technology.

Inspectors need tools to help find nuclear materials hidden behind thick shielding or smuggled inside any of the 100 million-plus cargo containers shipped around the world each year. Uranium is perhaps the easiest nuclear material to obtain and hide, Umstadter said.

Device detected the uranium disc in the steel container, as shown // Source: unl.edu

The researchers demonstrated that laser-produced X-rays can detect an even smaller amount of uranium than the minimum amount required by current inspection standards (one kilogram) and can penetrate much thicker steel than the walls of cargo containers.

The laser X-ray source offers a number of advantages. Much like a laser pointer can be directed across a large auditorium, the technology can shoot a thin X-ray beam long distances, enabling inspection of cargo ships before they reach port. Yet it emits much lower levels of radiation than conventional X-rays, making it safer for use around workers and bystanders.

Unlike previous sources of similar X-rays, which require stadium-sized facilities, this X-ray source is portable and could be moved in a semi-trailer truck, increasing its potential for use as a nuclear site inspection tool.

Umstadter and his team announced in 2013 they had developed the laser-driven X-ray source, called a laser-wakefield-accelerator-driven inverse-Compton-scattering, or LWFA-ICS, source. At the time, they said the new source not only would increase the availability of sophisticated forms of X-rays needed for physics research, but it could be used to detect hidden or smuggled nuclear materials. Since then, Umstadter and his team have set about proving that the X-ray machine would work for those purposes.

"It's not unusual for scientists to go beyond basic research to develop new technologies, as we did with our device," he said. "However, the great urgency and importance of detecting smuggled nuclear materials compelled us to go even further and be the first to apply the new technology."

UNL holds a patent on the new detection method, Umstadter said. The University of Michigan's Department of Nuclear Engineering and Radiological Sciences provided numerical simulation support as a subcontractor on the project.

UNL says that the next step in this project for Umstadter and his team is to improve the performance of the X-ray device as well as the precision with which it can identify shielded nuclear materials.

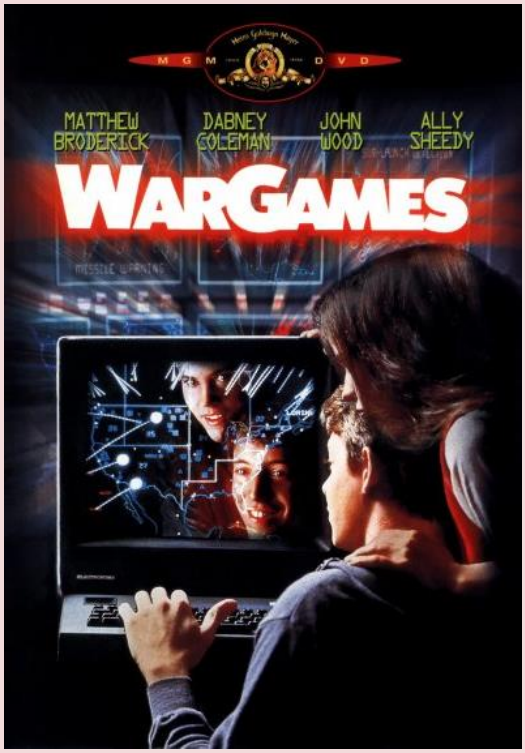
Umstadter and Shouyuan Chen, a UNL research assistant professor of physics and astronomy, presented their findings at the International Meeting on Laser-Driven Radiation Sources for Nuclear Applications at George Washington University in Washington, D.C., on 15 December.

— Read more in Shouyuan Chen et al., "Shielded radiography with a laser-driven MeV-energy X-ray source," Nuclear Instruments and Methods in Physics Research, B: Beam Interactions with Materials and Atoms 366 (1 January 2016): 217-23.

A Map of Global Nuclear Weapons Brings 'WarGames' into the 21st Century

Source: http://www.citylab.com/design/2016/01/a-map-of-global-nuclear-weapons-brings-wargames-into-the-21st-century/423828/

Jan 14 – ***Shall we play a game?*** In the 1983 geek-classic *WarGames,* a high-school hacker



dials his way to the government supercomputer in charge of American nukes. When the talking machine suggests they play checkers, chess, and a little thermonuclear war, the teen thinks it's mere fun. But World War Three may actually be imminent.

In the finale, a missile-launch sequence flashes across massive Air Force computer maps, apparently signaling global apocalypse. Fortunately, it turns out to be just a game—with a strong anti-proliferation message.

That scene just got a makeover in a new interactive from Mapbox.

Mapmakers Anya A'Hearn and Allan Walker recreated the iconic *WarGames* world map in a fully 1980s digital aesthetic, populated with open-source data on the current whereabouts of the world's known nuclear weapons. Surprisingly, this information is relatively up-to-date, and freely available, on the websites of the Bulletin of the Atomic Scientists, the Federation of American Scientists, and a smattering of rabbit hole-y sites that document things like global locations of surface-to-air missiles.

Nuclear weapon-loaded aircraft carriers, air force bases, and international target ranges are mapped in terrifying detail across the U.S., Russia, China, Iran, India, Turkey, Israel, the

UK, and a clutch of other European countries. You'll find missile silos and parked ballistics on fields from North Dakota to just outside of Paris. The team also created a "command terminal" and interactive dashboard that lets you "talk" to Joshua, the computer from the film.

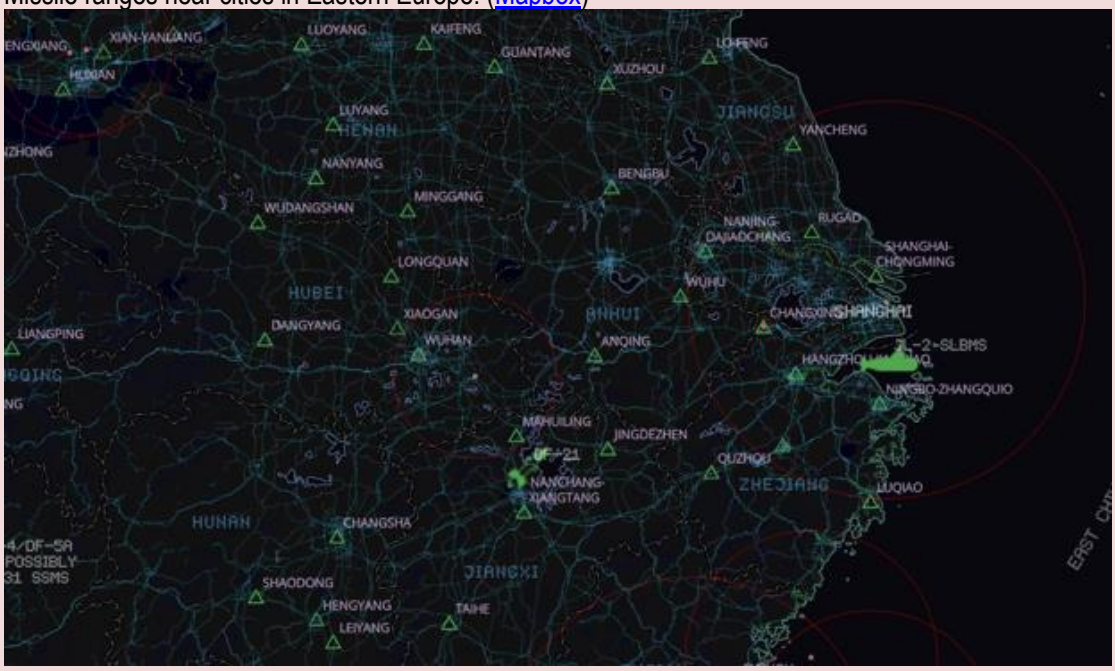
With North Korea inching towards a functional nuclear arsenal, the Obama administration modernizing its weapons stash, and the Iran nuclear deal playing out in unexpected ways, the moral of *WarGames* is as relevant as ever.

Matthew Irwin, who helps head government and humanitarian work at Mapbox, says that the map takes abstract information that would otherwise be lost in a spreadsheet and makes it more palpable and real.

"It means nothing to me to talk about the numeric blast radius of a weapon," he says. "But when you see a dot on a map the size of Detroit that represents it, that's really scary."

The map can be an overwhelming experience, in its level of detail and subject matter. It works best in macro, as a reminder of the film's wise and witty message: *A strange game*, the computer says. *The only winning move is not to play*.

Missile ranges near cities in Eastern Europe. (Mapbox)



Air force, submarine, and nuclear missile installations in China. (Mapbox)

SNP bid to ban nuclear convoys through Lothians

Source: http://www.edinburghnews.scotsman.com/news/politics/snp-bid-to-ban-nuclear-convoys-through-lothians-1-4006172

Jan 20 – **Midlothian MP Owen Thompson will today launch a Commons bid to ban convoys of nuclear weapons travelling through towns and cities.**

The move follows reports of at least two incidents when convoys were spotted near Penicuik, including one when the weapons were parked just yards from two schools.

Mr Thompson said he had serious concerns about the safety of driving nuclear weapons on long journeys on public roads and in highly populated areas.

He has tabled a motion at Westminster condemning the "unacceptable risk to public safety" and is to propose a Ten Minute Rule Bill this afternoon seeking to restrict the transportation of the weapons.

He said: "The idea that weapons of mass destruction are being transported through the streets of Midlothian, and all across the UK is absolutely chilling.

"One weekday lunchtime last May, a convoy was parked at Glencorse barracks for a break. It was off the road, but the barracks are next door to Beeslack High School and across the road from Mauricewood Primary School. So you can imagine pupils playing in the school grounds and just over the fence are these weapons of mass destruction."

The convoys – tracked by campaign group Nukewatch – travel between Berkshire, where the weapons are made and serviced, and Coulport in Argyll, where they are stored and loaded.

Mr Thompson said they typically consisted of 15 or 20 vehicles in total, including extra security, and they varied their route but he claimed the risk was still "far too high".

"The **potential** for an accident is huge," he said. "The Ministry of Defence says it has an unblemished safety record, but that does not take account of the many near misses. They have breakdowns, there are pictures of them having to change tyres at the roadside and the normal things that happen to vehicles.

"When you think of what they are carrying it's unbelievable they are on the roads.

"I'm calling on MPs of all parties to join me in condemning the unacceptable risk to public safety.

"The impact of any safety breach simply does not bear thinking about. The Ministry of Defence must now detail exactly what safety precautions they take while these nuclear weapons travel through the UK – and put an immediate stop to the convoys."

Ten Minute Rule Bills offer MPs the chance to raise an issue of concern in the Commons chamber, but they often do not proceed much further.

Mr Thompson has also lodged an Early Day Motion, condemning the risk to public safety, calling on the UK government to clarify what safety measures they have in place and urging a stop to the convoys.

He said: "In Scotland, people have made clear our opposition to weapons of mass destruction being based on the Clyde – and the transport of nuclear weapons from one end of the country to the other should not be based on an argument of convenience at the expense of safety.

"The policy as it stands lacks transparency, is counterproductive against protecting us from terrorist attacks and shows a blatant disregard to the communities that they pass through.

"Of course, the only way to fully guarantee public safety is to remove these immoral, strategically useless weapons once and for all."

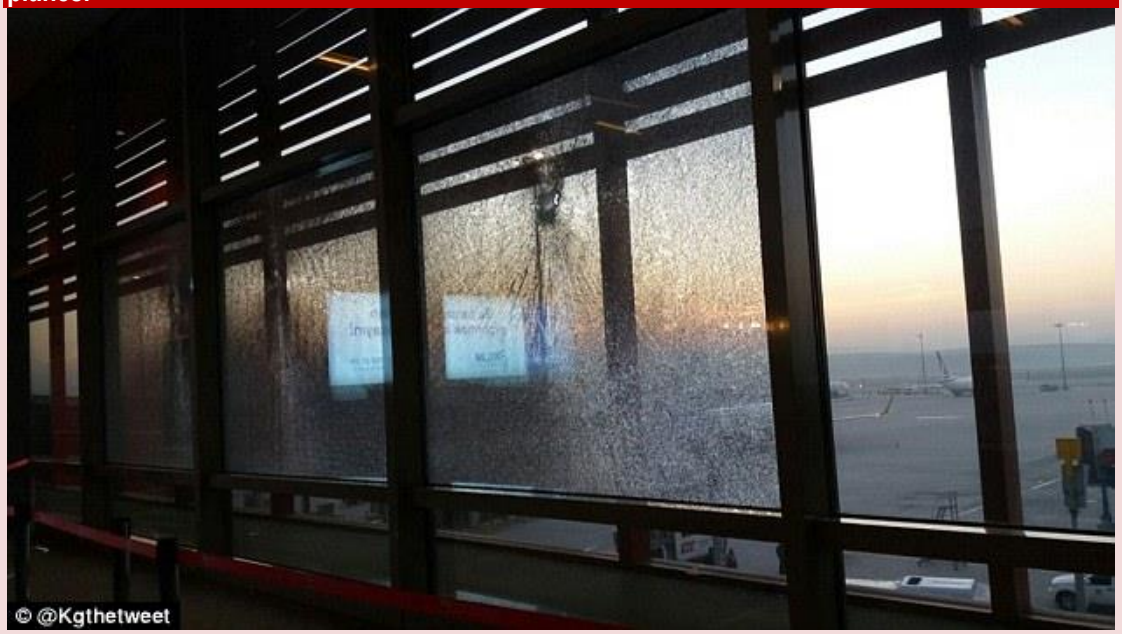
EDITOR'S COMMENT: Everything for 10 sec of publicity? Next step will be the abolishment of Armed Forces at all! Too much peace is bad for citizens' health! On the other hand he could ask funds for creating a peripheral road surpassing his town minimizing the "potential" of an accident or to be informed about safety rules implemented during these evil transportations.

Istanbul airport explosion kills cleaner

Source: http://www.theguardian.com/world/2015/dec/23/istanbul-sabiha-gokcen-airport-explosion-kills-cleaner

Dec 23 – **An overnight explosion at an airport in Istanbul killed one person and damaged three planes hundreds of metres apart,** Turkish media said, triggering a security alert as authorities sought to determine if a bomb was responsible.

The blast at Sabiha Gokcen, the city's second airport and located on its Asian side, occurred shortly after 2am, local budget carrier Pegasus said, fatally wounding a cleaner on one of its planes.



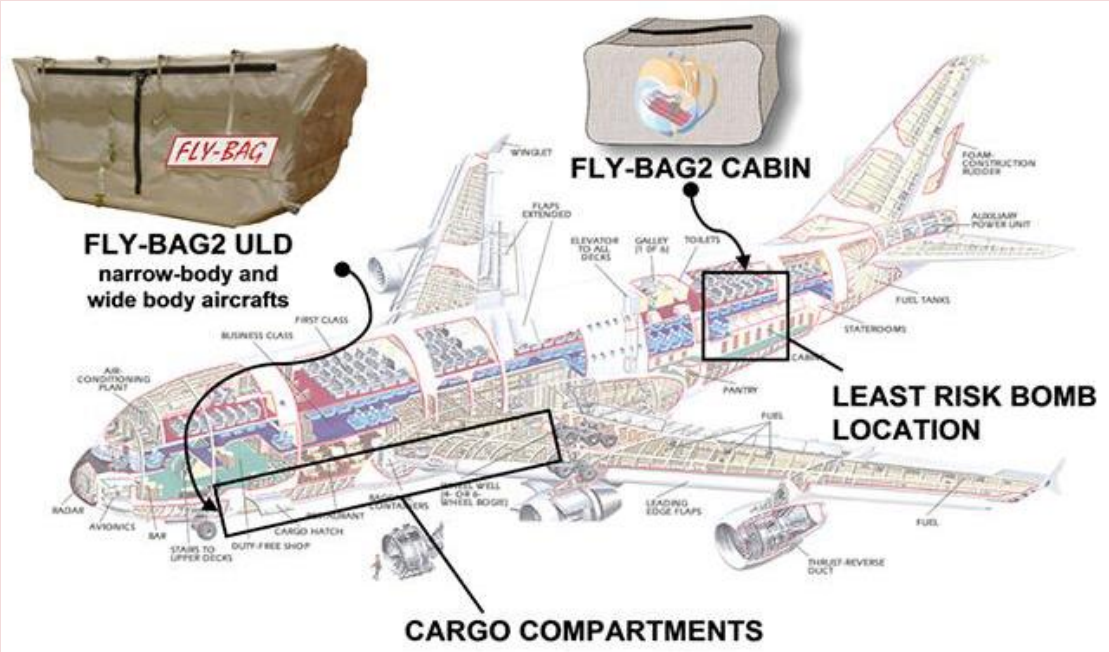
The airport's owner, Malaysia Airports, referred to more than one explosion "at the tarmac area", adding that normal flight operations had resumed by 4am.
Police declined to comment, while the airport said investigations into the cause of the blast were ongoing.

Bomb attacks by Kurdish, leftist and Islamist militants are common in Turkey. A three-decades-old conflict between the state and the militant Kurdistan Workers Party has flared up in the country's mainly Kurdish south-east since the collapse of a ceasefire in July.
No passengers were in the area at the time of the airport blast, which the Dogan news agency said caused damage to at least three planes as far as 300 metres from each other.
A photo on Dogan's website showed a hole in one plane window. Video footage showed investigators taking photos of a terminal building wall, dozens of metres from the nearest planes.
Police armed with rifles and protective vests imposed tight security at entrances to the airport, searching vehicles while a police helicopter circled overhead, the state-run Anadolu agency said.
According to its website, Sabiha Gokcen served around 26 million passengers in the first 11 months of the year, less than half the number at the main Ataturk airport on the European side of the city.

This Solution Could Protect Planes against Bombs

Source: http://i-hls.com/2015/12/watch-this-solution-could-protect-planes-against-bombs/

Dec 30 – The recent downing of Russian Metrojet plane in Egypt has once again brought to the forelight a major issue facing modern airliners: planes are fragile and incredibly easy to bring down. A simple, small bomb – hidden inside a soft drink can in the case of Metrojet – can destroy a whole plane, ending the lives of all passengers and crew.



An international team of scientists has now made a significant headway into making flights far, far safer. They have figured out how to bombproof the luggage hold of a commercial plane, keeping it safe in the event of an explosion.

Fly-Bag, as their solution is called, is a flexible, bombproof material designed to line the inside of commercial airliner's luggage hold. It's constructed from multiple layers of high-strength, heat-resistant materials. For example, Aramid, one of the

composite materials, is used in ballistic body armour.

It's the flexibility of the Fly-Bag that allows it to contain the power of the explosion – by stretching to accommodate the shock wave – while protecting the plane's machinery and the people inside from shrapnel and blast fragments.

The Fly-Bag was developed in a cooperative effort by a coalition of European partners from the United Kingdom, Germany, Sweden, Spain, Greece, Italy, and the Netherlands.

The protective "bag" was first tested at the blast laboratory at the University of Sheffield. Once the prototypes were proven effective, testing moved on to real-world conditions, with controlled explosions in the holds of a Boeing 747 and an Airbus 321. To everyone's relief, the Fly-Bag proved successful in the tests and contained the explosions.

"Key to the concept is that the lining is flexible and this adds to its resilience when containing the explosive force and any fragments produced," says Dr Andy Tyas, of the Department of Civil and Structural Engineering at the University of Sheffield. "This helps to ensure that the Fly-Bag acts as a membrane rather than as a rigid-walled container which might shatter on impact."

Remote-controlled robot inspects suitcase bombs

Source: http://phys.org/news/2016-01-remote-controlled-robot-suitcase.html

Abandoned items of luggage are frequently found at airports and train stations. This is a case for the emergency services, who have to assume that these items might contain bombs. They must assess the potential threat quickly, avert any possible danger, and preserve evidence for criminal proceedings. In the future, police will have the support of a remote-controlled sensor system as they go about their duties. Fraunhofer researchers are developing this sensor suite in cooperation with industry partners and criminal investigation authorities.

Anyone who forgets their luggage in public places, airports or train stations will spark off a large-scale police operation. Time and again, suitcases, bags or backpacks left lying around unsupervised cause a bomb alert. Admittedly, most abandoned luggage items turn out to be harmless. But in the first instance the emergency services have to proceed on the assumption of possible danger and check whether they are dealing with an improvised

explosive device (IED) that might blow up at any time. This involves getting up close to the luggage to inspect it. A system that makes it possible to assess the danger of the situation quickly – and also records 3D images of the contents and shape of the luggage as well as of the surrounding area – would make the specialists' work considerably easier, speed up the reconnaissance process, and minimize the risk for the emergency personnel.

Since November 2014, researchers at the Fraunhofer Institute for High Frequency Physics and Radar Techniques FHR in Wachtberg have been developing such a system together with the North Rhine-Westphalia State Office of Criminal Investigation, the Leibnitz University in Hannover, ELP GmbH and Hentschel System GmbH. The German Federal Office of Criminal Investigation in Wiesbaden and the German Federal Police Force are supporting the project as additional expert consultants. The German Federal Ministry of Education and Research is funding the USBV Inspector project with a grant of two

million euros as part of its Research for Civil Security program.

Emergency services do not have to enter the danger zone

The system the researchers have developed comprises a multimodal sensor suite consisting of a millimeter wave scanner, a high-resolution digital camera, and a 3D environment monitoring system. The components are contained in a housing and mounted on a robot platform. Bomb disposal engineers remotely control the robot from a safe distance. Its swiveling 3D sensors make a three-dimensional survey of the crime scene, and the digital camera provides high-resolution images for later optical evidence preservation. Meanwhile the millimeter wave sensor scans the source of danger and creates an image of what's inside. A built-in embedded PC on the robot collects the data and sends it to the investigators, where it will be merged on the computer by means of sensor data fusion.

"Up to now our techniques have not allowed us to form a 3D outline of suitcase bombs, and it has been impossible – or only partially possible – to make a spatial map of the contents. With the sensor suite we can visualize in three dimensions what's inside a luggage item, and so determine the composition of the bomb and how the parts are arranged in the luggage," explains Stefan A. Lang, team leader at the FHR and the project's coordinator. This lets the explosives experts quickly assess the threat, and going forward they will also be able to preserve as much evidence as possible about the bomb. Until now, specialists were often forced to destroy suitcase bombs – making it difficult to identify the perpetrators. Other advantages of the contact-free detection system: it is light, compact, and platform independent, which means it can be mounted on any robot.

Within the project, the FHR researchers are developing the millimeter wave scanner (also referred to as a radar sensor) for fast reconnaissance. This scanner allows a very high depth resolution. "For the radar we make use of the synthetic aperture radar, or SAR, principle, by which the sensor is moved along a trajectory, a kind of track – from left to right in front of the case, for example – and the Doppler information generated in the process is used to create an image," explains Lang. Apart from the research work on the sensor, the expert and his team are also looking into ways of determining the optimum trajectory for surveying an object. This depends on the shape of the luggage item or container, its position in the environment, and the position of the robot.

A radar sensor demonstrator will be ready in April 2016. Extensive field tests of the remote-controlled sensor suite begin in the middle of 2017, with the multimodal sensor suite set to be launched in 2019.

.

Troops use robotic arm to defuse powerful TNT filled cooker IED

Source: http://www.dailyexcelsior.com/troops-use-robotic-arm-to-defuse-powerful-tnt-filled-cooker-ied/

Dec 27 – Troops of Rashtriya Rifles battalion of Counter Insurgency Romeo Force today averted major tragedy when it detected and defused powerful TNT filled Improvised Explosive Device (IED), fitted by the militants under a bridge at Saglet in Sakhi Maidaan area of Mendhar tehsil in Poonch district.

The militants had planted the IED to blast the bridge and cause casualties of security forces and civilians but the alert troops foiled their designs by recovering the IED well in time and defusing it.

The troops used

robotic arm to defuse the IED to ensure that there were no casualties of the security personnel by defusing it manually.

Official sources said the troops of Rashtriya Rifles battalion of Counter Insurgency Romeo Force spotted a cooker IED fitted under Saglet Bridge in Sakhi Maidaan area of Mendhar tehsil in Poonch district at 7.30 am today and immediately stopped traffic on Mendhar-Poonch road via Mankote.

The troops called Bomb Disposal Squads of police and Army. Senior police officers rushed to the spot and stopped movement of civilians in the area.

The troops used robotic arm to defuse the IED to ensure that there were no casualties of Bomb Disposal Squad while defusing very powerful explosive device. The cooker was filled with five kilograms TNT explosive device, which was capable of blasting Saget bridge and causing extensive damage to vehicles crossing over it.

Sources said target of the militants by planting the IED under bridge was vehicles of security forces and civilians as they intended to cause casualties by carrying out major subversive activity to make their presence felt in the border district of Poonch, where they were presently lying very low.

"The IED was successfully defused at 1.15 pm," sources said, adding the traffic on Mendhar-Poonch road via Mankote was restored only after Army and police sanitized the area and declared it fit for traffic.

Though there has been no major presence of militants in the border district, some militants and Over Ground Workers were reportedly active and in possession of explosive devices. Sources said the IED might have been fabricated and planted by one such group.

"The analysis of the bomb indicated presence of about five kilograms of powerful TNT explosive material inside the pressure cooker," sources said, adding the vigilant and timely action by the troops has averted what could have been a major catastrophe.

They pointed out that blasting of the bridge would have de-linked Mendhar with Poonch via Mankote. The IED was capable of blasting the bridge and disrupting the vehicular movement.

Defusal experts in cat-and-mouse game with bombmakers - veteran bomb technician

Source: https://www.rt.com/shows/sophieco/326388-bomb-disposal-explosive-device/

Dec 2015 – A profession in which one makes a mistake only once. Called *"the most dangerous job in the world,"* bomb disposal is unforgiving - and yet, vital in the era of terrorism. Widely portrayed in the media, the details, the intricacies of defusing explosive devices still remain unknown. How do you detect a bomb? How do you make sure lives are saved? And when life and death are on a stake, how do you cut the right wire? In this special interview, one of the British most experienced bomb disposal veteran, gives us insight into his risky craft. Major Chris Hunter is on Sophie&Co today.

Sophie Shevarnadze: *Major Chris Hunter, one of the British army's most experienced bomb-disposal experts, a counter-terrorism specialist, welcome to the show, it's really great to have you with us. So, improvised explosive devices, IEDs, they have been the*

bane of the coalition forces in Iraq, the number one cause of death among NATO troops in Afghanistan. How's that any terrorist with that 10 dollar tin can bomb can defeat the hi-tech army?

Chris Hunter: It's a real force multiplier for insurgents and terrorists. I remember when I went to Iraq in 2004, the insurgency have been going for about 12 months, and prior to that, my colleagues and I have been pitting our wits against the IRA, who are the most technically advanced terrorists in terms of the IED in 30 years, and that level of technical sophistication was superseded in 12 months by the insurgents in Iraq, because the availability of the information, the Internet, the passage of the information by the other terror groups, and, of course, off-the-shelf availability of components makes it a really cheap but highly effective weapon system.

SS: *So, Chris, was this asymmetrical answer to the might of the West expected to be so potent?*

CH: I think it was a capability that was pretty much overlooked, actually. I think many of the great nations, the great powers around the world, have had their own internal security issues at some point, and have built up a capability for domestic security and engaging with dissent, if you like, internally, but, I think, the extent, the volume to which we've seen this as a *"capability",* if you like, is pretty much unprecedented, prior to the last decade, if you like, and I think, we saw it in Iraq, really effectively, we saw it in Afghanistan, we saw it in Chechnya - and if you got a well equipped, well trained military force that covers land, sea and air capabilities, then no insurgence force is going to be able to match that or defeat it with conventional tactics and conventional capabilities - but, when they're hiding amongst the population, when they're using devices and weapon systems that, effectively, they have no rules of conflict in the use of those, then they become a very-very potent weapon and a real force multiplier for the insurgents.

SS: *As you said, the IEDs have improved massively since the days of IRA, and ever since the start of Iraq and Afghanistan, what exactly has changed?*

CH: I think, in most insurgencies, what we tend to see is an evolution. You start with things like command-wire IEDs, an explosive charge that may be placed at the side of the main road, and there'll be a hard wire link back to the firing point, potentially up to a kilometer away. The perpetrator of the attack, the terrorist identifies the target, whether it may be a patrol of soldiers or some sort of vehicle, a convoy, something like that and at the point at which it passes the contact point, he will then initiate a firing switch a detonate it. What we then see is, because there's a physical wire there, it's potentially easy to detect, and it also constrains the firer to a single firing point, which limits his escape routes as well. So, we then see these, what we call, *"Drop and Pop"* devices where there's a wireless link, there's no hard wire, therefore they can fire it from 360 degrees, although what they still need to do is to provide some sort of the overwatch and that's why that 75% of the IEDs we see around the world are radio-controlled IEDs, wireless IEDs - but what we do see is a continual evolution in the technology and the ability to buy it off the shelf, and of course, any technology, once it's publicly available, the price tends to go down - so, insurgents, terrorists can pretty much turn anything into a bomb if it has some sort of electronic output.

SS: *So, how do you keep up with terrorist innovation? I mean, what kind of strategies are used in response to such innovations?*

CH: First and foremost, intelligence sharing is absolutely essential, and there's a very good network around the world now of law enforcement agencies who have what they call *"Bomb Data centers"* and they effectively input all of the date of every single incident in that particular country or countries in which they have an interest, and then that data can be data-mined, if you like - but they also share the intelligence with other countries as well, and that's essential, because many of these terror groups, groups like Daesh that we see at the moment, they don't recognize international boundaries. They are global in nature, and so, where they employ a certain type of devices, a certain type of technology, it's essential that that information is shared so that any country that potentially would become a target of them can develop a capability. So, it's constantly looking at technology, constantly carrying up research and development to see if you can turn it into a bomb yourself and then watching what the terrorists do and effectively exploiting that technology so that you can come up with some sort of counter-measure to it.

SS: *Nowadays you have protective suits, you have robots, the IEDs aren't stuck in the last century either - can the work of the defuser be done with robots eventually? Can technology make your form of job, this line of work, obsolete in the future?*

CH: The use of robotics, the use of drones are becoming increasingly more integrated into explosive ordnance disposal as the Render Safe Procedure and the very first, sort of principle, in any EOD operation is remote means where possible and if you can't use a robot or some sort of remote means, then semi-remotes where you put on bomb suits, grab it with some hook and line or something and then go back to safe area and pull that line and get that particular type of system to carry out some sort of action - whether it's gonna move the device, shift it, potentially even activate it. And it's only when you can't do those remote actions or the semi-remote actions, you then go to a manual operation where you go down there, where you physically got to carry out some sort of Render Safe Procedure while you're hunched over the bomb. And, just like the terrorists, look at various different ways to come up with new technologies, to beat the bomb technicians. We continually look at ways to identify how we can counter their particular capabilities. The difficulty is, in most developed nations, there are procurement strategies, cycles, bureaucratic red tape to go through, and it may take up for 18 months from concept to implementation for a certain system to defeat a device, if you're trying to implement that in developed nation. The insurgents, quite often, will just come out with a new device in 5 or 6 days, so it's a continuous of cat-and-mouse game, a game of extreme chess - it's very very difficult to get those technologies in, in time.

SS: *Now, the IRA used bombs to deadly effect - you saw that with your own eyes in Lisburn, Northern Ireland. Radical Islamist terrorists started using suicide bombings as a real tactic. We're seeing it being used in combat by ISIS, everywhere… What other tricks do terrorists have up their sleeves? What other surprises they may have in store?*

CH: Basically, you have to look at the terror group to start with, and identify what their objective is. Is that some sort of nationalistic objective, is it religious, is it the establishment of caliphate - and then you have to look at the capabilities, at potential technologies that they have. With the IRA, they didn't want to kill civilians, because they realized that their popularity, the support base, will be affected detrimentally. So, they would give coded warnings, they would put out car bombs, they would try and destroy infrastructure and the economy, but they didn't want to kill people and they certainly wanted to run away to be able to fight another day. So, what we see with extremist groups however, is that their capabilities are far broader and the potential components that they can use are far more widely available. Also, their objective and their tactics, techniques and procedures are very much into creating true terror. Terrorism is designed to create terror so that you can influence a population or a body of people, and they use these deadly and determined attacks, and, of course, suicide terrorism, really-really affects the population. The London 7/7 bombings, you know, they were, you know… there were fewer more than 50 people actually killed in them, but most Londoners will be able to tell you where they were on the day of 7/7 bombings, and you know, the Tube, the metro system wasn't really occupied for several weeks afterwards. But, it's not just IEDs. They use maiming, they use raids, hijackings, kidnappings, shootings, assassinations, beatings - all sorts of different tactics, techniques and procedures, as long as they will create some sort of fear.

SS: *Chris, how do you deal with facing a bomb you've never seen before? How do you approach it? Are they all similar in basis? Or are you forced to improvise all the time?*

CH: All bomb technicians are taught the principles of ammunition, the principles of explosives, ballistics, metallurgy, nuclear physics, explosive chemistry, and every type of weapon system, ranging from a hand grenade, a bullet for a pistol, right away to guided weapon systems. So, they are all equipped with those first principles of ammunition and explosive design, but when you go to an improvised device, by definition, even if you've seen that type of device before, you never know, how it's going to be manufactured, they're not made with factory precision standards - so you have to treat every single device as if it's a new one. So you have to go through a really complex thought process, you have think about where the bomb is, who's placed the bomb, who has designed it to actually kill, what other sort of potential influence and factors there may be, if there may be some sort of peripheral threats as well. As you go through that process you start to try and mitigate the different types of threats and you look at, you know, is it potentially a time

bomb, is it potentially a booby-trap, a victim-operated device, is it potentially a command-initiated device - and as you start to wriggle down and identify what these devices are, you can then start to effect a Render Safe procedure, actually take that long walk up to the bomb; but actually it's only when you make that very final cut of the detonator and the power source, you truly made that device safe, and at that point you can go and exploit it, but you always send some sort of report, technical report to make sure that all those other bomb data centers, all those other operators around the world are aware of this particular type of device, so that if they do encounter it, then they've got some sort of idea as to what they're dealing with.

SS: *Now, it must be strange when you never see any real enemy, just car- and road-bombs. How taxing is that psychologically?*

CH: It's like a game of extreme chess. You're trying to sort of identify who's the bomber and how does he think, and what they're trying to achieve - what we call the *"tactical design":* are they trying to kill civilians, are trying to kill members of the security forces, there's something that's more sinister, a design to actually lure me in and kill me as a bomb technician. So, you've got this sort of man-vs-man concept to start with, and you're trying to pit your wits against this adversary that you, generally, haven't seen and haven't met. But, you're also faced with this extreme technical challenge - you're trying to identify whether the bomb is a time bomb, a victim-operated bomb, a command-initiated bomb, radio controlled and something like that. And then, once you've done that, you're trying to actually to get down to the bomb, without setting any patterns, because you know you're probably being watched, and if it's a radio-controlled bomb, you've got to try and somehow protect yourself, potentially jam the airwaves to make sure that if there's a trigger-man out there you can actually detonate a device as you get up to it. And when you get there, it's like you're interpreting this bird's nest loop of wires, and you've got to try and identify exactly how that bomb works, and then, of course, come up with a decision as to how you can actually render it safe. So, there's a great deal of pressure, but you go into complete tunnel vision, and become completely focused, and forget everything else in the outside world.

SS: *But would it be easier mentally to be faced with an actual enemy, with enemy troops?*

CH: I think it's definitely easier if you're faced with an adversary that you know, you've met, you understand, you've studied - I mean, if you think about boxing or something like that, you know, when they get into the ring with their adversaries, they watch the videos of them, the watch the films, they've studied them to pieces; whereas with bombs and bomb-makers, it's very difficult to do that, so it is far more challenging when it's the enemy that you don't know. But what we do, is try and identify the bomb-maker's signature. It's not just the bomb itself that we neutralize, we actually go into a complex investigation, we look at the forensics, at the DNA, the biometrics, and the type of attack and how it's been planned. Anything at all, it would give us an indication as to who the bomb-maker is, and then we actually start to bring all the different intelligence sources together, evidence, witnesses, and at some point actually find out where they are, so we can go and interdict them and arrest them and bring them to justice.

SS: *So, in which situations have you found yourself more often: where your training and expertise would be enough for the job, or more when you needed guts and adrenalin or dumb luck to see it through?*

CH: I think, to be honest with you, you need all of them in equal measure. You have to rely on your training - you know, the training is very-very extensive, and quite brutal as well, you know. My basic course was 14 months with 203 exams, and we were only allowed to fail three exams - you know, you can fail 3 exams in the final week of that course, you know. So, the training was very-very extensive, and very punishing -t o make sure that you have the right sort of mentality and that you're equipped with the right knowledge. But, when you actually get out onto the ground, there are significant pressures, so sometime you have to rely on your courage, sometimes you have to rely on your knowledge, your training, your experience... but, there is that element of luck as well, because there are improvised devices and at some point, your time and your luck could run out.

SS: *How to describe these moments, as getting in the mind of the bomb-maker? What do you mean by this? I mean, do bomb-makers purposely set traps for you, trying to make it difficult for you?*

CH: There's only a finite number of bombers with the requisite skill-sets. To manufacture the technically advanced type of IEDs that we're seeing in war zones and around the world, you know - attacks on aircrafts, attacks on infrastructure - and, in order to make, develop those devices in that sort of volumes at that level of sophistication.... there's, you know, a finite number of these people. So, if we can to start to identify them, and work out how they think, what makes them tick, look at the patterns of behaviour, look at the patterns of the IEDs themselves, look at the signatures, and as I say, the DNA, the forensics, at some point we can actually start to identify who these people are, where they may be - through a number of different techniques. And then, of course, once we've taken those people out of the equation, it goes a long way to actually disrupting an insurgency, because the IED is the weapon of choice - and therefore, if you can prevent it from being made at source, by going *"left of the boom"* as we call it, then you can have a very-very significant effect on disrupting that insurgency and having a positive outcome.

SS: *Now, as you say, sometimes, the bombs are dummies, made to lure you out - do bomb-makers or terrorists target you personally? Or, make bombs specifically for you?*

CH: Because those bomb-makers are so advanced, and because they know we're trying to not just neutralize the bombs but actually trying to interdict them and remove them from the insurgency, they will try just as hard to attack us as well. When I was in Iraq in 2004, I had a price placed on my head. I had no idea what it was at the time, actually, but St. Andrews University published something recently and said that the bomb technicians at that time in Iraq had a price of a $150,000 placed for my head, which is quite a significant sum, considering the daily and weekly incomes of the population there. So, there's a very-very concerted effort to try to kill bomb technicians. In Northern Ireland, we saw that extensively, and I had another incident where the IRA tried to target me there. In Iraq, obviously; but also, even in Russia as well, you know. We've seen Russian bomb technicians who have been targeted and, unfortunately, killed by the insurgents there.

SS: *Now, you've advised government in the aftermath of the London 7/7 bombings, you worked both in Iraqi cities and London... Is dealing with bomb threats specific to every city, are they different regionally, nationally?*

CH: At an actual bomb incident itself, quite often, they will have to confirm that there's a bomb to start with, because, at any city, there are always cars illegally parked or left in the wrong place, items of unattended luggage - you couldn't treat anyone of those as a bomb. Once you've confirmed that it's an IED, then you would look at cordoning and an evacuation to a sensible safe area, as quickly as possible and in a safest possible way. Once you've confirmed, you've cleared, you've cordoned the area, then you've basically got to make sure that you've checked the area for any secondary devices, potentially - because, quite often, the terrorists will know that you've evacuated to a certain distance, based on the type and size of the device. So, they may put secondary devices around cordoned positions to try and kill the civilians, the camera crews, the emergency services that are on these cordones, and, of course, you're checking all the time as well for any other threats and any other activities, and looking to see if there any other evidence, any unusual behaviour, because in the same way as arsonists usually watch the scene and stay at the scene of the arson attack, you quite often see the same with bombers, and you certainly see it when it comes to radio-controlled bombs, because they've got to be able to overwatch the contact point, the seat of the explosion, in order to fire it off. So, there's a number of things that emergency services would that are quite commonplace, but they are attuned or redefined depending on the actual country and the landscape itself.

SS: *So, here's something that boggles my mind every time - how do you go about making highly explosive material yourself at home? I mean, shouldn't it be difficult to obtain? The Paris attacks demonstrated that terrorists have no problem building a bomb in a European capital.*

CH: What we tend to see, Sophie, is that, depending on the country and the accessibility of certain explosive components, or weapon systems that will very much steer the capability of the terror groups. We've seen ISIS-inspired attacks, an Al-Qaeda inspired-attacks on continent of Europe, and we've seen that in the United Kingdom as well. What Al-Qaeda started to introduce in their "Inspire" magazine - so, they came up with this principle of "death-by-a-thousand-cuts" in their "Inspire" magazine, which is their online-magazine that went out to everybody who wanted to read it, so they could become lone wolf terrorists. And it said, "rather than

doing these complex, expensive, multi-personell type of attacks" that involve all sorts of continually shifting components, it said, go for really crude instruments - go to a Piazza, to a public real, a public place, and drive a car into lots of people, gets some knives out and start cutting people and stabbing them, but make sure that it's all filmed on social media, because what you want, of course, is to terrorise the population and scare people. So, we saw just last week, in London, a stabbing, where somebody in the Metro system said "I'm doing this for ISIS" which qualifies this as terrorist attack, albeit a very crude one, whereas on the continental Europe we tend to see the more advanced, the more complex roving gunmen type of attacks recently. Roving terrorists types of firearms attacks.

SS: *Chris, when you were ready to leave the army, you said you were worried your time was up, or your luck was running out, or something. Is facing a bomb you can't defuse at some point a reality for every bomb technician? Do you meet your match sooner or later?*

CH: I think, there's two components to it, you know. When you're dealing with an IED, it's incredibly gratifying on a spiritual level, it's incredibly gratifying on a adrenalin-fuelled level, if you like. When you go into a bomb scene and you see a scene of utter carnage after an explosion, when you see maimed, wounded, dead people, spread all across an area, and destruction - it's horrendous. But, when you can actually get there and neutralize the bomb, and you realize you've prevented that carnage from occurring - it gives you a real sense of gratification and a huge lift amongst the entire team. But, there's also that sort of real adrenalin base, as I mentioned as well. You're potentially, continually, testing your luck - every device you come across, you counter, you don't know what it is, until you've made that final cut of the wire, and so, at some point, irrespective of the knowledge base that you've built up, your experiential learning, your true ability as an operator, built up over the years, there's some point where your time or luck could run out - and that could be a device that you just can't work out, or can't get access to to neutralize it, or it could be that you've just get there too late, and the device detonates as you approach it and you get killed.

SS: *Chris, thank you very much for this interesting insight. We were talking to Major Chris Hunter, veteran of the British Army's Bomb Disposal Forces, talking about living life with no second chances and overcoming deadly danger of explosives. That's it for this edition of Sophie&Co, I will see you next time.*

Irish army bomb experts win EU project to develop system to deal with chemical or nuclear explosion

Source: http://www.irishexaminer.com/ireland/irish-army-bomb-experts-win-eu-project-to-develop-system-to-deal-with-chemical-or-nuclear-explosion-377092.html

Jan 20 – Army bomb experts are to develop a hi-tech system to deal with a chemical, biological or nuclear explosion.

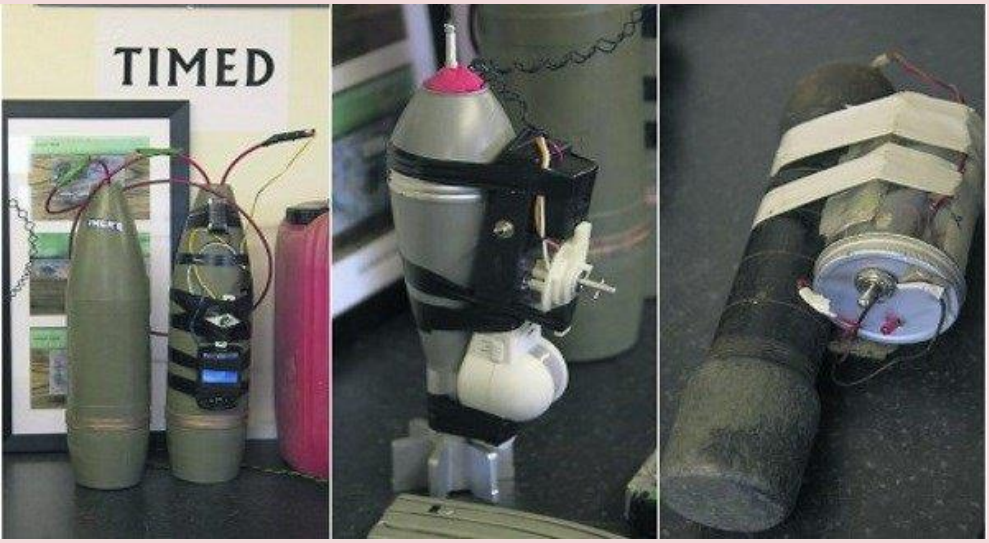
The Irish Defence Forces' bomb disposal units were deployed 141 times in 2015.

The Irish Defence Forces is part of a consortium including NUI Galway and Saab which this week won a coveted €4m European Commission project.

They intend to build a ground robot or a drone-type aircraft to remotely respond to such an explosion, including in a highly populated area, such as a stadium or on the battlefield.

The Irish submission topped 40 other bidders. The news emerged during a lengthy media tour yesterday of the Ordnance School at Defence Forces HQ at the Curragh, Co Kildare.

Ray, a top-level officer in the school, who spoke on condition of anonymity, said the aim was to develop a "remote operational system" to deal with a chemical, biological, radiological, or nuclear attack in various scenarios, such as in a "stadium or built-up area".



He said the system could be a "ground robot" or "an unmanned aerial vehicle", such as a drone.

Different types of improvised explosive devices that the Irish Defence Forces have encountered.

In a situation where a chemical, biological, radiological or nuclear bomb had "functioned", or gone off, the robot or drone would go in and take a sample and bring it back for analysis.

Ray said the technology could also be deployed to prevent an explosion. It could also be used in international settings, such as conventional battlefields.

Regards responding to incidents such as the November 13 terror attacks on Paris, Ray said: "Threats change all the time. We adapt and respond and we try to be ahead of what's coming down the line."

The Ordnance School is a logistical and operational unit, the latter better known for its Explosive Ordnance Disposal teams or bomb squads, which were deployed 141 times in 2015.

A two-year course is given to recruits, who typically join with a degree in science, engineering, or electronics.

The school boasts a range of equipment, from EOD blast suits (weighing 31.5kg), special chemical, biological, radiological or nuclear suits and detectors, to 'Hobo' bomb disposal robots.

Senior school instructor Paul, also speaking on condition of anonymity, said the recruits were trained in engineering and tactics, including 'counter improvised explosive devices', which involves understanding the threat, responding to it and countering the next threat.

This involved targeting the full network, from the triggerman to the planner to the builder to the supplier.

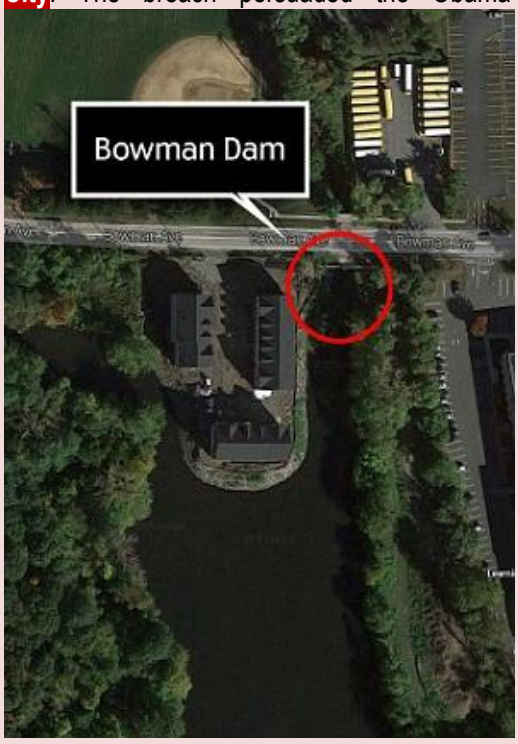
Paul said the 2001 attacks on the World Trade Center opened a "Pandora's Box" and demanded a new response.

He said the improvised mortar devices designed by the dissident republicans demonstrated a "significant capability" and was to be "taken seriously".

Iranian hackers attacked New York dam

Source: http://www.homelandsecuritynewswire.com/dr20151222-iranian-hackers-attacked-new-york-dam

Dec 22 – **In 2013, Iranian government hackers infiltrated the control system of Bowman Avenue Dam in Rye, New York, located twenty-five miles from New York City**. The breach persuaded the Obama administration significantly to bolster U.S. cyber defenses, and appeal to private corporations to cooperate with the government in trying to guard against cyberattacks.



The United States has been worried about data theft for a while, but the attacks on the dam offered vivid demonstration of the vulnerability of many parts of the U.S. infrastructure.

CNN reports that on twelve occasions in the last decade hackers managed to gain top-level access to key power networks, which would have allowed them to trigger massive blackouts in cities, and deny power to military facilities. A couple of months ago DHS revealed that ISIS had been trying to hack U.S. power companies.

As dams go, the Rye dam is small at about 20ft tall — controlling the flow of Blind Brook as it heads toward Long Island Sound. By getting into the dam's control system, the hackers, using a cellular modem, could have released larger volumes of upstream water without warning.

The *Wall Street Journal* reports that there was some confusion initially, as DHS and DOE thought a similarly named dam in Oregon — the Arthur R. Bowman Dam – was the one hacked. The Oregon dam, at 245 feet, is much bigger, and hacking its control systems could have had much more serious consequences.

The Iranian attack on the New York dam was in retaliation for the Stuxnet attack on Iran's uranium enrichment

centrifuges. The Iranian government hackers also tried to hack major U.S. financial institutions.

"We are not where we need to be," on protecting U.S. infrastructure networks against cyberattacks, Alejandro Mayorkas, deputy secretary of DHS, told the AP. He noted that the U.S. electricity grid may be particularly vulnerable because much of it still relies on ageing computers installed and programmed before cyberattacks were a concern.

Cyberattacks on infrastructure are often conducted for the purpose of collecting information, including detailed drawings, for potential use later.

"If the geopolitical situation changes and Iran wants to target these facilities, if they have this kind of information it will make it a lot easier," Robert M. Lee, a former U.S. Air Force cyberwarfare operations officer, told AP. "It will also help them stay quiet and stealthy."

DHS also maintains the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) to respond to such attacks. **According to ICS-CERT, in 2014 the team responded to 245 cyber incidents reported by critical infrastructure operators, 32 percent of which were in the energy sector and 27 percent of which were in critical manufacturing.**

A Comprehensive Cyber Attack on ISIS – Pros and Cons

Source: http://i-hls.com/2015/12/67446/

Dec 23 – The Pentagon is set to step up its cyber warfare efforts against ISIS, and is arguing that disabling the group's computers, mobile phones, and servers could help disrupt terrorist attacks and recruitment efforts.

US military hackers, from the Cyber Command at Fort Meade, Maryland, have developed a range of malware tools to attack ISIS' propaganda and recruitment capabilities, said a US official on condition of anonymity.

Other intelligence agencies, notably the FBI, are resisting the move. They fear that taking drastic measures against ISIS' online activity would harm intelligence collection, obscuring the locations and intentions of ISIS militants and leaders.

Further, such tools could harm humanitarian aid, opposition groups, and US-backed rebels in Iraq and Syria. There is also the likely risk of the malware spreading beyond the borders of ISIS' stronghold.

The White House wants "to see options" for countering ISIS online, said a US official. "That doesn't mean they are all in play. It just means they want to look at what ways we can pressure" ISIS.
For the moment, White House officials prefer targeted attacks against particular targets, when intelligence gathering can point to specific phones, computer, or digital services used by ISIS.
"If you do see something that is in service of an active operation, you may want to take some action to disrupt that operation," said deputy national security adviser Ben Rhodes in an interview.
Cyber Command has been targeting ISIS networks and social media accounts so far, but Pentagon officials want more to be done. They argue that viruses, denial of service attacks, and other cyber-attacks, could and should incapacitate ISIS' communications.
Cyber security experts, however, are weary of such drastic action. They argue that such moves could force ISIS to use more secure and harder to detect methods of communication.
"Sitting there trying to play whack-a-mole to knock these communications platforms off can be so complicated and so resource intensive and only marginally effective," said John D. Cohen, a former senior Homeland Security counterterrorism official who teaches at Rutgers University.

Cyber Terrorists Are Gaining Ground

Source: http://i-hls.com/2015/12/cyber-terrorists-are-gaining-ground/

Dec 21 – The field of cyber warfare has brought about a paradigm shift in the old balance of power. Sheer force of numbers and financial and scientific superiority can only go so far when technology and the advantages it offers, like a double-edged sword, carry within them a whole slew of new risks, threat vectors, and dangers. By its very nature, the digital world provides small, disparate actors with the tools to potentially challenge powerful nations, while simultaneously increasing the capabilities of all such states, be they China, Russia, or the United States.

"You can spend a little bit of money and a little bit of time and exploit some of our weaknesses, and cause us to have to spend a lot of money, a lot of time," said Terry Halvorsen, CIO of the Department of Defense, at a conference in September. Unlike in previous ages of warfare, in the cyber era it can take only one determined, capable individual to exploit a security weakness negligently left unattended and harm a vital piece of equipment or infrastructure. These attacks can be perpetrated from across the globe with close to no risk to the perpetrator.

The tools and know-how required for such operations are mostly readily available. Would-be hackers have freely available to them everything from basic tools designed to exploit unpatched vulnerabilities, to reams of documentation and practical guides needed to gain knowledge of the most advanced, fundamental systems online. This is not lost on state-actors, nor sinister non-governmental combatant forces.

Adversaries "continue to evolve and we've seen a number of our threat actors that they realize it's a low cost, if you will, to get into this space and they're using that to their advantage," said Col. Robert "Chipper" Cole, Director of Air Forces Cyber Forward, 24th Air Force.

Potential notwithstanding, so far terrorist organizations and other non-state actors do not, for the most part, possess the requisite capabilities to inflict serious damage. Cyber attacks that cause significant damage, such as the hack that "massively" damaged a steel mill in Germany in 2014, are a significant but rare occurrence. Attacks similar to the infamous Stuxnet worm that destroyed Iranian nuclear centrifuges, widely attributed to Israeli security forces, still require capabilities terror groups as yet do not possess. **It "takes a large, well-resourced, and time-intensive effort to use cyber tools for major disruption or physical damage,"** wrote in a report James Lewis, program director at the Centre for Strategic and International Studies.

Western allies, however, cannot rest easy in the knowledge of their comparative advantage. Terrorist organizations are pouring significant resources into beefing up their cyber efforts. While Al Qaeda is hampered in the cyber field by over 25 years of covert operations, hiding out in remote locations, and massive efforts in avoiding detection, the same cannot be said of its successors. ISIS is "changing the landscape of al Qaeda-related cyber activities, however," according to a report by the

American Enterprise Institute's Critical Threat, "Al Qaeda Electronic: A Sleeping Dog."

While Al Qaeda's online activity so far, as detailed in the report, is mostly constrained to website defacement and sporadic denial-of-service attacks, the group is reportedly expending significant resources on catching up with its rivals. "It remains plausible that AQE could move onto targets of greater importance and deploy more powerful software," the report states. Other groups, such as the Syrian Electronic Army and ISIS, cannot be written off so lightly. The latter has used its resources to collect personal information on American servicemen and women, force a French television station off the air, and other intricate operations.

Non-governmental actors are so far lagging behind powerful nation states, but their capabilities are constantly evolving and advancing. The cyber domain has in many ways levelled the playing field, with few individuals able to pose a significant threat to large organizations. Western allies must be alert to the risks posed by the evolving landscape and take proper precautions to not be caught off-guard. ISIS is not yet able to launch devastating cyber-attacks, but it, and others, may soon be able to do so if their advancement is not checked.

Jihadists Plans Are Public – Why Aren't Authorities Acting?

Source: http://i-hls.com/2015/12/67505/?mc_cid=f08ab290d0&mc_eid=521c0e089a

Recently there have been increasingly vocal calls for weakening encryption heard around the world, with the strongest of them in the US. Federal authorities claim that weakened encryption could have prevented the San Bernardino shooting and other atrocities. It seems, however, that **intelligence agencies are not utilising the data already at their disposal, and it is far from certain breaking encryption would assist them in performing their jobs.**

"There is in fact no evidence that this or any of these … attacks could have been prevented by regulation of encryption technology," writes Rita Katz in an article published in the Washington Post. Katz is the director of the SITE Intelligence Group who has spent nearly two decades studying jihadists.

Elton Simpson, one of perpetrators of the 3 Mat attack in Garland, Texas "exchanged 109 [encrypted] messages with an overseas terrorist" just before the attack, said FBI Director James Comey to the Senate Judiciary Committee. Comey was arguing for the weakening of encryption. The simple fact of the matter, however, is that Simpson used Twitter – an unencrypted platform – to communicate with several high-profile terrorists. He was also known to the FBI from previous terror-related investigations.

The incitement for the attack came from one of Simpson's Twitter connections, and was discovered using open-source information by SITE. It was reported to the FBI a week prior to the attack, but the agency failed to prevent it. While the encrypted messages were discovered only after the attack, the open-source communication was available long before it. Unfortunately, "the FBI is reluctant to recognize open-source as an important — arguably the most important — tool to track jihadists online," writes Katz.

It has long been established that ISIS – and other groups – are adept at using the newest digital tools at their disposal. They rank and recommend different services for their followers to use. Curtailing one service would only lead jihadists to use another quicker than authorities can respond. It would be a whack-a-mole game intelligence services would struggle to win. What's more, outlawing or weakening encryption would only sabotage the security of law abiding citizens. There is no reason to believe that those who are willing to kill for their beliefs would be deterred from employing illegal means to achieve their aims. Outlawing the mathematical algorithms used for encryption would be futile, as would be enforcement attempts.

The most important issues at hand are why are intelligence agencies, and the FBI most of all, so reluctant to use data already at their disposal; and, why, when they already have the data, are they so inept at utilising it. Many atrocities could have been prevented had the intelligence community done its due diligence in following up on traditional leads, had it employed readily available tools to analyse data –

and fostered the development of new tools to do so better.

Currently, authorities are attempting to make our digital lives – soon to be indistinguishable from our "real" lives" – less secure. Weakening encryption would jeopardise everything from online banking, to patient confidentiality, to the very systems that protect critical infrastructure. The "government must first know how to utilize the mass amount of data it has been collecting and to improve its' monitoring of jihadist activity online," writes Katz.

Anonymous Declares War on Turkey

Source: http://i-hls.com/2015/12/67488/?mc_cid=f08ab290d0&mc_eid=521c0e089a

Dec 27 – Turkey has been accused by a variety of sources of aiding and abetting ISIS. Some of the accusations include giving medical treatment to ISIS militants, providing a safe harbour for them to rest and regroup on Turkish territory, and buying oil from the self-declared caliphate, thus providing the group with vital finances allowing it to continue its operations.

For this reasons, **hacktivist collective Anonymous have declared an online war against Turkey.** Anonymous threatened to sabotage the country's airports, banks, and military services, as well as government facilities, by targeting their servers and data links.

So far, the hacktivist campaign has brought down nearly 40,000 websites across Turkey through coordinated action against the country's root DNS servers – used for addressing and directing browsing traffic to websites.

Anonymous' announcement demands Turkey stops assisting ISIS at once.

'Turkey is supporting Daesh by buying oil from them, and hospitalizing their fighters. We won't accept that Erdogan, the leader of Turkey, will help ISIS any longer.

If you don't stop supporting ISIS, we will continue attacking your internet, your root DNS, your banks and take your government sites down.

After the root DNS we will start to hit your airports, military assets and private state connections. We will destroy your critical banking infrastructure.

Stop this insanity now Turkey. Your fate is in your own hands,'

Previously, Anonymous began an operation targeting ISIS. They have taken down thousands of the social media accounts used by the terrorist group, and disrupted their online communications. The group has also released personal information of about 1,000 alleged Ku Klux Klan members.

Cyberattack on Ukraine grid: here's how it worked and perhaps why it was done

By Michael McElfresh

Source: http://www.homelandsecuritynewswire.com/dr20160120-cyberattack-on-ukraine-grid-here-s-how-it-worked-and-perhaps-why-it-was-done

Jan 20 – **On 23 December 2015, two days before Christmas, the power grid in the Ivano-Frankivsk region of Ukraine went down for a reported six hours, leaving about half the homes in the region with a population of 1.4 million without power, according to the Ukrainian news media outlet TSN.**

It reported that the cause of the power outage was a "hacker attack" utilizing a "virus." Outages were caused when substations — devices that route power and change voltages — were disconnected from the grid, TSN said.

There have been a handful of documented attacks on the power grid and control systems of energy systems, such as oil refineries. But this cyberattack in Ukraine counts as only the second or third to successfully derail power delivery using a software-based attack.

Because of its success, the incident has sent shock waves through cybersecurity circles. How was this attack carried out? And could something similar happen in other countries?

Stuxnet to BlackEnergy

Cyberattacks designed to take out the power grid have been a big concern of security specialists for many years. Much of the concern has been focused on potential attacks on the control systems, called Supervisory Control and Data Acquisition (SCADA) systems, on which power grids are highly dependent for safe, reliable and secure operation. SCADA systems also provide critical data for operations, automation and remote control.

Some computer worms have been specifically designed to attack the types of control systems commonly found in power utilities. The most well-known is called **Stuxnet**, which was used to compromise Iran's uranium enrichment facilities. But a variety of similar worms have been developed that experts have feared would be used to bring down the power grid.

While the Ukraine outages were reported to involve only one utility, Prykarpattyaoblenergo, evidence of computer malware known as **Blackenergy** was identified at that utility and two other regional utilities. Samples of the suspect code have since been studied, and various security companies, including iSight Partners, EBET, and SANS-ICS, have verified that it contained elements of the Blackenergy malware.

The BlackEnergy malware is generally associated with a group referred to as Sandworm, which is believed to be based in Russia. It is not clear if Sandworm has an association with the Russian government.

Growing sophistication

BlackEnergy started as a malware system for launching denial-of-service (DoS) attacks, which are designed to prevent legitimate users from accessing a server by any one of a number of possible mechanisms. BlackEnergy has since evolved into an effective system for data exfiltration, or the unauthorized transfer of data from a computer. Such a transfer may be manual and carried out by someone able to access the computer, or it may be automated and carried out through malicious programming placed on the computer being attacked.

About two years ago, a new version of BlackEnergy began to appear with new functions that included stealing passwords, covertly taking screenshots, gaining persistent access to command and control channels and destroying hard drives.

More recently, security software maker ESET found evidence of several new features, including a wiper component dubbed KillDisk. A wiper is software designed to erase portions of a disk and can be used to cover up evidence of an attack. In the Ukraine attack, it is not clear if Blackenergy was used, but some of its components were present; in particular, there is evidence of KillDisk.

Some experts contend that this may not technically have been be a cyberattack. The malware allowed attackers to manually intervene in the grid's operation; by contrast, the Stuxnet software inflicted damage on industrial machines as was.

Regardless, there was a sophisticated attack that required coordination of different types of malware, which appear to have enabled the attack.

Worries over disabling nuclear plants

The Ukrainian power grid has several attributes that cause some special concern.

The bulk of the power production at any time is provided by nuclear power plants, which provide most of the steady "baseload" power to supply electricity through most of the day.

To meet fluctuations in demand — for instance, increases in power use in the morning as people begin their day – grid operators in Ukraine primarily rely on coal power plants. They do not have many avenues to import power from other countries to meet spikes and dips in demand.

This situation means that if an cyberattack causes a power outage, Ukraine grid operators may not be able to respond rapidly enough and export an excess in the flow of power, which would lead to grid instabilities and the need to shut down nuclear reactors.

There is also the issue of cooling of reactors in the event of a power outage. The cooling pumps in the nuclear reactors in Ukraine are

dependent on AC power input from the grid, thereby making them susceptible in the event that backup diesel generators cannot be started.

Broader concerns

Could this happen in the West? In short, yes. U.S. utilities use software products from various major vendors which have been the targets of a Sandworm BlackEnergy campaign. Thus far, there doesn't seem to have been any financial benefit from the attack. What's more, when attackers use malware, they expose their methodology, which makes it possible for security people to develop protections for that line of attack. So we have to wonder what they had to gain from the exercise.

If they have nothing to gain in the short term, like robbing banks while the grid is down, did they gain valuable experience for their next, more effective attack?

The ability to hack into a utility to throw switches (breakers) at substations, as was done in Ukraine, opens up the possibility of more serious types of attacks, as was demonstrated by the Aurora Test. In that controlled experiment, circuit breakers associated with a generator were opened and closed using software in a way that resulted in permanent damage to equipment.

While it's hard to know the attackers' intentions for sure, it appears likely that the Ukraine power grid was attacked with at least the help of the BlackEnergy malware, increasing the technological potential for disrupting power grids in general.

This incident underscores the need for diligence and the increased effort in cybersecurity that we are seeing in the government and private sectors. The continuously increasing dependence on the power grid is driving the need for cybersecurity to be part of the design of all new systems.

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

One third of U.K.'s specialized terrorist response vehicles to be scrapped

Source: http://www.homelandsecuritynewswire.com/dr20151221-one-third-of-u-k-s-specialized-terrorist-response-vehicles-to-be-scrapped

Dec 21 – In 2004, following the U.K. government 2003 decision to participate in the U.S. invasion of Iraq, the British security authorities were growing anxious about possible terrorist retaliation for the U.K. participation in the war and the occupation of Iraq which followed.

To meet that threat, the Incident Response Units (IRUs), with their distinctive red coloring with yellow stripes, were introduced at a cost of £54 million.

The *Independent* reports that to save money, one third of all the fire brigade vehicles which were part of the IRUs, and which would have been called out in the event of terrorists setting off a "dirty bomb," are being scrapped.

The decision was taken in secrecy, and critics note that it contradicts other measures taken by the government to increase funding of intelligence and law enforcement agencies for the specific purpose of bolstering the ability of the government to thwart and, if need be, deal with acts of terror.

The IRU vehicles were equipped with the latest technology to deal with a chemical, biological, or nuclear attack. They have been distributed to different fire stations around the country so that they would not have to travel far to the site of an incident.

The vehicles do not belong to the fire brigade but to the Department of Communities and Local Government, and may be dispatched to the site of an incident only with the department's authorization.

Their IRUs vehicles also each carry dozens of specialized, and expensive, protective clothing called power respirator protective suits (PRPS). These suits must be replaced every ten years, and the need to do so next month was behind the department's decision to scrap 22 of the 63 IRUs, rather than replace the PRPS on all the vehicles.

Earlier this month the department circulated a briefing note to all the fire stations hosting the IRUs, saying: "The 22 IRUs identified as

surplus to requirements will be considered 'off the run' from 31 December. It has been necessary to remove the vehicles from service almost immediately due to the imminent expiry dates of the PRPS carried on these vehicles. The remaining 43 IRUs will be issued with replacement PRPS over the next two weeks."

The *Independent* notes that the Labor Party and the Fire Brigades Union criticized the decision. Andy Burnham, Labor's shadow Home Secretary, said: "It cannot possibly be the right time to cut, by a third, our ability to respond to serious terrorist incidents. Not only is it the wrong time, but it is even worse that these plans are being hatched in secret, without any public information or consultation. Ministers must put these plans on hold immediately and make a statement to Parliament as soon as it returns."

WiFi signals can be used to detect attackers

Source: http://www.homelandsecuritynewswire.com/dr20151222-wifi-signals-can-be-used-to-detect-attackers

Dec 22 – **Physical attacks on devices connected to the Internet can be detected by analyzing WiFi signals, computer scientists have discovered.**

Wireless devices are increasingly used for critical roles, such as security systems or industrial plant automation. Although wireless transmissions can be encrypted to protect transmitted data, it is hard to determine whether a device — such as a wirelessly connected security camera protecting critical buildings in airports or power stations — has been tampered with. **An attacker may simply rotate a camera's view away from the area it is guarding without triggering an alert.**

Wi-fi signals discovered at this "inactive" RAF building // Source: commons.wikimedia.org

Lancaster U reports that in their study, researchers at Lancaster University have created a method that analyzes WiFi signals at multiple receivers to detect physical attacks. A change in the pattern of wireless signals — known as Channel State Information (CSI) — picked up by the receivers can indicate a tamper situation. The algorithm detects attacks despite signal noise caused by natural changes to the environment such as people walking through the communication paths.

Dr. Utz Roedig, Reader in Lancaster University's School of Computing and Communications and one of the report's authors, said: "A large number of Internet of Things systems are using WiFi and many of these require a high level of security. This technique gives us a new way to introduce an additional layer of defense into our communication systems. Given that we use these systems around critically important infrastructure this additional protection is vital."

— Read more in Ibrahim Ethem Bagci et al., ""Using Channel State Information for Tamper Detection in the Internet of Things," Proceedings of the 31st Annual Computer Security Applications Conference (7 December 2015): 131-40.

The Blacksmith, the Nail, the Horse and Disaster Prevention

By Luiz Hargreaves

Source: http://www.experts.com/Articles/Disaster-Prevention-Blacksmith-Nail-Horse-By-Luiz-Hargreaves#.VnYW0V0CMgM.linkedin

"For want of a nail the shoe was lost, for want of a shoe the horse was lost; and for want of a horse the rider was lost; being overtaken and slain by the enemy, all for want of care about a horse-shoe nail."

Benjamin Frankilin

The proverb above has received different versions, including this one credited to Benjamin Franklin. A kingdom lost because of

a nail. We could also say, a disaster caused by a simple problem that could have been avoided.

Everybody that works with accident prevention knows that the great tragedies, with rare exceptions, are not the result of a single event, but a succession of failures. Lack of planning and risk identification, mitigation, failure in monitoring, lack of warning and alarm systems, little or no training. These are just some examples of "nails and horseshoes" capable of destroying the kingdom, just like the proverb.

There is no zero risk, there is no effective prevention without the commitment of everyone, including the community. It is not possible to identify risks, without knowledge of the threats and vulnerabilities and there is no adequate response, without prevention and preparedness. If misplaced "nails and horseshoes" start the sequence which can result in a disaster, whose responsibility is it to act as a blacksmith? The answer might be complex, but in few words, we can say that we are all responsible. The citizen cannot fail to assume their responsibility to drive carefully, to obey the law, not to put the lives of others at risk and act in such a way to benefit the community. When someone builds a home in a risky area for natural disasters, he is not just leaving his family vulnerable, but is also encouraging others to do the same and contributing to the sequence of events that will end in disaster.

The authorities cannot expect that the community exerts the role of agent for prevention and preparedness without support. It is essential that Government be prepared with planning, material and human resources, to operate in mitigation and in all phases of disasters. If the "horseshoe" is misplaced, the state cannot allow that these "horses" remain in battle, as it will be lost.

In many countries, it is usual that Government still invests little or almost nothing in response and prevention. Sometimes it is a cultural issue, but at the same time, the social responsibility is neglected and resources that should be used to protect the population are intended for investment in works and actions that are clearly focused on electoral goals or even corruption.

Treating "injured horses and riders" has much greater visual impact than fixing "nails in horseshoes". The relief arrives for victims, brought by the same hands of those who were unable to prevent the disaster, or worse, by their perpetrators. The image that is shown, however, is that they are the great rescuers.

"Nails and horseshoes" are set every day, every moment. "Horses and riders" toppled all the times. Disasters are the result.

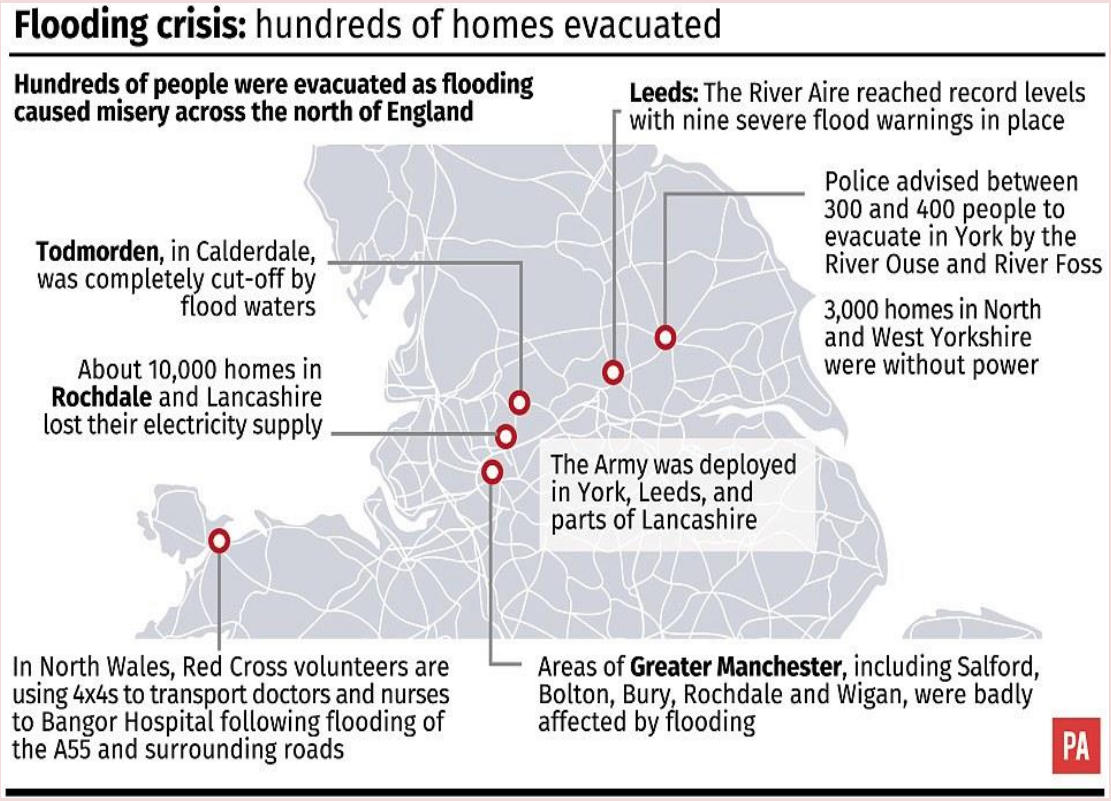
Naturally, even with all the prevention, preparedness and response performed adequately,

the unthinkable can happen. But this should be the exception and not the rule.

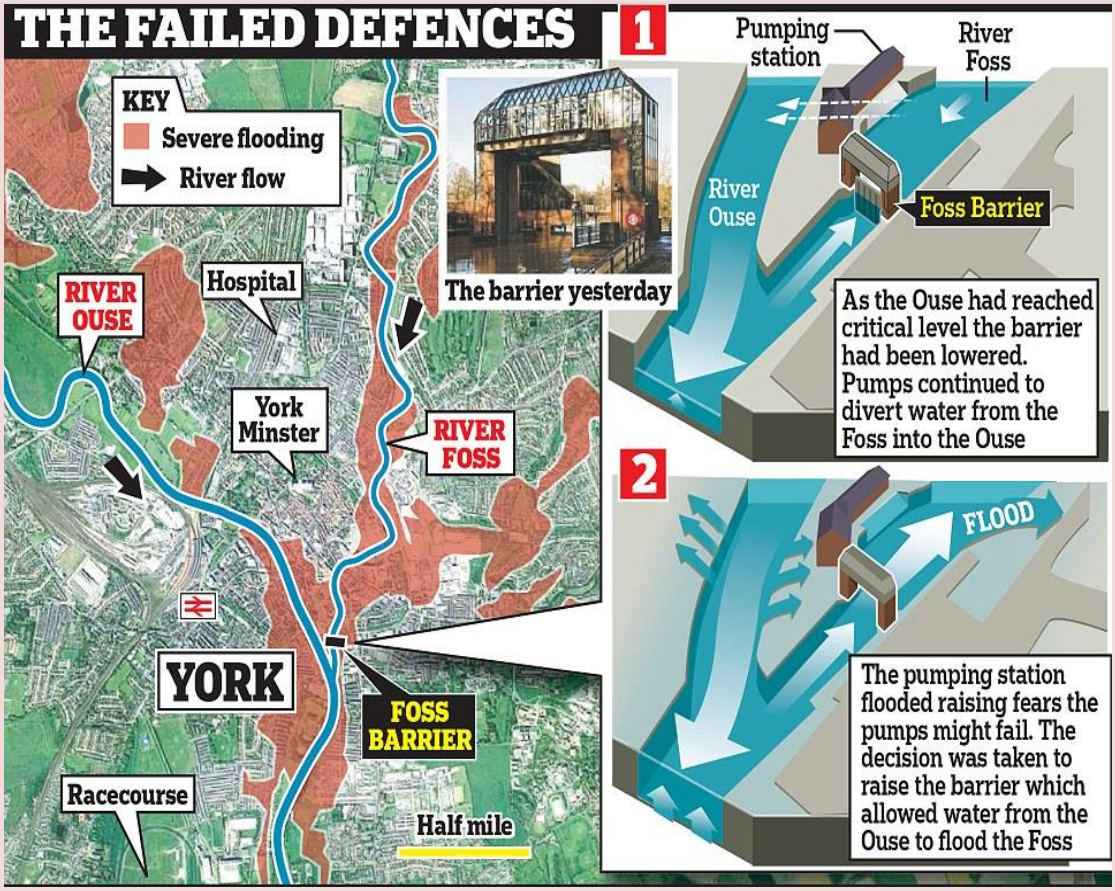
Luiz Hargreaves, AAS, MD, MS, MA is a Brazilian qualified Expert in Crisis Management and Disaster Preparedness. He has been working in these fields for more than 30 years, with a large experience in major events, counterterrorism, disaster prevention and emergency planning.

Engulfed by a Christmas catastrophe: Full scale of flood chaos is revealed as army work round-the-clock to rescue victims and begin airdropping provisions

Source: http://www.dailymail.co.uk/news/article-3376073/Pictured-Soldiers-collapsed-exhaustion-working-help-swamped-residents-flood-hit-communities-PM-puts-1-000-troops-standby-rain-way.html



- **Prime Minister David Cameron is expected to visit some of the worst-affected areas in the north of England today**
- **500 troops have already been scrambled to help flooding victims while 1,000 additional soldiers remain on standby**
- **Thousands of people have been evacuated from their homes in Yorkshire after rivers breached flood defences**
- **Forecasters warn another band of rain will sweep across flood-hit north on Wednesday, bringing further misery**
- **Dozens of 'danger to life' flood warnings remain in place today and thousands of properties are still without power**
- **Judith Blake, the leader of Leeds City Council, claims more was done to help flooding in the south than in the north**



The flood barrier gate on the River Foss in York was raised after water entered the flood defence's main building. It was feared that if the electrics stopped working, the Environment Agency would not have been able to pump water out of the town – putting more lives at risk

Assessing the damage: Prime Minister David Cameron visited some of the worst flood-hit areas in York today to offer his sympathy

Exhausted: The troops from the 2nd Battalion Duke of Lancaster's Regiment have been working around-the-clock to help rescue residents from their flooded homes. More than 500 Army troops have already been scrambled to help and another 1,000 soldiers remain on standby

EDITOR'S COMMENT: Why always citizen's "maids" – the military? Just for the opportunity of a "selfie"? I cannot see citizens gathering sand sacks to defend from rising waters. Why? No comment on River Foos barrier main building…

U.K. government rejected flood warnings from own advisers

Source: http://www.homelandsecuritynewswire.com/dr20151228-u-k-government-rejected-flood-warnings-from-own-advisers

Dec 28 – **Critics charge that the U.K. government was warned by both the government's own climate change experts and outside consultants that there was a need to take urgent action to protect the increasing number areas in Britain which are becoming susceptible to flooding, but that the government rejected the advice.**

The *Independent* reports that the decision not to develop and implement a comprehensive strategy to tackle to growing risks of flooding was made in October – only a few weeks before the flooding in Cumbria before Christmas and the most recent flooding in Lancashire and Yorkshire.

Chancellor of the Exchequer George Osborne, in the wake of the devastation of the last few days in Cumbria, announced a £50 million repair fund for those whose property had been damaged, but expert note that the cost of clearing up the most recent flooding effecting in both Leeds and York would be much higher.

The Committee on Climate Change (CCC) said that Prime Minister David Cameron's promised to have a flood strategy developed, but that the government had failed to learn lessons from the widespread flooding in 2013/14.

Six months ago, in June, the CCC issued a report analyzing the progress toward tackling the consequences of climate change, in which it pointedly noted that the government's most serious failing was the way it had dealt – or, rather, failed to deal – with floods caused by extreme weather.

"Plans and policies, or progress in addressing vulnerabilities, are lacking," the CCC said.

The CCC recommended that the government should "develop a strategy to address the increasing number of homes in areas of high flood risk."

In response to the CCC harsh report, the government, in October, replied: "We believe that a strategy to address future residual risk would not be appropriate at this time."

Daniel Johns, the CCC's head of adaptation told the *Guardian*: "The CCC made a very clear recommendation in its statutory advice, but the government rejected it.

"But the government has no strategy to address this residual risk."

A government spokeswoman told the *Independent*: "This government has been clear on its commitment to climate change action and we are pushing for an ambitious global deal in Paris as well as driving innovation to build a low-carbon economy. We are also investing £2.3 billion over the next six years to better protect 300,000 homes. The Environment Agency's figures take account of climate change and show that this investment will reduce flood risk."

U.K.: Economic costs from flooding could reach £1.5bn, reduce GDP growth

Source: http://www.homelandsecuritynewswire.com/dr20151228-u-k-economic-costs-from-flooding-could-reach-1-5bn-reduce-gdp-growth

Dec 28 – **Economic losses caused by the flooding which has devastated parts of Britain in the past few days could exceed £1.5 billion, experts believe.**

The accounting firm PwC said that insurers will likely shoulder the bulk of the burden after first Storm Desmond and then Storm Eva saw waters swamp large swathes of the country.

PwC's Mohammad Khan told the *Telegraph* that, "We would give a very initial estimate of economic losses of between £900 million and £1.3 billion, with the insurance industry bearing between £700 million to £1 billion of this.

"If rain continues to fall in large quantities, and the areas with warnings in place do indeed flood significantly, it could well be that the total economic losses could breach £1.5 billion with an additional significant increase in insurer losses from our initial estimate."

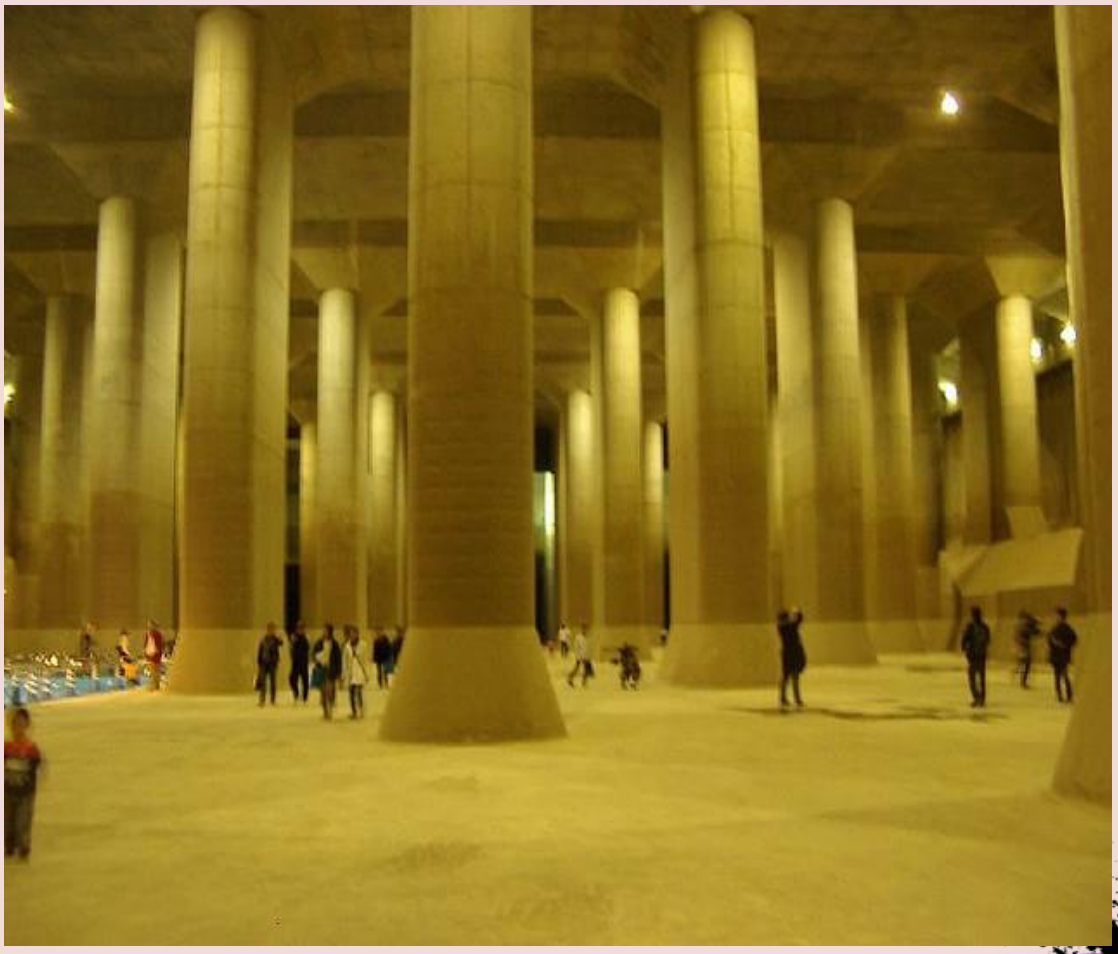
Howard Archer, chief U.K. and European economist at IHS Global Insight, said the floods could also hamper wider economic growth.

He said: "The floods could well shave 0.2-0.3 percent off GDP growth overall in the quarter that it occurs in terms of businesses not being able to open, loss of agricultural output, people not being able to get to the shops, travel, etc.

"There is also the cost to insurance companies. There is also the loss of work from those people not actually able to get to work," he told the *Telegraph.*

Arrangements have been made to put in place emergency financial assistance for areas affected by the floods. Homes and businesses damaged by flooding caused by Eva will have access to the same package of support announced for those affected by Storm Desmond.

EDITOR'S COMMENT: The UK gov did not listen to climate change experts and now is paying the price. Why is it so difficult to high officials to understand that preparedness costs less than mitigation and restoration of community in the aftermath of a disaster? Why we should always hear that the "catastrophe was beyond imagination"? – and alike. Why we are not planning based on the worst scenario instead of making plans for just some extra rain, snow, wind or higher temperatures? Why don't we let bright minds to unfold their ideas and incorporate them into our civil defenses? Readers of the Newsletter might remember a proposal to connect rivers or create new ones. I was reading the other time about how Japanese constructed a 2 billion USD underground huge flood tunnel (G-Cans Project) in Tokyo (photos below) than can absorb huge amounts of surface city waters. When people will realize that Nature is almost impossible to defeat?



The two aspects of life

Dec 31 – Address Downtown Dubai Hotel megafire (left) a few moments before the beginning of festivities for the New Year 2016 with epicenter the nearby Burj Khalifa skyscraper.

Fire crews finish the job in Dubai hotel blaze

Source: http://www.thenational.ae/uae/fire-crews-finish-the-job-in-dubai-hotel-blaze

Jan 01, 2016 – Firefighters worked to contain small pockets of fire at The Address Downtown Dubai hotel yesterday after Thursday night's blaze engulfed the 63-storey building.

Civil Defence workers perched on a ladder and trained jets of water at the flames, and teams inside the hotel checked sections of the structure where 16 people were injured on New Year's Eve.

Plumes of dark smoke poured from the building yesterday morning while flames were seen in the lower part of the building in the afternoon.

On his Twitter account, **Sheikh Mohammed bin Rashid, Vice President and Ruler of Dubai, praised the emirate's fire teams in fighting the New Year blaze: "Proud of our police, civil defence and ambulance services. You demonstrated best in world capabilities last night."**

Royalty also played its part in the operation itself. State news agency Wam reported that Sheikh Saif bin Zayed, Minister of Interior and Deputy Prime Minister, helped supervise the operation to put out the blaze. Sheikh Mansoor bin Mohammed, son of the Ruler of Dubai, was photographed at the scene in a firefighter's uniform.

Officials said yesterday they were trying to ascertain the cause of the fire.

The area surrounding the Dubai Fountain was blocked off and crowds of shoppers inside Dubai Mall were prevented by security guards from entering the outdoor zones.

"Sometimes it happens that the fire continues to burn because of air pockets," said a civil defence official, who explained the sporadic fires yesterday.

Earlier yesterday, flames ripped through the glass facade along the building's rim on the eighth floor and large chunks of debris fell as a fire burned on the 20th floor, where the blaze reportedly began at 9.30pm on Thursday.

More than 40 vehicles from Dubai Police and the civil defence were at the scene and a one-kilometre stretch of the Sheikh Mohammed bin Rashid Boulevard was blocked to traffic.

The Dubai Civil Defence team was joined by a German squad, which specialise in fighting tower blazes, from Abu Dhabi.

Given the intensity of the fire and the speed with which it spread, the building was evacuated with calm efficiency.

The broad efforts were coordinated by the Crisis and Disaster Management Committee, headed by Maj Gen Khamis Al Muzainah, commander general of Dubai Police.

He told state news agency Wam that 15 people suffered "light to moderate injuries" and there was a heart attack.

"All injured were moved to hospital and discharged later after receiving medical care, except for the cases of a pregnant woman and an elderly man, whose conditions are stable," he said.

Gas lines to nearby restaurants were shut down as a precaution. Some restaurants across the road from the hotel were shut at breakfast but opened from lunch onwards.

"All our guests were evacuated last night for safety reasons," said Thaer, the owner of an Arabic restaurant opposite the hotel.

"Restaurants on the boulevard were cleared and people were evacuated quickly. It was terrible that this happened."

Hotel guests and employees were safely evacuated, said a spokeswoman of The Address.

"An investigation is ongoing and details will be provided once they are ascertained."

The hotel said it had set up a hotline for guests affected by the fire and was working to provide them alternative accommodation across the city.

EDITOR'S COMMENT: A very difficult operation ideally ideally executed by Dubai's First Responders! Well done! A solid proof that preparedness and training always pay back! Now we will wait for the report on the causes of mega-fire and hope that results will not dislose any connection between the ownership of the tower with evil minds! Strong decision from the Royalties to proceed with the New Years' festivities based on confidence to their own people!

Floods, earthquakes, wildfires and heat waves: the worst natural disasters of 2015

2015 proved deadly for many people around the world

Source: http://www.cbc.ca/news/world/year-end-2015-natural-disasters-1.3346639

Dec 30 – Floods, cyclones, wildfires, heat waves, earthquakes and landslides made 2015 a devastating year for a lot of people around the world. We take a look at some of the worst natural disasters of the past year.

January 2015

Flooding in southeastern Africa

Unusually heavy rains hit Malawi and caused widespread flooding, leaving 200 people dead or missing and 120,000 forced from their homes, according to UNICEF. The aid agency said it was "a race against time" to reach displaced communities, as stagnant water and poor sanitation threatened to kill children in one of the poorest countries in southern Africa. In neighbouring Mozambique, the rains caused extreme flooding of river basins and cut off communities. Twenty-five people were reportedly killed in that country.

March 2015

Cyclone Pam rips through Vanuatu

Winds of 270 kilometres an hour tore through the 65-island South Pacific archipelago, home to about 267,000 people. One of the heavily damaged areas was the capital, Port Vila, where 47,000 people live. The destruction was even worse on the outer island of Tanna, where the Australian military estimated about 80 per cent of the buildings were flattened, and the hospital and airport were damaged. To complicate matters, the island's remote location made it difficult for rescuers to get through. Throughout Vanuatu, an estimated 11 people were killed and thousands were left homeless.

April 2015

Deadly earthquake devastates Nepal

On April 25, a 7.8 magnitude earthquake left more than 8,000 people dead in Nepal and turned much of the country, including the capital, Kathmandu, into a disaster zone.

The earthquake triggered an avalanche on Mount Everest that killed 19 climbers. About three weeks later, a 7.3 magnitude earthquake rocked Nepal again, killing dozens more people, injuring hundreds and terrifying the country's citizens just as they were trying to rebuild from the first disaster.

May/June 2015

Heat waves kill thousands in India and Pakistan

By the end of May, about 2,200 people in India were dead from a raging heat wave that began in April. Temperatures went up to 47 C. Most of the people killed were in Andhra Pradesh and Telangana states in the southern part of the country.

In June, the worst heat wave in at least a decade hit southern Pakistan, particularly the port city of Karachi. More than 830 people died as temperatures reached as high as 45 C. Karachi's inefficient power grid and shortage of potable water were blamed for worsening the situation. On the worst days, people in the city of 20 million tried to get water from broken pipes.

July 2015

Flash floods hit Pakistan

Triggered by monsoon rains, flash floods killed more than 100 people in various parts of Pakistan and left tens of thousands homeless, according to the country's National Disaster Management Authority. More than 2,000 villages were flooded.

Almost 3,000 homes collapsed or suffered damage. In the northwestern city of Chitral, homes, mosques, hotels, bridges and a power station were destroyed.

Wildfires force largest evacuation in Saskatchewan's history

Hot weather, very dry conditions and lightning strikes contributed to hundreds of wildfires in western Canada during the summer of 2015. In Saskatchewan, more than 13,000 people were forced from their homes in the largest evacuation effort in the province's history. The Canadian military was dispatched to help in the hard-hit La Ronge area, about 380 kilometres north of Saskatoon.

The increased wildfire activity in 2015 — and the ballooning firefighting costs — prompted Saskatchewan Premier Brad Wall and B.C. Premier Christy Clark to call for a national forest fire plan by next year.

September 2015

California wildfires

California suffered one of its worst forest fire seasons on record in 2015 as wildfires raged in northern

parts of the state. One fire, north of San Francisco, was the fourth-worst blaze in California's history, with three people killed and more than 1,000 homes destroyed.

A separate fire in the Sierra Nevada foothills killed two people and ruined more than 500 homes. A volunteer firefighter lost his own home while out battling blazes. Thousands of people were evacuated from dozens of communities. According to the Cal Fire website, there were more than 6,200 wildfires throughout the state in 2015, burning about 125,000 hectares of land. Compare that to 2014, when Cal Fire documented about 4,200 wildfires that burned about 77,000 hectares.

Chile earthquake

On Sept. 16, an 8.3 magnitude earthquake killed 11 people in central Chile and triggered tsunami warnings as far away as Hawaii and California. More than one million people fled their homes and waves up to 4.5 metres high slammed into Chile's northern port city of Coquimbo, washing large fishing boats up onto the streets.

Still, many people who remember the devastating 8.8. Magnitude quake of 2010, which caused a massive tsunami and killed more than 500 people, were relieved the death toll and destruction wasn't worse. When September's earthquake struck, the Chilean government ordered evacuations from coastal areas and said it had learned from previous disasters.

Japan floods

Heavy rain after Tropical Storm Etau pummelled Japan in September and triggered huge floods, forcing thousands of people from their homes. When the Kinugawa River broke through a flood berm in Joso near Tokyo, it washed away entire houses and left hundreds of people stranded. Many waited on rooftops to be rescued.

October 2015

U.S. floods

U.S. President Barack Obama declared a state of emergency after Hurricane Joaquin-related storms slammed South Carolina with floods. Streets and roads turned into rivers, leaving many people trapped in their cars. A dozen people died of weather-related causes in South Carolina and neighbouring North Carolina.

One woman died when her SUV was swept away by floodwaters; another man drowned after he drove around a barricade. A transportation worker was also among those killed. South Carolina Governor Nikki Haley said 550 roads and bridges had to be closed across the state.

November 2015

Deadly Australian wildfires

Four people were killed and hundreds of homes were evacuated as wildfires raged across southwest Australia in November. Fierce winds and a heat wave were blamed for making the fires worse as firefighters tried to contain them. November is summertime in the southern hemisphere, and wildfires are common across much of Australia during the season.

Burma landslide

On Nov. 21, a landslide in Burma, also known as Myanmar, killed more than 100 people when a 60-metre high mountain of dirt discarded by mining companies collapsed. The disaster happened in the mining community of Hpakant in the jade-rich northern part of the country.

At first, officials said the dead were mostly men picking through the mining waste looking for jade to sell — a common occurrence in the extremely poor town. Later, they said the landslide happened in the middle of the night and buried more than 70 makeshift huts where the miners slept.

December 2015

Chennai floods after heaviest rainfall in 100 years

Massive floods in India drove thousands of people from their homes in December after the heaviest rainfall in more than a century hit the state of Tamil Nadu. More than 250 people died — some by electrocution before authorities turned power off in some areas.

Vast swaths of Chennai — India's fourth-largest city — were under up to three metres of water. Homes and cars were submerged, and people escaped their homes using ladders or jumping out windows onto makeshift rafts.

Encouraging innovation in first responder tech

Source: https://www.crisis-response.com/comment/blogpost.php?post=185

First responders face many challenges in the field: disasters impair communication between responders, create situations where it is difficult for them to see or hear, and make it difficult to collect information about the current status of the disaster. In order to help solve these and other challenges, the US Homeland Security's Science and Technology division has created the EMERGE Accelerator Programme for Wearable Tech for First Responders (EMERGE).

The EMERGE accelerator is aimed at entrepreneurs who have developed innovative ideas that address the needs of first responders. With two partner companies, Tech Wildcatters and TechNexus, EMERGE helps these entrepreneurs further develop their products and start investable companies by providing mentorship, early market validation, and access to private investment.

Selected from roughly a hundred candidates, more than a dozen firms are participating in the EMERGE accelerator this year. Their ideas range from a triage language translator, to a robotic environmental sensor ball, to a power-harvesting system for mobile devices. A few of these innovative ideas are profiled below.

Mindtalk Technology uses bone conduction technology in mouth guards to allow firefighters, SWAT teams, the Coast Guard, and others to be able to communicate with each other in extremely loud environments where headphones won't work and outer ear protection is necessary. Originally developed to allow athletes to listen to MP3s and receive radio communication, the mouth guards will be extremely useful in maintaining communication between first responders in critical situations.

Select Engineering Services' Automated Injury Detection System is the first wearable active sensor technology with the ability to automatically summon help without human assistance. It can send notifications when a first responder in injured – even if they cannot send these notifications themselves – which would increase response times and save first responders' lives.

The TeleSense Sensor Ball can be rolled into hazardous situations ahead of first responders to get a complete picture of the environmental conditions they are facing in real-time. This allows first responders to stay safe and to

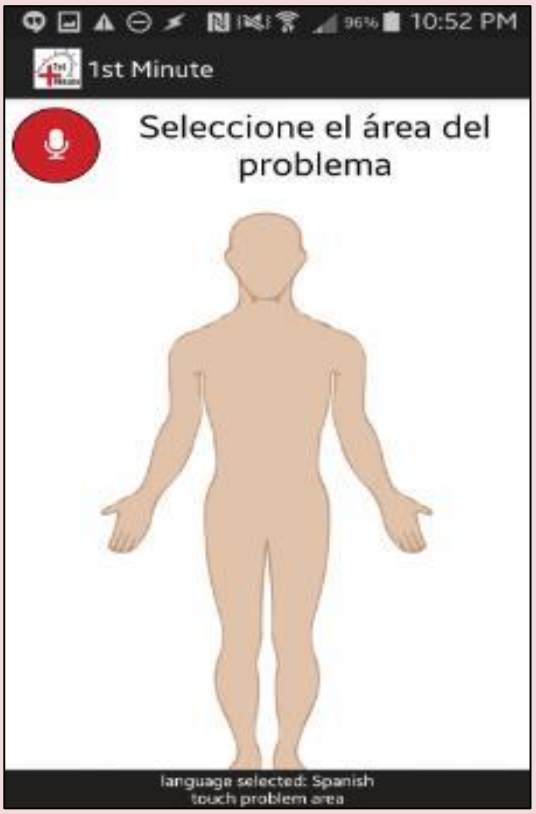
make smart, informed decisions about the best course of action.

Pivothead Wearable Imaging is innovative camera eyewear that has the ability to live broadcast exactly what the wearer is seeing. In disaster situations, this would enable a first responder to show other members of the response team what the situation is, and to receive relevant advice and insights from their superiors or other team members. Such footage would also help decisions makers in the disaster response better understand the actual situation in real time, enabling faster and more informed

decisions.

International Thermodyne's PhelTex (previously called PowerFelt) captures energy from heat and motion, and converts it into electricity. The innovative cloth-like material – whose flexibility and thinness opens up a wide variety of applications – is able to capture both heat and motion energy that occur naturally in our environment. In addition to being able to extend the battery life of portable electronics, the material can also act as a heating or cooling device on demand. This would allow first responders to charge their communication devices and have clothing or blankets that keep them warm or cool depending on what the situation requires.

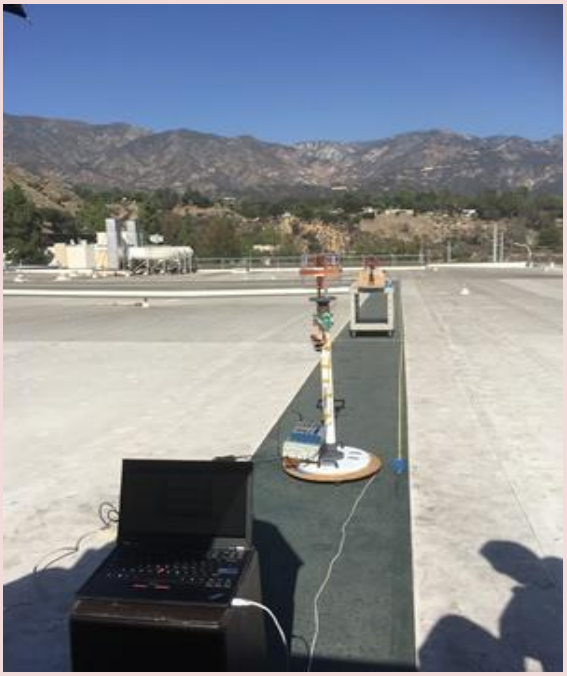
LanguageMAPS' 1st Minute App is designed to help first responders overcome language barriers when treating injured people in an emergency. A language barrier causes first responders to miss key



information, like pain location and severity, medical history, allergies, or medications. LanguageMAPS' app allows first responders to get this essential information so they can provide appropriate treatment.

Precisely pinpointing first responder locations

Source: http://www.homelandsecuritynewswire.com/dr20160106-precisely-pinpointing-first-responder-locations



Jan 06 – When firefighters rush into a burning building, it is essential that they and their operations team know their precise locations at all times. Even with global positioning systems (GPS) and other tracking technologies, environmental conditions, obstructions and interference from the building materials can severely limit pinpointing them. In the event of an injury, search teams rely on communications systems to rescue these first responders. DHS Science and Technology Directorate (S&T) says it is developing a new system, known as the **Precision Outdoor and Indoor Navigation and Tracking for Emergency Responders (POINTER)** to help tackle this challenge.

"This technology is critical to ensuring the safety of our first responders. In the event that they lose communication with their

command unit, we will be able to pinpoint locations as close as three feet," said Deputy Under-Secretary for Science and Technology Dr. Robert Griffin, a former firefighter. "Besides assisting the first responder community, we could use this technology for a variety of response capabilities, such as a mine collapse to pinpoint the exact location of trapped individuals."

S&T partnered with National Aeronautics and Space Administration (NASA) Jet Propulsion Lab (JPL) to begin development of POINTER in 2014. Recently, S&T conducted testing which determined that the technology is reliable with a margin of error of less than three feet. This would allow rescue workers to determine the specific location of a first responder who is wearing the transmitter. The next step for testing involves a three dimensional tracking capability, allowing the system to identify both the location and floor the responder is on.

"A locator device that can pinpoint someone within one meter or less of their actual location is critical to keeping our first responders safe. We are very close to achieving that with our POINTER system," said S&T's First Responders Group Director of Responder Technologies Greg Price.

Traditional locator devices use GPS, inertial measurement units and other technologies. POINTER sets itself apart by using low-frequency magnetic fields that can transmit signals through any building materials.

"POINTER uses a system of electrically-small magnetic field loops to generate a field of energy that can penetrate most material," said Price.

The responder wears a small transmitter — which sends location information to a receiver and ultimately a base station or command post. S&T notes that during field trials, POINTER was tested rigorously in structures that simulated the type of environments first responders' work in. The technology will go through additional field trials in the spring of 2016. The technology is expected to be transitioned to commercial use in 2017.

America, Wake Up: Harden Your Soft Targets

By Vincent J. Bove

Source: https://www.linkedin.com/pulse/america-wake-up-harden-your-soft-targets-vincent-j-bove-cpp

Jan 06 – **Law enforcement, military, and private security professionals refer to two types of targets for individuals with violent intentions. These are commonly understood as hard and soft targets.**

Security must be assessed and enhanced at both, as these are violent times throughout the world and here in America.

Hard Targets

Hard targets have numerous layers of protection including physical, personnel, procedural, and cybersecurity.

These are normally more challenging to compromise because they are fortified with countermeasures of layers of protection, or defense in depth.

Hard targets include military bases, embassies, and numerous high-risk government facilities.

Although attacks on hard targets are more difficult, there have been breaches of security that have included the 1998 U.S. embassy bombings in which over 200 people were killed in two East African cities. Another was the 2012 Benghazi attack with killings by militant extremists of a U.S. Ambassador, U.S. Foreign Service Officer, and two CIA contractors.

Security with hard targets must always be enhanced and vigilance maintained. The reality is that there are individuals making sophisticated and unprecedented plans to exploit vulnerabilities.

Soft Targets

Soft targets are much easier to compromise and are normally understood as places full of ordinary people, as opposed to a military base.

There are soft targets throughout society that include trains, subways, museums, hospitals, corporations, schools, colleges, restaurants, hotels, shopping malls, houses of worship, transportation terminals, cultural sites, financial institutions, and sporting events.

Law enforcement and private security, along with the general public must be vigilant together to prevent attacks. Any attack on a soft target can have catastrophic impact on civilians, police, and first responders, as well as to the morale of the nation.

Acts of violence, including the accelerating incidents of terrorism throughout the world, must motivate us to not only enhance security of hard targets, but harden soft targets as well.

Public, Private, Citizen Collaboration

As one walks the streets of our great cities, the vigilant presence of dedicated police officers protecting us must be appreciated.

The vigilance of the NYPD must be recognized, not only with their presence throughout the city with special events, but with uniformed officers walking the beat, and with highly-trained and heavily-armed units.

But the NYPD and any police department in America, cannot do it alone. There must always be collaboration between the police, private security, and citizens.

There can be an attempted attack anytime, anyplace, and by any means and all of us must be aware of our surroundings, and work together to protect one another.

Hardening Soft Targets

In my article titled "Mass Shootings: America's Public Health Crisis," published in the Dec. 10, 2015 edition of the Epoch Times, I argued that "a robust security program must be comprehensive, proactive, and continually updated. Security must never be piecemeal, negligent, or have its importance minimized."

In the article, I presented basic security countermeasures to prevent violence, applicable to hardening soft targets. These include security vulnerability assessments, background checks/investigations, training, warning signs, physical/personnel/procedural security, and cybersecurity.

Complementing these basic security principles is the importance of private security partnerships with law enforcement as exemplified by the NYPD SHIELD program. This is America's public-private collaboration model dedicated to protecting New York City through information sharing.

Enhancing Private Security Professionals

Private security must honestly evaluate its services in light of unprecedented violence unleashed throughout America to prevent future tragedies.

This review must include background and criminal records checks for all security personnel-both contractual and in-house-ongoing training initiatives exceeding legal requirements, and certifications that exceed the status quo.

Also, the implementation of critical response private security personnel demands serious consideration to harden high-profile soft targets. This is the new reality of private security-certified, licensed, and experienced armed security personnel-in highly visible tactical gear, serving as a deterrent and with experience to respond to any crisis. These individuals should have either law enforcement or military experience with specialty units, such as SWAT (special weapons and tactics teams) or emergency services.

There are ready, willing, and able professionals ready to harden soft targets with critical response programs. America must not have its head in the sand, oblivious to the war drums of violence that demands vigilant countermeasures.

The realities of violence demand that we are proactive, rather than reactive, and do everything necessary to harden our soft targets. Private security must be on the cutting edge-implementing new countermeasures, protocols, and initiatives- and seeing things with a new set of eyes.

Final Reflections

These are challenging times for police, private security, and citizens, but we must rise to the occasion to prevent all acts of violence with an unwavering dedication to collaboration.

America, to be forewarned is to be forearmed, and without haste; harden your soft targets.

Vincent Bove *CPP, is considered one of the foremost national experts on school and workplace violence prevention, specializing in facility protection, evacuations, terrorism prevention, and leadership training for law enforcement personnel, bringing him the support, respect, and energy of his peers in the law enforcement community.*

Redirected flood waters leading to unintended consequences

Source: http://www.homelandsecuritynewswire.com/dr20160107-redirected-flood-waters-leading-to-unintended-consequences

Jan 07 – An intricate system of basins, channels, and levees called the Headwaters Diversion carries water from the eastern Missouri Ozark Plateau to the Mississippi River south of Cape Girardeau. The system protects 1.2 million acres of agricultural lands in southeast Missouri from both overflow from the Mississippi River during flooding events and from Ozark Plateau runoff. Historical and more recent extensive rainfall and subsequent flooding prompted University of Illinois researcher Ken Olson to look more closely at

where the excess or diverted water goes.

"There is a need for additional floodwater storage in the confluence area of the greater Ohio-Mississippi Rivers," says Olson. "A regional effort on both sides of the Ohio and Mississippi Rivers is needed to strategically identify floodplain areas that could provide temporary water storage and policy incentives for landowners of low-lying lands to profitably invest in crops and income alternatives."

U of I reports that Olson and his colleagues are studying the levees, diversions, and floodways, which for the past 200 years have allowed land conversion from wetlands to agriculture. "It has substantively altered the hydrologic cycle of the region," he says. "The Little River levee and Little River Drainage District Headwaters Diversion channel built in the 1910s successfully permitted the drainage of the 1.2 million acres Big Swamp in southeast Missouri. However, it also had the unintended consequence of increasing the peak flow of Mississippi River water south of Cape Girardeau through the Thebes gap and south to Helena, Arkansas, a distance of approximately 360 river miles.

"When the Ozark uplands and Francois Mountains experience above-average rainfall for extended periods of time, the additional runoff transported by the diversion channel increases the chances of Mississippi River levee breaches south of Commerce, Missouri, and adds to the peak river height at the confluence of the Ohio and Mississippi rivers."

Olson says the increase in Mississippi River peak flow placed additional river pressure on levees and led to increased flooding, especially during the floods of 1927, 1937, 2011, and 2015-2016.

"The Kentucky, Illinois, and Missouri farmers' and land owners' response to the additional volume and height of the Mississippi River from the diversion channel valley and the prevention of the Mississippi River floodwaters from flowing into the ancient Mississippi River valley and Big Swamp was to build floodwalls and levees," Olson says.

After the 1915 flood, Cape Girardeau built a floodwall to protect the city. Likewise, after the Great Flood of 1927, Cairo built a floodwall, strengthened levees, and created the Birds Point-New Madrid floodway. Missouri farmers built the Commerce Farmer levee that failed in 2011. Kentucky farmers built the Hickman levee — strengthened later by USACE — and did not fail.

"Illinois farmers built the Fayville-Len Small levee that breached in 1993 and 2011," Olson says. "It breached a third time on Jan. 2, 2016, when the Thebes river gage reached a record 47.7 feet –14.7 feet above flood stage. As of Jan. 5, the farmland, homes, and

roads were still under floodwaters."

Olson says climate scientists predict a continued pattern of extreme rainfall events in the upper Mississippi River region. "This suggests that unexpected above average rainfall events in the Ohio and Mississippi River basins will continue to increase the frequency of extreme flooding events on these Great Rivers."

Olson is a researcher in the Department of Natural Resources and Environmental Sciences in the College of Agricultural, Consumer and Environmental Sciences at the University of Illinois.

— Read more in "Missouri Ozark Plateau Headwaters Diversion engineering feat," Journal of Soil and Water Conservation 71, no. 1 (January-February 2016): 13a-19a.

Ambulances Redirected as Sacramento County's Hospitals Were Swamped

Source: http://www.emergencymgmt.com/health/Ambulances-redirected-Tuesday-night-as-Sacramento-countys-hospitals-were-swamped.html

Jan 07 – On Tuesday evening, as emergency room waiting lists grew longer and longer, the Sacramento County Emergency Medical Services Agency made a game-time decision to enact its Level Two Expanded Emergency protocol to address the uncommon surge in patients.

It was the first time in more than five years that action of this level was required, officials said.

Starting in the early evening, UC Davis Medical Center began experiencing what it called an "extremely high patient volume." Ben Merin, EMS coordinator for the county, said the facility was not alone.

"Every health-care area was really busy yesterday," he said. "It was raining, there were car accidents. Hospitals go through this regularly, there are upticks and slows. Yesterday was just a day when everything came together."

When a facility reports concerns about high volume to the county, as UCD did Tuesday night, EMS can make a decision to put that hospital on diversion. That would mean closing that emergency room to new, noncritical patients, and routing all ambulances carrying noncritical patients to the nearest equipped hospital. Facilities would continue to take critical patients even during high-volume periods, Merin said.

Tuesday night, however, all the local hospitals were so busy that putting UCD on diversion would have just inundated the nearest facility and caused a cascade after that, he said.

Instead, EMS chose to enact the level two plan, which mandates that noncritical patients be evenly distributed throughout all the emergency rooms in the county.

The county told each hospital to enact its surge plans, or individual protocols for handling busy nights. They also took charge at their control center, at UC Davis Medical Center, to keep an eye on how close to capacity each hospital was, Merin said.

Each time a paramedic picked up a patient, he or she called the control center to find out which facility to deliver to in order to keep the patient numbers evenly distributed. Normally, the paramedic would drive the patient to the nearest facility, or a facility of the patient's choosing.

"The hospitals see surges all the time," Merin said. "They manage those surges individually, just fine, all the time. Tuesday night it happened to be enough of the hospitals surging that it had a communitywide impact. So rather than having diversions happening, we enacted protocol to control that."

But even with the even distribution protocol, the high volume was problematic, said Dr. Justin Wagner, medical director of the Sutter Emergency Department, in an email.

"This caused tremendous strain on the other hospitals in Sacramento County, which had to pick up the slack," he said.

The emergency patient distribution method lasted for about four hours, and ended at 9:40 p.m. Tuesday. After that, ambulances returned to delivering patients based on standard protocol.

At UC Davis, eight elective surgeries that had been scheduled for Wednesday were canceled. The emergency department is accepting noncritical patients, but is taking patients transferred from other hospitals only on a limited basis, according to a statement from the medical center.

"As with all other hospitals in the Sacramento area, UC Davis Medical Center is experiencing an extremely high patient volume," the statement said. "UC Davis Medical Center staff are working around the clock to ensure that every patient receives the appropriate level of care during this extraordinary period. Patient safety remains the hospital's No. 1 priority."

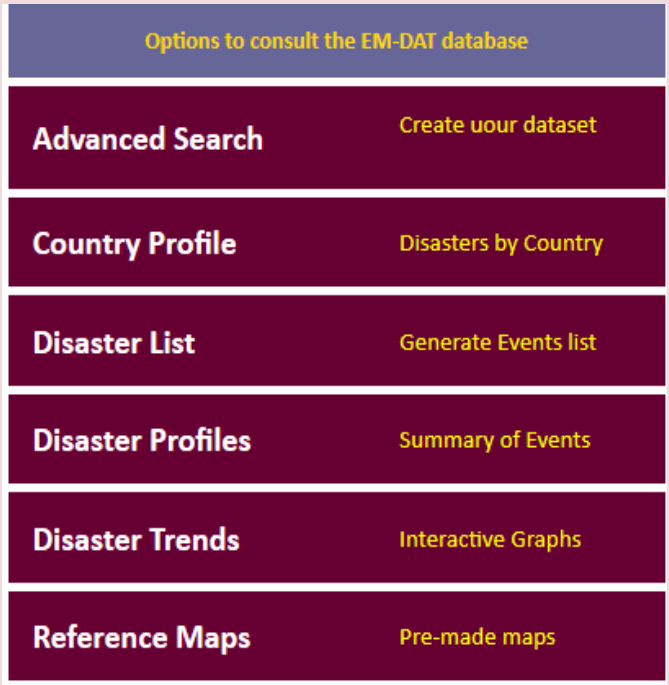
Kaiser Permanente issued a statement Wednesday saying its emergency department was no longer experiencing a surge. Dignity Health did not make representatives available for comment.

Source: http://www.emdat.be/

Development and relief agencies have long recognized the important role played by data and information in mitigating the impacts of disasters on vulnerable populations. Systematic collection and analysis of these data provides invaluable information to governments and agencies in charge of relief and recovery activities. It also aids the integration of health components into development and poverty alleviation programmes.

However, there is a lack of international consensus regarding best practices for collecting these data. Together with the complexity of collecting reliable information, there remains huge variability in definitions, methodologies, tools and sourcing.

CRED has along history of standardized data compilation, validation and analysis. It provides free and open access to its data through its website. One of CRED's core data products is the EM-DAT the International Disaster Database.



EM-DAT provides an objective basis for vulnerability assessment and rational decision-making in disaster situations. For example, it helps policymakers identify disaster types that are most common in a given country and have had significant historical impacts on specific human populations.

In addition to providing information on the human impact of disasters, such as the number of people killed, injured or affected, EM-DAT provides disaster-related economic damage estimates and disaster-specific international aid contributions.

Source: http://www.cedat.be/

The Complex Emergency Database (CE-DAT) is an international initiative that monitors and evaluates the health status of populations affected by complex emergencies.
CE-DAT is managed by the Centre for Research on the Epidemiology of Disasters (CRED) and was created in 2003 as an outcome of SMART, an interagency initiative to encourage rational, evidence-driven humanitarian decision-making.
CE-DAT is a database of mortality and malnutrition rates - the most commonly used public health indicators of the severity of a humanitarian crisis. Field agencies use mortality and nutrition indicators to identify and measure the severity of needs in order to prioritize human and financial resources. These indicators have also been shown to be useful in monitoring the extent to which the relief system is meeting the needs of vulnerable populations and thus the overall impact and effectiveness of the relief system.
Today, **with over 2,000 surveys and 20,000 health indicators,** CE-DAT serves as a unique source of field data for monitoring the health status of conflict-affected populations and for the production of trend analyses, impact briefings and policy recommendations.

CRED Network

CRED

EM-DAT

APHES

MICRODIS

emBRACE

MICROCON

UCLouvain

About CRED
The Centre for Research on the Epidemiology of Disasters (CRED) is based at the School of Public Health of the Université catholique de Louvain in Brussels, Belgium. For over 35 years, CRED has been active in the field of international disaster and conflict health research. It promotes research, training and technical expertise on humanitarian emergencies, with a special focus on public health and epidemiology. Since 1980, CRED has been a World Health Organization Collaborating Centre.
The Centre is actively involved in stimulating debate on the efectiveness of humanitarian interventions. It encourages scientific and policy discussions on existing and potential interventions and their impacts on malnutrition, human survival, morbidity, infectious diseases, and mental health.

The CRED team works in four main areas:
- Natural disasters and their impacts
- Civil conflict and health research
- Database and information support
- Capacity building and training

Overview of natural and man-made disaster risks in the EU
Source: http://www.sos112.si/slo/tdocs/eu_risks_overview.pdf

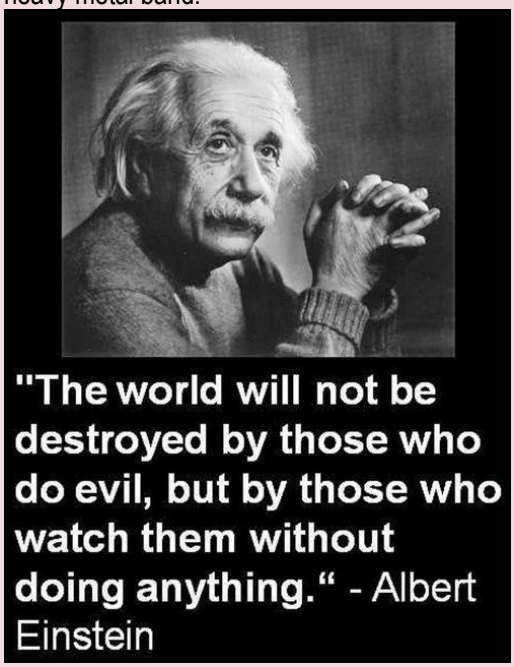
How to plan for workplace terrorism (without causing fear)

By John Leifer

Source: http://www.bizjournals.com/bizjournals/how-to/growth-strategies/2016/01/how-to-plan-for-workplace-terrorism-without.html?page=all

Jan 13 – In the U.S., most acts of domestic terrorism have focused on the workplace, and this makes workplace preparedness a priority. But it's important to plan without inciting unnecessary fear.

It was a routine night for Parisians. Some were enjoying the ambiance of a quiet café, while others rocked to the pounding sounds of a heavy metal band.



As the night wore on, neither group realized that they were minutes away from coming face to face with armed terrorists bent on their extermination.

Within weeks, terror would leapfrog the Atlantic and land squarely in the middle of California, as a married couple in their mid-20s used semiautomatic rifles and handguns to methodically mow down co-workers at a holiday gathering.

Terrorism was, once more, front and center in the minds of Americans, and a familiar question resurfaced: What can be done to protect our citizens?

Most acts of domestic terrorism have focused on the workplace, and this makes workplace preparedness a priority.

In a report called Workplace Preparedness for Terrorism, Dr. Robert Ursano wrote, *"Because most acts of terrorism in the U.S. have occurred where and when people work, and because corporations and the workplace are identified high value targets of international terrorism, it is essential that interventions for preparedness, response and recovery occur in occupational settings."*

So while we may not be able to prevent a terroristic event, we can be vigilant, well-prepared and able to respond to such threats.

Unfortunately, multiple studies have revealed that many companies are ill-prepared.

Despite the fact that preparedness diverts time and resources from other activities, there are overwhelming reasons why businesses must address this issue now.

The Workplace Preparedness for Terrorism Report notes that even at great distances, terrorism can impact the health and well-being of your workforce.

"People exposed to terrorism, whether in close proximity to or far from the affected site, are at increased risk for a range of health-related responses," Ursano wrote.

These responses might include mental illness, distress, or behavior changes.

Without adequate preparation, business continuity may be seriously impaired by terrorist acts. Ready.gov's Project Management page says that according to the Insurance Information Institute, "Up to 40% of businesses affected by a natural or human-caused disaster never reopen."

When businesses suffer, the entire economy can be at risk, as could be seen in the months following the September 11 terrorist attacks on the U.S. Economist Brian Wesbury analyzed the effects of the attacks on the economy. In his article, "September 11: One Year Later," he wrote, *"In September 2001, retail sales fell by $6 billion (2.1 percent); durable goods new orders fell $11.6 billion (6.8 percent); and new claims for un employment surged by 50,000, the biggest monthly jump since August 1982… [in total] the economy shed 1.1 million jobs in the final four months of 2001."*

Failure to prepare for a potential terrorist act may create a liability for business. In Company Primer:

Preparedness and Response Planning for Terrorist and Bioterrorist Attacks, the executive summary explains that terrorism is now considered a foreseeable risk. "In a separate case, the Port Authority of New York and New Jersey was found 'negligent' in safeguarding the World Trade Center before the first terror attack in 1993. The result of these two rulings is that companies can be held liable if they cannot demonstrate that they have taken reasonable actions to prepare for, and respond to, a terrorist attack."

A few basic guidelines can help ensure that you develop an efficient and effective preparedness plan. Begin by carefully selecting the team responsible for the creation, execution, and refinement of the plan. The team should be cross-functional, and represent multiple levels of responsibility within your organization — including senior management.

The team's task is to:

Examine potential areas of vulnerability within your company, and its current state of preparedness.

According to Spencer Williams' article on Ready.gov, Every Business Should Have a Plan, "The specific industry, size and scope of your individual company will determine your organization's risk assessment needs."

Assess and address the operational requirements for your company to maintain business continuity during a period of adversity.

That means examining everything from potential supply chain vulnerabilities to creating redundant payroll, manufacturing, IT, customer service and other core functions at additional locations. It also means securing vital information off-site.

Define emergency response protocols to keep employees, contractors, and others safe.

Identify the most efficient and effective methods for communicating with leadership, employees, and critically important external parties — ranging from customers to first responders.

Educate your employees through ongoing communication about preparedness.

Ensure that a crisis communication plan has been put in place that enumerates how communication with employees and other constituencies will be maintained in the wake of an emergency.

Determine whether your company would be well served to have additional insurance.

Make sure you learn about the costs, coverage, and potential limitations of such insurance.

An essential part of planning is practice

That means drills for your employees on how to execute the key points within the plan. While going through this exercise, it is important to remember that there is a balancing point between preparedness and provoking unnecessary anxiety.

In *Terrorism, The Worker and The City*, Luke Howie wrote, "More than anything, overreacting to terrorism can create workplace stress and anxiety, be detrimental to perceptions of security and safety which can in turn decrease motivation, productivity, and efficiency and subsequently hand terrorists an unnecessary victory."

Few managers are trained to develop detailed preparedness plans. Fortunately, there are abundant resources available on the web to help your business accomplish this objective, including:

- Ready.Gov: Every Business Should Have a Plan.
- Center for the Study of Traumatic Stress: Workplace Preparedness for Terrorism.
- CDC: Emergency Response Resources: Emergency Preparedness for Business.
- Ready.gov: Terrorist Hazards.

James Woolsey, former Director of the CIA, explained the need for terrorism preparedness succinctly: "ISIS, Iran, al Qaeda, and other terrorist organizations are focused on destroying our way of life. We should all recognize their unrelenting focus and determined intent to attack America. Making common sense preparations for a possible attack on our Homeland should be a consideration for all Americans."

Terrorism, by definition, will always provoke fear. But as Thomas Hardy reminds us, "Fear is the mother of foresight."

__John Leifer__ has spent more than 30 years seeking to understand and influence the health care industry as a senior health care executive, consultant, academician and writer. An outspoken advocate for patients' rights, Leifer has published widely on the need for patients to receive appropriate, safe and effective care — including two recent books: "The Myths of Modern Medicine: The Alarming Truth About American Healthcare" and "After You Hear It's Cancer: A Guide to Surviving the Difficult Journey Ahead."

Floods - What Can and Should Be Done?

Source: http://www.drj.com/articles/online-exclusive/floods-what-can-and-should-be-done.html

Jan 11 – A few weeks ago we posted a short column about the flooding in the Southern United States, Northern England and South America. At the time, it was too early to dig into any analysis or review of measures that could have been taken to prepare citizens, communities, organizations and decision-makers of how and what to do to ensure safety and minimize loss.

While there is never a "right time" to discuss, analyze, and debate what could have or should have been done after any disaster, there is now some analysis in the media of what happened and needs to be done to prevent such similar natural disasters from occurring. In today's column, we take a look at some of this discussion and provide you with links to articles from a range of sources related to this most recent natural disaster.

"And that is the shock: that our modern assumptions about safety are punctured by a few days of rain, and so distressingly and violently. We have come to think of ourselves as protected by our tarmac and infrastructure and industrialised life, and the powers of nature – and its dangers – have receded, though only in our assumptions….They think nothing will happen to them, or that nature won't turn against them. But it does. (The Guardian)"

This excerpt from a personal analysis by journalist Rose George of The Guardian, really sums up what so many believe. The idea that we're all safe and secure - until, we're not. The sentiment expressed in this column is of personal experience seeing the flooded urban communities and the people who really had no idea that where was any reason to be concerned from an increase in rainfall, but this unfortunately is also a systemic reaction.

In an article in the Des Moines Register, this frustration with lack of action and the inability to recognize that changes need to be made to protect and prepare people gets straight to the point of what needs to be done.

"The state of Iowa recently received a "C+" grade in the "States at Risk: America's Preparedness Report," a new national analysis that grades states individually on their readiness to address flooding, extreme heat and drought. We can, and need, to do better. The report finds that while Iowa has taken action to address current natural disaster risks, the state needs to increase its awareness of future climate risks and also assess the underlying environmental issues that are causing these disasters to occur more frequently and with greater strength. Until we take an honest look at the underlying cause for increased flooding, we won't be able to avoid these disasters. It's time to take the politics out of environmental issues so we can work toward establishing a statewide plan to address future natural disasters and lessen their frequency and impact. Rural and urban communities in Iowa can work together to address issues and collaborate on ways to manage excessive soil erosion and other sustainable practices to preserve our rich farmland and the communities downstream. Through public and private partnerships, we can find solutions that work for everyone. (Des Moines Register)"

So the question lingers, what is the correct approach? What can be done to ensure that such disasters do not occur again? This is the not the first time that these areas have been hit with foods - so why are people failing to react and respond. In an article from The Independent, journalist Katie Grant has compiled 10 actions that can and should be taken to prevent further flooding. While these are specific

to England, these measures can be implemented anywhere:

1. Introduce better flood warning systems
2. Modify homes and businesses to help them withstand floods
3. Construct buildings above flood levels
4. Tackle climate change
5. Increase spending on flood defences
6. Protect wetlands and introduce/plan trees strategically
7. Restore rivers to their natural courses
8. Introduce water storage areas
9. Improve soil conditions
10. Put up more flood barriers

Now consider recent research by Kounkuey Design Initiative in Kenya of the rampant flooding in Kiberia:

"The team quickly recognized that Nairobi's recent blitz of road construction, which greatly increased the amount of flat surfaces in the region but only included a few drainage channels funneling toward Kibera, was contributing to the flooding. People assume that the flooding problem comes from the river, but to see how much of that comes from the drainage — this data brings to light so many problems that wouldn't be intuitive," Odbert says.

Odbert says the robust data sets and resulting detailed maps have allowed KDI to advocate for county-level flood prevention strategies by bolstering partnerships between KDI and Nairobi public works departments to identify inefficient drainage channels and determine practical solutions for flood prevention. (enasia.com)"

The flooding in the Southern United States, Northern England and South America captured news headlines and has people talking. Time will tell whether any positive change will come out of the loss and destruction.

Emerging Threats to Cities 2016

Source: http://www.allenvanguard-cts.com/en/news-events/emerging-threats-to-cities-2016/

Allen Vanguard Counter-Threat Solutions has stated in its blog that "*the traditional intelligence community must move to make room for open source. After all we are all in this together*." These are strong words and they are applicable to the analysis of the emerging threats to cities in 2016. A few case studies drawn from open source intelligence (OSINT) from 2014 to 2015 illustrate some of the threats to be addressed by the public, business workplaces, industry, government and specialist counter-terrorist policy and operations.

One form of analysis through OSINT is to cluster cities to identify terrorist motivation, capability, intention, weapons effects, choice of targets and tactics that have severely impacted critical functions of city life and operations.

Using many media and other sources means OSINT analysis has an agility and adaptability to match the constantly changing terror tactics, targets and technology that emerge to threaten the sustainability of cities, and as such is valuable for policy makers and security planners.

As a brief example, a cluster such as Paris, Ramadi, Kabul and Karachi brings together cities with vastly different populations, culture and economies. The effects of terror attacks on such a cluster can be used by cities in Europe and many other countries threatened by the self-proclaimed Islamic State (IS) in 2016, particularly countries whose nationals have travelled to the new Islamic State in Syria and Iraq or trained in Libya, Afghanistan and Pakistan.

- **Paris:** The availability, response times and capability of the French armed police response to several attacks in Paris on November 13, 2015 reduced the potential for shock effects on the city which recovered within days despite an ongoing search for members of the attack team. Guns rather than explosives proved to be the most potent weapon as there were few casualties from the explosives worn and deployed by the attackers.
- **Karachi:** In 2014 Karachi suffered attacks on a naval dockyard with reports of attempts to capture a ship for an attack on a US supply ship and there was also an attack on Jinnah International Airport. In the same year there was discussion in the media about the security of two Chinese supplied 1,100 MW reactors to be built in this city of 20 million people.
- **Kabul:** In August 2015 Kabul suffered many attacks including significant ones on police cadets and recruits from a suicide bomber, an attempt on a US special operations base and a massive truck bomb outside an army base in a residential area killing 20 and wounding several hundred. The continuous attacks on Kabul highlight the power of the Taliban to target the city at any time but the city remains resilient. In 2016 the growing presence of IS in Afghanistan may bring new forces and tactics that will test the resilience of the Afghan government.
- **Ramadi** In 2015 has demonstrated how a city suddenly collapses under sustained shock attacks deployed by IS with many suicide and other vehicle-borne devices attacking the city's defenses in May. These tactics caused the Iraqi army to flee leaving equipment that was subsequently utilised by the invading fighters. The Iraqi army claimed the recovery of the city late in December 2015 but there will be uncertainty over the long-term security of the city, which has suffered massive destruction of infrastructure and a displaced population.

Terror attacks on major cities impact on internal and external perceptions of a nation's capacity to secure the population, industry and trade. By studying clusters of cities under threat of terrorism it is possible to identify policies for city strengthening especially because the analysis of clusters gives a wider focus on changing tactics, targets and technology. The analysis also shows the robustness of cities under very significant attacks. However there are some conditions under which cities can move into a total collapse and be dominated by relatively small numbers of terrorists once the attackers have access to military weapons and are able to psychologically dominate the population. The failure of Ramadi is an important lesson for western cities unused to the concept of fragility in counter-terror operations.

Using OSINT to protect the world's cities

Cities across the world function in many similar ways and OSINT cluster analysis can open many emerging threat scenarios that will provide data for counter-terrorist policies, operational planning and workforce exercising, and also in the design of self-protection information programs for the public.

Some of the applications of OSINT analysis that have not been widely recognized lie in this type of cluster analysis and also in unusual emerging threat factors that at times may not be recognized because they are not within closed source intelligence capture. One such example has been the use of two brothers in the 2013 Boston Marathon bombings.

Cities require long-term policy development and this can be well served by scrutinising OSINT databases and identification of unusual factors or new trends. In hardening the population through understanding terrorism and for advice to industry and workplace organisations, OSINT has the advantages of being tested for confirmation of facts, sourced and with contextual information. The data are open and can be shared with administrators, business workers, and technical specialists in industry, as well as with civilian security personnel who are often in the front line of city attacks. More significantly, the data can help legislators understand future trends and agree counter-terrorism policies.

A conclusion is that not only are "*we all in this together*" but that access to open source data helps us to understand the phenomenon of emerging terror threats in cities and that cities are critical to national security.

Dr Sally Leivesley has read TRITON reports since 2001 and applies the data to training exercises and research. She is Managing Director of Newrisk Limited, a member of The Exercise Group7 and a member of the Register of Security Engineers and Specialists.

Animals as Part of the Whole Community

By Anne McCann and Richard Green

Source:http://www.domesticpreparedness.com/First_Responder/Emergency_Management/Animals_as_Part_of_the_Whole_Community/

Animal issues are people issues. As such, all species – household pets, service and assistance animals, agricultural animals/livestock, wildlife, and other animals (including zoo animals, shelter animals, and animals used in medical research) – must be an integral part of a community's disaster plan at the local, state, and federal levels.

Jan 20 – Animals are integral to American society, and all hazards that pose risks to humans pose risks to animals as well. When a society's normal state is undermined, people naturally cling to family, which for many includes the animals in their lives. People have strong bonds with animals and often go to great lengths to protect them. This bond is often heightened in times of stress. There are countless examples of people putting their lives at risk to rescue animals left behind and similar examples of families not evacuating if they were not able to take their animals with them. People are much more inclined to cooperate with emergency responders' instructions if provisions are made to safeguard their animals. In addition, certain animals can present clear human health and safety risks to emergency responders and the public if not effectively managed. Recognizing these risks, it is incumbent upon the emergency management community to prepare for and manage animal issues during responses to better protect human life.

Resources & Response Management

Understanding the full range of animal issues in the community, as well as engaging animal resources that are present within a jurisdiction, will ensure that a jurisdiction is equipped to address animal issues – both planned (e.g., evacuation and sheltering) and unplanned (e.g., escaped animals from a farm or zoo). An all-hazards/all-species approach will help during the planning process for the many response issues that animals present. All-species responses should plan for household pets, service and assistance animals, agricultural animals/livestock, wildlife, and other animals (including zoo animals, shelter animals, and animals used in medical research) within a jurisdiction. Animal issues occur in both Stafford Act and non-Stafford Act incidents, either as incidents (e.g., an animal disease outbreak) or as secondary issues within a larger incident (e.g., zoo evacuations, household pet search-and-rescue operations, and animal decontamination).

From a response management standpoint, keeping people and their animals together whenever possible greatly simplifies managing an incident. Fully integrating whole community all-hazards/all-species animal planning into the human responder framework is essential to efficiently and effectively manage incidents and coordinate resources.

Animal responses require multiagency coordination at all levels, with a well-established coordinating structure that encompasses the private sector, nongovernmental organizations, and various levels of government. Success depends on an

integrated emergency response requiring a full spectrum of capabilities. Based on its risk assessment, each jurisdiction should determine how animal response activities need to be integrated into its emergency operations plan.

Animal Response at the Local & State Levels

Specific authorities, resources, and capabilities associated with animals, including household pets and service animals, are dispersed across a broad range of response providers, government agencies, and emergency support functions. Many jurisdictions have a legally designated lead agency for animal responses. Typically, at the local level, the animal control agency is the authority having jurisdiction for animal issues. At the state level, the Department of Agriculture, Board of Animal Health, State Wildlife Management Agency, Public Health, or the Emergency Management Agency coordinate animal response activities. Whether a designated authority exists or not, or when there are diffuse authorities (e.g., when different state agencies have authority for agriculture animals, wildlife, and pets), jurisdictional emergency operations plans should clearly identify the lead agency/organization tasked with managing animal emergencies.

Emergency management officials, planners, and coordinators, as well as elected officials, should plan for plausible animal responses and, where practical, integrate existing infrastructures. Animal emergency management will always be a whole community effort – a blending of emergency management and animal welfare expertise.

The animal infrastructure at the local level includes veterinarians, farmers, animal control agencies, humane organizations, breeders, and wildlife rehabilitators. These entities should be encouraged to collaborate with government agencies to meet emergency animal needs. Many states have integrated animal response capabilities, such as state and/or county animal response teams and veterinary medical reserve corps.

Animal Response at the National Level

Nationally, the coordinating structure for animal response includes the Federal Emergency Management Agency, the U.S. Department of Agriculture, the Department of Health and Human Services, the Department of the Interior, and other federal agencies, along with nongovernmental partners including the National Alliance of State Animal and Agricultural Emergency Programs (NASAAEP) and the National Animal Rescue and Sheltering Coalition (NARSC).

NASAAEP includes the agencies within a state that have authority to manage animal emergencies and animal resources. NASAAEP facilitates state-to-state resource sharing and has convened national subject matter experts to compile best practices, which are available to communities and states to help plan for animal disaster issues. Additionally, NASAAEP will host its 2016 Summit on Animal Emergency Management in College Station, Texas, 17-19 May 2016, to share information and best practices with animal emergency managers.

NARSC is a coalition of the leading national private sector and nongovernmental organizations that have agreed to follow the guidelines established in the National Incident Management System, train together, and share resources to provide surge capabilities, as needed, to augment animal response activities by states and local jurisdictions. During emergencies, NASAAEP and NARSC have agreed to participate in a multiagency coordination system to most effectively coordinate limited resources. This is a flexible and scalable way to effectively and efficiently support animal incident management.

In summary, animal response issues, at their core, are people issues. Animal issues are relevant to all five mission areas and the core capabilities as defined in the National Preparedness Goal. As such, animals cannot be considered independently of the human aspects of preparedness, response, and recovery issues.

Anne McCann *is the national emergency programs coordinator for the U.S. Department of Agriculture's (USDA) Animal Care Program. In this capacity, she supports the U.S. Department of Homeland Security/Federal Emergency Management Agency planning initiatives, serves as program liaison to Emergency Support Function #11 (Agriculture and Natural Resources), and works with government and nongovernmental partners to build and sustain a shared national strategy and capabilities for pet/animal emergency*

management. Before coming to USDA, she served as an all-hazards planner with the Delaware Emergency Management Agency, supporting planning for pets, unattended children, and people with disabilities and others with access and functional needs, and as vice president of the National Alliance of State Animal and Agricultural Emergency Programs (NASAAEP).

***Richard (Dick) Green** is currently the senior director of disaster response for the American Society for the Prevention of Cruelty to Animals (ASPCA). Before coming to the ASPCA, he was the emergency relief manager for disasters at the International Fund for Animal Welfare (IFAW). He has responded to well over 100 international and national disasters. Over the last several years, he has presented his work in disaster preparedness and response to professional groups in China, Costa Rica, Australia, Mexico, Iceland, Canada, Chile, Philippines, Indonesia, Israel, and the United States.*

*Significant contribution to this article was made by **David (Dave) Sacks**. Since 2013, he has been the communications officer for the U.S. Department of Agriculture Animal Care, after serving four years as the organization's media spokesman. Before that, he was a public affairs specialist for the U.S. Marshals for 14 years, and an editorial assistant with Discovery Channel.*

Mitigating for Sea Level Rise, Terrorism on Local to-Do List

Source: http://www.emergencymgmt.com/safety/Mitigating-for-sea-level-rise-terrorism-on-local-to-do-list.html

A new hazard mitigation plan lays out how local community officials can reduce vulnerability to natural and man-made hazards in Chatham County. That reduced vulnerability, in turn, can lead to lower flood insurance rates.

Emergency planners explained the latest edition of Chatham County's hazard mitigation plan at a public meeting Thursday afternoon at Garden City City Hall.

For the first time, the 2015 plan includes the threat of sea level rise, a reality that's becoming more apparent as high-tide flooding more frequently swamps area roads.

"In all coastal counties we're seeing a lot of that," said Margaret Walton, project manager for Atkins, the consulting company that helped produce the plan.

The plan lists mitigation actions for each community, with a high of 61 possible actions spelled out for Savannah and just four for Bloomingdale. Walton said local governments aren't obligated to complete each item, but that having such a "wish list" helps make federal grant funding more available if needed.

The 211-page document includes plans to do more planning -- such as a Chatham County item that reads "Assist nursing homes and assisted living facilities with writing a County Emergency Management-approved emergency plan that includes evacuation."

But it also lists concrete actions such as a Garden City item that reads "Relocate Fire Station 2 located at 2604 Highway 80 out of susceptible flooding area."

Atkins was paid $40,000 to provide professional mitigation planning services. That money came from a federal hazard mitigation planning grant funneled through the Georgia Emergency Management Agency.

This is the third iteration of the Chatham County hazard mitigation plan. Such plans are prescribed by the federal Disaster mitigation Act of 2000 and must be updated every five years for communities to remain eligible for federal disaster and mitigation-related grant programs.

Although Thursday's meeting was billed as an opportunity to provide "valuable feedback" on the plan, the Federal Emergency Management Agency has already reviewed and conditionally approved it.

It's also already been adopted by Chatham County, Tybee,

Thunderbolt and Bloomingdale. It was on the agenda for Port Wentworth's council Thursday night and will be before Savannah's council Tuesday and Garden City's in January.

Hazards that are examined and planned for range from drought to flooding and include natural disasters such as hurricanes, tornados and earthquakes as well as man-made terror threats.

On Savannah's to-do list, for example, is providing better protection for its chlorine tanks at the I & D Water Plant "to prevent ease of access to chemical by potential terrorists."

Regarding the newly added threat of sea-level rise, the plan notes that recent studies show the rate of sea level rise has been increasing steadily over the past century.

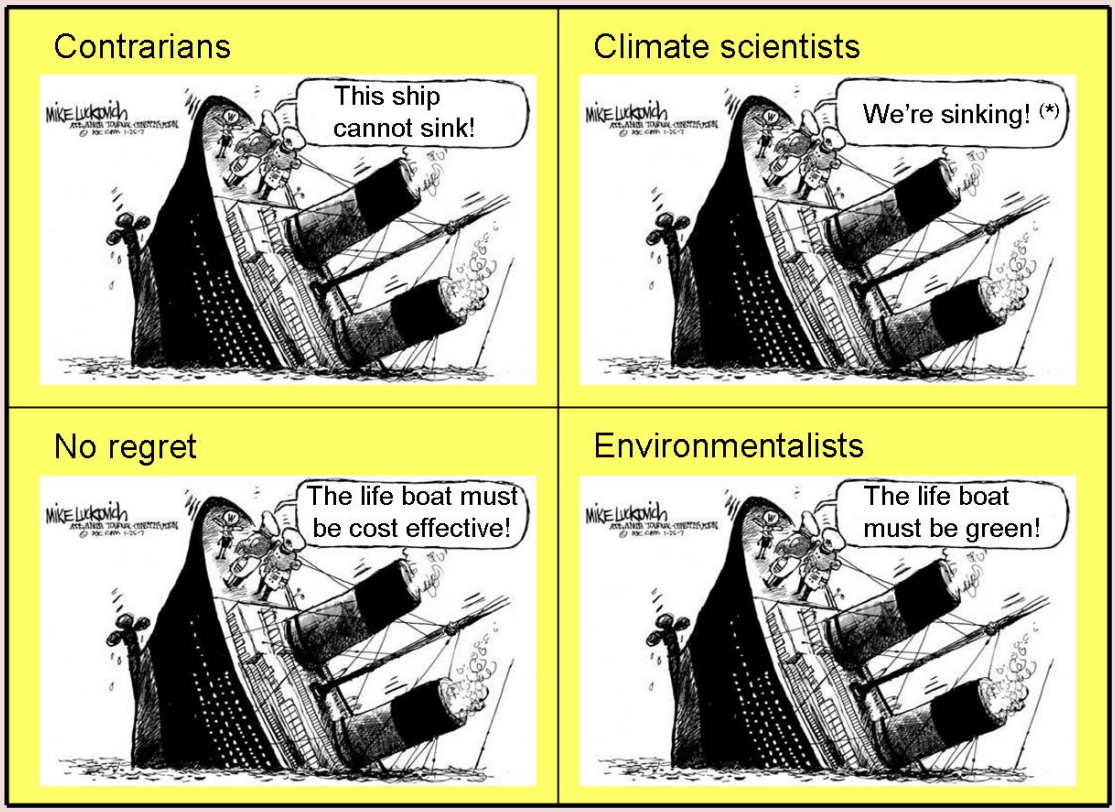
"This increase in rate will likely have a quicker and potentially more devastating effect on people and property than any sea level rise that has taken place in the past," it states.

Along with sea-level rise, the plan added drought, extreme heat, hailstorm, lightning, severe thunderstorm/high wind, winter storm and freeze, earthquake, dam and levee failure, and erosion as threats to consider.

Much of the plan's emphasis is on flooding, a likely hazard for a coastal county. The all-hazards plan doubles as a flood mitigation document for all but Savannah, which has an additional plan specific to flood.

Its flood planning that relates most directly to residents' pocketbooks, CEMA officials said. That's because the community rating system used to establish federal flood insurance rates takes into account many of the activities the hazard mitigation plan lays out.

"The things that you're doing to your buildings, roads and the public participation and the public education, all these are like little things that help lower your points," said Kate Busbee, CEMA's chief planner.



Major incident management trends – 2016

Source: http://info.xmatters.com/rs/178-CPU-592/images/MIM_2016_Survey_Report_Final.PDF

Reliance on digital infrastructures has dramatically increased the impact and frequency of major incidents. In fact, more than 90% of large businesses report major incidents occur at least several times

Only 52%
of companies have a major incident team

Only 44%
of companies staff major incident teams with dedicated personnel

In the absence of a major incident team, various roles lead the major incident response

76%
of business stakeholders are tolerant that major incidents are an unavoidable fact of business

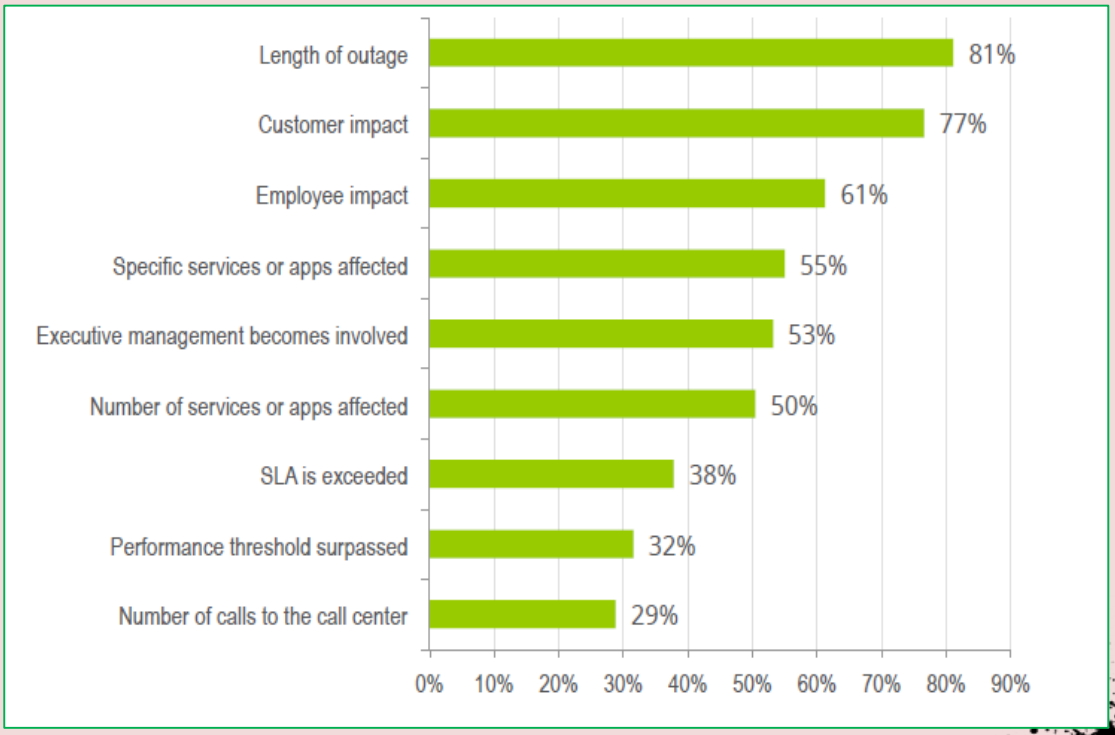
87%
say executives must be informed during major incidents

64%
have target resolution times

76%
frequently miss those target resolution times

a year and nearly 60% report major incidents occur at least monthly. A survey of more than 400 IT professionals reveals that IT and business leaders within individual companies are mostly aligned on what constitutes major incidents and how to resolve them. However, standard definitions and processes are lacking between companies and across industries. Without these standards, IT departments lack benchmarks and best practices to help drive improvements.

Numerous Factors Determine When an Incident Becomes a Major Incident



A more complete picture reveals itself when we combine our recent survey results with our customers' experience and our own expertise. In this report we will attempt to put the results of the latest survey in context for better analysis.

▶ **Read this very interesting report at source's URL.**

The Emergency Management Gap - Why It Could Threaten Business Resilience

By Vincent B. Davis

Source: https://www.linkedin.com/pulse/emergency-management-gap-why-could-threaten-vincent-davis-cem

Jan 07 – This past summer I began my 15th year as an emergency manager on an exciting new path, moving from frigid Chicago to sunny southern California to assume a newly created position of Corporate Emergency Preparedness Manager for Sony Network Entertainment in San Diego. As I began to settle into my new role, I attended a series of internal meeting and events with colleagues, part of a carefully planned on boarding process to acclimate me to the culture of the company.

In preparation, I held a fresh stack of business cards, a single page bio, and a firm understanding of my profession as an emergency manager. As I walked into meetings with an outstretched hand and met my new colleagues from the various business units, the response was quite welcoming, although a bit awkward at times. "Oh, you're part of the Business Continuity team" was the standard greeting. Not exactly, I politely retorted. Then without missing the opportunity for clarity, I forged ahead to explain the difference between emergency management and business continuity.

In the years since the Y2K scare, through the tech boom, the explosion of the internet, and evolution of sophisticated cyber systems, corporations have spent billions of dollars in their efforts to ensure business resiliency in the face of new threats, risks and vulnerabilities. Often lost within these processes, procedures and plans for redundancy of data systems and information, is a subtle but powerful reality…..If you can't effectively manage the event response, none of your long-term efforts to protect the business will succeed.

Many corporations have invested little time, effort and resources to prepare to "manage" the inevitable outcome of a catastrophe at its onset. That discipline is the core of **emergency management,** not business continuity. I equate this failure to having a new, state-of-the-art computerized automobile with all the bells and whistles, but forgetting to include a tire jack with instructions on how to use it.

If the wheels fall off all your continuity planning work, it will likely be the result of a disorganized and disconnected response, fraught with chaos and

confusion at every level. This means facing some hard facts about where your corporate team is with regard to emergencies.

Four fundamental realities make up a phenomena I call the "Emergency Management Gap":

1. Most businesses don't employ a full-time emergency manager because they believe managing disasters can be handled by an existing security or functional management staff such as facilities.
2. The heavy emphasis of business managers on data and IT recovery has left a gap that does not account for prevention, protection, employee preparedness and capabilities essential to response and recovery of the *whole* business.
3. The assumption that managing emergencies is a "natural" consequence of managing the business has itself led to a deficiency of proper planning, training, and exercises to manage life-safety and response operations for many businesses.
4. The training, experience, and insight needed to effectively harness the coordination of response and recovery in a major emergency is best left to those most qualified....emergency managers.

Contributing to the **Emergency Management Gap** is something I've found to be conspicuously absent in the business planning cycle of companies with whom I've worked, dialogued, and benchmarked……a robust employee and family preparedness program.

Add in a mix of "**corporate fear**" among business managers, many of whom may feel intimidated and threatened by their deficiency of understanding of emergency management best practices such as ICS and EOC operations, and you've got the perfect storm for a failed response to major disasters, or even minor emergencies.

In my many travels throughout corporate structures, I've experienced multiple models and hybrid subsets of emergency management and business continuity planning, most of which evolved independently within wide-ranging corporate structures. The result has been a mixed bag of programs that vary in their emphasis and approach. For clarity I've provided the following matrix of program types:

	Funded Budgeted	Has Response Plans	IT Led	Integrated with Risk	Employee Preparedness	Public-Private Partnerships	EOC Mgt. Program	Integrated Training & Exercise Program
Business Continuity Program	✓		✓	✓				
Emergency Mgt. Program		✓			✓	✓	✓	✓
Corporate Security	✓	✓				✓		
Facilities Mgt.	✓		✓					

The matrix is a first step in assessing where you are with regard to BC Planning and Emergency Management. Integrated programs work, however, they must be firmly anchored in true collaboration and understanding of what is needed, what is important, and what is effective. When it fails, the results can be catastrophic. A fully mature program will have no gaps that are unchecked either as part of overall planning.

An example of such failure is a company I'll call ABC manufacturing. They spent hundreds of thousands of dollars establishing very detailed IT recovery plans and strategies, but excluded (intentionally) all other departments and disciplines from the planning process.

The *"we're in charge and we know what's best"* attitude of the company's lead planners was fully in play. A structural fire at a main data facility exposed the fact that despite their planning, the company had not created a simple evacuation plan or conducted a drill for the employees at the data facility.

Although this sounds improbable, it actually happened, and thankfully nobody was killed or injured. The incident did,

however, underscore the very weaknesses I've described in many corporate plans, and led to changes in the company's planning policies.

A few lessons learned may help corporate leaders address the Emergency Management Gap.

- **Lesson A:** Don't allow BC, IT, Risk, Compliance, Security or other key business functions to plan in a vacuum. While these organizations are typically specialists, they often lack a broader understanding of emergency planning. Not a criticism, just a fact. This means you can't necessarily expect your key stakeholders to play nice and collaborate on their own, because chances are it won't happen. To ensure accountability, consider the following:
- **Lesson B:** Establish a planning team representative of the key players. If possible, retain an outside consultant to help establish regular planning meetings, goals, objectives and outcomes. This will help prevent "turf wars" and ensure all voices are equally heard in the planning process
- **Lesson C:** If you don't already have one, hire an experienced emergency manager. Although your BC and other teams may be staffed with quality people, they are not necessarily experienced in the nuances of emergency planning and operations.
- **Lesson D:** Establish an inclusive and comprehensive guidance document that clearly sets forth the company's philosophy, culture, and methodology for handling emergencies. Don't leave planning to chance, and don't assume all your key managers and departments are entering the discussion from the same vantage point. Collaborate at all costs, don't assume any function has all the answers

Finally, every company's goal is to be resilient to support its stockholders, investors, and customers, and to continue to lead the long-term financial viability of the communities it serves. Often forgotten in that effort is the **people** who make it happen.

Every business continuity or emergency management program plan should begin and end with the understanding that regardless of your business controls and sophistication of technology, it can't run by itself without employees.

Part of every resilience plan, emergency program, and business continuity activity must beg the question, *what have we done today to ensure our employees are equipped and capable of supporting recovery?*

Disaster planning should be anchored in a robust **employee and family preparedness** program. Be sure you actively engage HR on your planning team. If an employee's family is affected by the emergency, they won't be inclined to come to work to play their part in the company's recovery.

Vincent Davis, *CEM is Manager-Emergency Preparedness at Sony.*