Dedicated to Global First Responders

CBRNE NEWSLETTER TERRORISM

May 2018

www.cbrne-terrorism-newsletter.com

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

DIRTY R-NEWS

Why Putin's new 'doomsday' device is so much more deadly and horrific than a regular nuke

Source: http://www.businessinsider.com/putin-doomsday-status-6-nuclear-weapon-2018-3

March 2018 – Russian President Vladimir Putin announced a raft of new nuclear weapons systems at his State of the Nation address on March 1 — and one demonstrates Russia's apparent disregard for human life.

Known as the Status 6, the underwater, high-speed nuclear-capable torpedo isn't like other nuclear weapons. While any time an atom is split, there's a risk of radioactivity, nuclear weapons typically use nuclear detonations to create heat and pressure, with lingering radioactivity as a dangerous side effect.

But Putin's nuclear torpedo uses radioactive waste to deter, scare, and potentially punish enemies for decades to come.

President Donald Trump's nuclear posture review released earlier this year appeared to confirm the weapon, noting that Russia is developing "a new intercontinental, nuclear-armed, nuclear-powered, undersea autonomous torpedo."

What makes the doomsday device so dirty?

A briefing slide of the alleged Status-6 nuclear torpedo captured from Russian television.BBC

"Nuclear weapons only generate significant amounts of radioactive fallout when they are detonated at, near, or beneath ground level," Stephen Schwartz, author of "Atomic Audit: The Costs and Consequences of US Nuclear Weapons Since 1940," told Business Insider.

These types of nuclear explosions "suck up dirt, or water, contaminates it with debris from the bomb, and then lofts it into the atmosphere," Schwartz said.

US nuclear weapons, which are mainly designed to destroy other nuclear weapons in a mutual nuclear exchange, detonate in the air to create the maximum amount of pressure to targets on the ground.

The amount of pressure created by a US Minuteman III ICBM would crush much of a city, but their strategic purpose lies in holding Russia, or another country's ICBM silos at risk.

"Where the fireball does not touch the surface of the earth," as can be the case with air-burst nuclear weapons, "the only fallout is from the bomb debris itself and any dust particles in the air that come into contact with it," Schwartz said.

"When a thermonuclear weapon is surrounded with with ordinary cobalt (cobalt-59) metal," as Russia's Status 6 is rumored to be, "the fast neutrons escaping the explosion will instantly transmute it into radioactive cobalt-60, which would vaporize, condense, and then fall back to earth tens, hundreds, or thousands of miles from the site of the explosion."

How the doomsday bomb could make thousands of square miles uninhabitable for the better part of a century

The result would be a shroud of radioactive cobalt spreading indiscriminately across the planet. A cobalt bomb detonated in Washington DC could contaminate Canadian or Mexican soil. Schwartz estimates the cobalt would take 53 years to return to non-dangerous levels, and that other radioactive elements could

persist for much longer.

"Any contaminated areas would be rendered essentially uninhabitable for that amount of time and people in shelters would not be safe if they returned to the surface for any period of time," Schwartz said. "If detonated in a populated area, decontamination costs would be astronomical."

In the US, nuclear modernization has meant for decades improving the survivability, accuracy, and precision of nuclear systems to hit small targets with minimal collateral damage.

The Russian idea of nuclear superiority, as revealed by Putin, involves making the Earth uninhabitable and visiting unimaginably horrific destruction for the sake of instilling fear, or simply for killing.

More details

Poseidon (previously known as **Status-6** (Russian code name) and **Kanyon** (American code name)) is a nuclear-powered and nuclear-armed unmanned underwater vehicle under development by the Russian Federation that can deliver conventional and nuclear payloads. According to Russian state TV, it may be able to deliver a thermonuclear cobalt bomb of up to 100 megatonnes against enemy's naval ports and coastal cities. In 2018, the U.S. Nuclear Posture Review stated that Russia is developing a "new intercontinental, nuclear armed, nuclear-powered, undersea autonomous torpedo".

"Kanyon" is the name given to this drone by the Central Intelligence Agency. In March 2018, Russian Ministry of Defence officially named the drone "Poseidon" following a public vote.

The Poseidon weapon is designed to create a tsunami wave up to 500 metres (1,600 ft) tall, which would contaminate a wide area on an enemy's coast with radioactive isotopes, as well as being immune to anti-missile defence systems such as anti-ballistic missiles, laser weapons and railguns that might disable an ICBM or a SLBM.

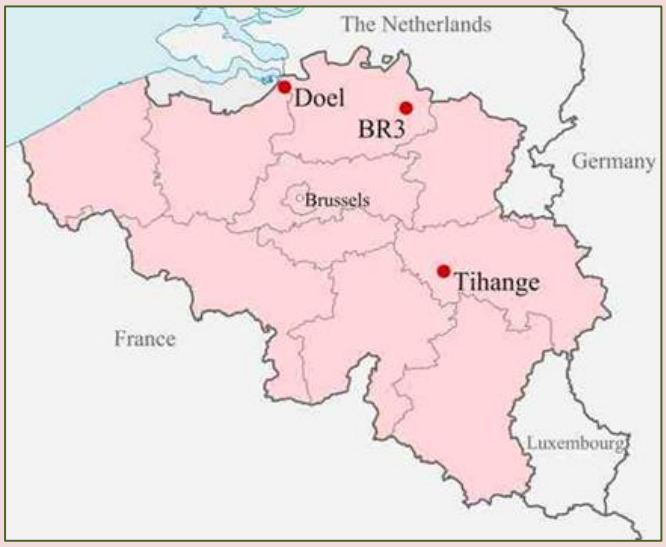
An aircraft carrier battle group would have reduced chances of defending itself against it. The drone could detonate its very large warhead at standoff range, and anti-submarine warfare units would have very little time to react because of the speed at which it travels.

Two potential carrier submarines, which would allegedly carry the Poseidon externally, the Project 09852 Oscar-class submarine *Belgorod*, and the Project 09851 Yasen-class submarine *Khabarovsk*, are new boats laid down in 2012 and 2014, respectively. Oscar-class submarines could carry four Poseidon torpedoes at the same time for the total yield of up to 400.

Poseidon appears to be a deterrent weapon of last resort. It appears to be a torpedo-shaped robotic mini-submarine which can travel at speeds of 185 km/h (100 kn). More recent information suggests a top speed of 100 km/h (54 kn), with a range of 10,000 km (5,400 nmi; 6,200 mi) and a depth maximum of 1,000 m (3,300 ft). This underwater drone is cloaked by stealth technology to elude acoustic tracking devices. Its size appears to be 1.6 metres in diameter, and 24 metres long. The warhead shown in the leaked figure is a cylinder 1.5 metres in diameter by 4 metres in length, giving a volume of 7 cubic meters. Comparing this to the volumes of other large thermonuclear bombs, the 1961 Soviet-era Tsar Bomba itself measured 8 metres long by 2.1 metres in diameter, indicates that the yield is at least several tens of megatons, generally consistent with early reports.

Belgian Nuclear Power Plant Suffers Water Leak in Reactor

Source: https://sputniknews.com/europe/201804281064002182-belgian-nuclear-power-plant/



Apr 28 – Due to an increased level of radiation in the given block, maintenance works in the reactor have been most recently handicapped, but the maintenance company says there is no need to worry.

The reactor cooling system at the Doel nuclear power station has suffered a leak, although no danger is posed to the personnel or to the environment, the operating company Engie-Electrabel reported Saturday.

"A minor water efflux has been spotted in a reserve pipe line of the cooling system. The efflux is rather small, we are still well below the mark which would cause an automatic switch-off of the reactor. It does not affect security," the company's representative noted.

According to Belga news agency, the leakage has surfaced in the nuclear part of the first energy block of the Doel nuclear power station, which was turned off out-of-schedule on April 23 for routine maintenance of its cooling system.

Given the high radiation level in this part of the reactor, maintenance works are hindered. The nuclear power plant reactor will remain unplugged at least till October 1, the agency concluded.

Belgium houses seven nuclear reactors. Two Belgian nuclear power plants – The Doel, on of the oldest plants in Europe, and The Tihange, which feature four and three reactors, respectively, are capable of producing roughly 6 MW of electricity, catering to the needs of 55 percent of the country's population.

North Korea's Secret Weapon: A Huge Electromagnetic Storm

By James Stavridis

Source: https://www.bloomberg.com/view/articles/2018-04-25/north-korea-s-secret-weapon-an-electromagnetic-storm

Apr 25 – The diplomatic circuit is awash in optimism as the proposed summit between North Korean dictator Kim Jong Un and President Donald Trump draws near. Indeed, Trump is right to go to the table with the North Koreans and negotiate for full denuclearization.

Still, given the long history of North Korea's double-dealing, outright lying, and surreptitious construction of weapons of mass destruction, the likelihood of Kim actually surrendering his nuclear weapons is extremely low, no matter what he says publicly.

And what makes it so worrisome is not only the handful of nuclear weapons in the hands of a dictator who may be able to lob a few to Honolulu or even to Seattle. We also need to consider North Korea's ability to deploy one or two nuclear weapons at altitude over the continental U.S. in order to create a devastating burst of energy called an electromagnetic pulse.

While the science of EMPs is not fully settled — largely because it is impossible to test on a grand scale — there is plenty of credible evidence that they constitute a real threat, especially in the context of North Korea.

The short burst of vastly powerful electrical and magnetic shocks involved in an EMP could potentially devastate everything from your iPhone to the entire U.S. power grid. Imagine thousands of lightning strikes hitting every home and business in America.

Bursts from a high altitude nuclear weapon — or a major solar event, by the way — could start by producing a so-called E1 shock, a brief pulse that is particularly devastating to what are known as supervisory control and data acquisition systems. The developed world is dependent on these Scada systems, which include manufacturing facilities, water-treatment plants, HVAC systems and many other things we take for granted.

Immediately after the E1 would follow an E2 burst, which is of lesser magnitude and may last as little as a microsecond. Yet these pulses are still able to cause significant damage, in large part because many protection systems will have been wiped out by the E1.

Finally, a longer E3 pulse could last several minutes and attack long-line systems such as the electric power grid by destroying substations across the nation. E1 and E3 are the effects of greatest concern because we are the least hardened against them. Together, they could deprive large parts of the country of electricity for weeks, months, or even a year or two.

How likely are these scenarios? The idea of either a terrorist group or a rogue state using a high-altitude EMP burst has been seriously examined by scientific and government groups, but there is no agreement on the potential size of the effect.

Some analysts insist an EMP would not be as apocalyptic as described in the widely referenced 2011 dystopian novel "One Second After," which portrays an America brought to its knees by such a strike. Others contend that it's highly unlikely that any hostile power would attempt one, given the overwhelming U.S. nuclear counterstrike that would quickly follow.

Maybe the skeptics are right. But given the potential devastating consequences of an EMP, can we really take the chance? That the North Koreans are probably very close to developing this capability — if they aren't there already — is all the more reason to work hard at the negotiating table.

Still, even as talks progress, there are military options the U.S. can take simultaneously for a higher level of defense.

First and foremost, we can harden our key systems, beginning with intercontinental ballistic missiles and other nuclear strategic weapons. Next comes vital infrastructure — the electric grid, water supplies, transportation systems, financial and medical networks, and so on. The cost would run to the billions — but probably not the trillions. And it would make us safer not only against rogue nuclear strikes but also EMP effects from huge solar storms, which occur on a regular basis every century or two.

Second, the military needs to increase its ballistic missile defenses against the "single shot" attack that would use EMP. This could include more ground-based interceptors to knock down attacks over the North Pole — a

route that North Korea or Iran could attempt. The Navy should plan how it would position its destroyers and cruisers equipped with Aegis combat systems off our coasts in times of rising tension.

Third, the U.S. should be pursuing a variety of advanced systems that can counter long-range missiles through non-kinetic means: lasers (which can be deployed on aircraft or from space); cyber systems that can disable enemy missiles in pre-launch and possibly while airborne; and electronic jamming that can counter cruise missile variants of EMP systems. Finally, we need to focus more intently on intelligence and early warning systems, primarily based in space, that can detect the movement of launch systems, indications of pre-launch activity, a launch itself, and then track incoming threats. Part of this involves stitching together the various components of the "detect-to-kill chain" in an overarching system that itself is hardened against a preemptive cyber-attack.

We can all hope that the coming spring brings a thaw to U.S.-North Korean relations. But one swallow does not a spring make, as the saying goes — Americans need to be ready for another winter of confrontation if diplomacy does not succeed, and being prepared for EMP is a vital part of doing so.

James Stavridis *is a Bloomberg columnist. He is a retired U.S. Navy admiral and former military commander of NATO, and dean of the Fletcher School of Law and Diplomacy at Tufts University. His most recent book is "Sea Power: The History and Geopolitics of the World's Oceans."*

Russian nuclear forces, 2018

By Hans M. Kristensen and Robert S. Norris

Source: https://tandfonline.com/doi/full/10.1080/00963402.2018.1462912

ABSTRACT

The Nuclear Notebook is researched and written by Hans M. Kristensen, director of the Nuclear Information Project with the Federation of American Scientists, and Robert S. Norris, a senior fellow with the FAS. The Nuclear Notebook column has been published in the *Bulletin of the Atomic Scientists* since 1987. This issue's column examines Russia's nuclear arsenal, which includes 4,350 warheads that can be delivered via long-range strategic launchers and shorter-range tactical nuclear forces.

Hans M. Kristensen is the director of the Nuclear Information Project with the Federation of American Scientists in Washington, DC. His work focuses on researching and writing about the status of nuclear weapons and the policies that direct them. Kristensen is a co-author of the world nuclear forces overview in the *SIPRI Yearbook* (Oxford University Press) and a frequent adviser to the news media on nuclear weapons policy and operations. He has co-authored Nuclear Notebook since 2001. Inquiries should be directed to FAS, 1725 DeSales Street NW, Sixth Floor, Washington, DC, 20,036 USA; +1 (202) 546-3300.

Robert S. Norris is a senior fellow with the Federation of American Scientists in Washington, DC. A former senior research associate with the Natural Resources Defense Council, his principal areas of expertise include writing and research on all aspects of the nuclear weapons programs of the United States, the Soviet Union and Russia, the United Kingdom, France, and China, as well as India, Pakistan, and Israel. He is the author of *Racing for the Bomb: General Leslie R. Groves, the Manhattan Project's Indispensible Man* (Steerforth) and co-author of *Making the Russian Bomb: From Stalin to Yeltsin* (Westview). He co-authored or contributed to the chapter on nuclear weapons in the 1985 to 2000 editions of the *SIPRI Yearbook* (Oxford University Press) and has co-authored Nuclear Notebook since 1987.

Suggested Hospital Preparation for Dirty Bomb Incidents in a Densely Populated Area

By Dr. Jacob Kamen

Source: https://www.cbrneportal.com/suggested-hospital-preparation-for-dirty-bomb-incidents-in-a-densely-populated-area/

May 01 – On September 11, 2001, our own planes were used as missiles against our own city causing death, panic, and mass disruption as well as economical stress. There have been many incidents where terror groups have tried to use radioactive sources such as a particular isotope of cesium (**cesium-137**) as a dirty bomb. Unfortunately there are still many radioactive **irradiators** using cesium presently exist in many hospitals that could be used as dirty bomb against our own populated densely cities if they get to a wrong hand. **The incident in Guainía of Brazil in 1987 showed that 80 grams of cesium created 40 tons of radioactive waste with 4 deaths and 112,000 people had to be surveyed for radioactive contamination.** The Brazil incident was not a malicious attack; otherwise the incident may have been much worse. In addition, **according to a Homeland Security Scenario, one would expect about 10,000 people to become lightly contaminated from a large dirty bomb.** The question is how you prepare the hospital, how you assess the patient injuries, and how you mange the radioactive contamination and recover the facility.

Although there are three kinds of particles that could be emitted from radioisotopes (alpha, beta, and gamma), we have simplified this scenario by assuming that the most likely isotope that a terror group would use is **cesium-137**, which emits **gamma** radiation.

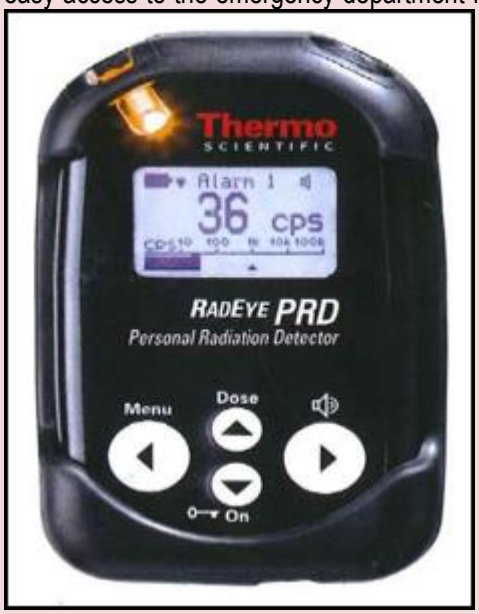
Hospitals should be able to assess the radiation injuries of the patients and to manage the influx of patients contaminated with radioactive materials. Having knowledgeable staff on board, such as radiobiologists or health physicists, would be an asset to the hospital. These individuals could help to assess the health effects of patients by consulting their knowledge of concepts such as radiation exposure, absorbed dose, radiation units, properties of common radioisotopes, and annual radiation exposure limits.

The hospital should review the hazard vulnerability analysis of where they are located and how many underground train entrances located around the hospital within what distance and what to expect in a real emergency. Is there any area that could be used as the triage area next to the emergency room of the hospital?

In such cases, time is of the essence. Hospitals must be able to **quickly detect** an event and activate access control to prevent contamination of the Hospital. Patients, visitor and staff would require **screening** and need to have access to **decontamination** areas before entering the facility. How would the hospital know if the people coming to the hospital are contaminated? **Radiation area monitors** could be installed at the entrances and the security guards with dosimeters could act as **portable portal monitors** but would need to be trained by the health physics professionals to check if the incoming persons are merely patients who have had medical procedures with radioactive pharmaceuticals or do a risk assessment for an individual who is determined to be contaminated with a radioactive source. If the radiation alarm goes off too many times in a short time, it is an indication of a mass influx of contaminated individuals to the hospital. In such an incident, the hospital management may consider **locking down the hospital** to prevent the spread of contamination inside the hospital.

Radioactive incidents are not well understood by the public and in many cases where the public believes they may think they require immediate evaluation to determine if they are affected they present to hospitals and emergency departments to be assessed. During the Iraqi scud missile attack on Israel, more than half of the people who ran to the emergency room were not hurt, but rather were in psychological shock. Having a mechanism to assess the **uninsured and worried** with appropriate support needs to be incorporated into in a plan in addition to public messaging to give instructions to remain safe and when to seek medical care. The message should be coordinated with the local health departments."

It is recommended for the hospital to have **decontamination showers external to the hospital** and with easy access to the emergency department for those who need care but also easy access to additional areas for those who only need shelter and reassurance. Most hospitals have areas identified to provide ambulatory and non ambulatory decontamination which are used for patients for contamination with radiological, biological and chemical incidents. These areas need to provide shelter from the environment, need to allow patients to safely disrobe or have clothing removed and either shower or be cleaned by a team in a temperature controlled location. **Exercises** for radioactive contamination should include a multidisciplinary group which at a minimum includes radiation safety staff and emergency staff in addition to other departments in the hospital but should also coordinate with external emergency response agencies such as fire department and police department to learn from such drills. There should be some sort of pre-arranged plan between the hospital and local Law Enforcement Agencies (LLEA) as who will do what in a real emergency.



The hospital should have on hand and maintain proper equipment for identifying and quantifying radioactive material. Such equipment may include a **portable Geiger-Muller counter** for detecting contamination, **pocket dosimeters** for recording real time radiation

dose, and **radioisotope identifiers** for indicating the type(s) of radioactive material that is/are present. Hospital staff should separate **children and pregnant individuals** from the rest of population to be surveyed for radioactive contamination because young individuals are more radiation sensitive. Processes need to be designed to single out individuals for decontamination. Although a GM counter could be used to survey a mass influx of people, there are other tools that might be employed to survey patients, a portable portal monitor, which is used in nuclear power plants, will be very effective at singling out contaminated individuals. Various tools can also be used to detect and estimate the **presence of radioactive materials inside the body** which pose an internal radiation hazard. This could, for example, involve the analysis of **nasal swabs or urine** of exposed individuals. Staff education, should also emphasize that in radiological contamination of patients the priority even before decontamination is life saving medical interventions, it is safe for care providers to render emergency care to contaminated patients. **No healthcare provider has ever died from helping a contaminated individual.** Therefore, the presence of contamination on the victims should not prevent the hospital staff to take care of a contaminated patient. Staff should protect themselves from contamination by using universal precaution such as gloves and lab coat and check their hands with a Geiger counter and replace the glove if it is contaminated.

During decontamination procedures, one has to remember that most of the contamination will be removed by just by removing the outer clothes. It is very important to decontaminate the victim from head to toe. Depending on the location, some states require collecting radioactive wash water but in reality this is simply unrealistic. It may be necessary to monitor a patients for their potential contamination through blood and other body fluid sampling which should be coordinated with Radiation Safety and Nuclear Medicine experts.

If there is an incident where radioactive shrapnel is inside the injured individual, it is recommended that a designated room be identified for operation with the radioactive victim. There has to be a mechanism to contain or to collect radioactive waste from this operation and radiation safety will dispose such waste properly.

For internal exposure to radioactive material, various treatments exist depending on the radioisotope and length of time since the exposure. Assuming cesium is used in a dirty bomb, the potassium iodide pills would be useless and in such cases the physician may prescribe the Prussian blue orally.

In conclusion, the top priority should be saving lives. No one has ever died from helping to decontaminate a contaminated individual. Contamination should not prevent medical stabilization of the injured. The help of a **psychological** support and public communication will be very beneficial during such a crisis to calm people down. **Drills** with local emergency responders to build up confidence and competence are very helpful. A pre-plan to ensure proper equipment, survey meters and supplies available is necessary. Precautions should be used to minimize the exposure and risk of contamination. Finally remember the first 24 hours are the worst and additional resources most probably will arrive.

Dr. Jacob Kamen *(ABHP certified) is the Chief Radiation and Laser Safety Officer, and an Associate Professor of Radiology, at the Mount Sinai Medical Center in New York City.*

Nuclear Inspectors Would Face Monumental Task in N.Korea

By Cho Yi-jun

Source:http://english.chosun.com/site/data/html_dir/2018/05/08/2018050801221.html

May 08 – The U.S.' call for a "permanent, verifiable, irreversible dismantlement" of North Korea's nuclear and ballistic missile programs would pose a monumental task for international inspectors.

U.S. officials project "the most extensive inspection campaign in the history of nuclear disarmament, one that would have to delve into a program that stretches back more than

half a century and now covers square miles of industrial sites and hidden tunnels across the mountainous North," according to the New York Times on Sunday.

The success of any verification hinges on accurately assessing North Korea's nuclear weapons and missile stockpiles, most of which are hidden away. Already U.S. intelligence agents are going all out to gather data about the North's nuclear and ballistic missile facilities.

The U.S. National Geospatial-Intelligence Agency recently launched a project that tracks the movements of all vehicles in and out of North Korean military installations, CNN reported. Washington has also monitored North Korean responses to American fighter planes flying overhead to arrive at an overall assessment of the North's hidden military bases.

One diplomatic source in Washington said the U.S. "may have assessed North Korea's secret military installations much more accurately than the North thinks."

The New York Times cited the RAND Corporation as arriving at no better assessment than that North Korea has 20 to 60 nuclear warheads and around 40 to 100 nuclear facilities, while one nuclear facility has more than 400 buildings.

"While there is no question Iran hid much of its weapons-designing past, North Korea has concealed programs on a far larger scale," the daily said.

The RAND Corporation predicts that it would take 273,000 U.S. troops just to locate and secure North Korea's weapons of mass destruction, which is more than the number of American soldiers deployed in Iraq at the peak of the U.S. invasion.

It warned that the International Atomic Energy Agency has only 300 inspectors, and 80 of them are already assigned to monitoring activities in Iran. If the North agrees in principle to denuclearize, the IAEA will have a huge task simply finding the personnel.

North Korea could easily conceal highly enriched uranium which could be used to produce a nuclear bomb, and it would be virtually impossible to find if the North fails to cooperate.

Justice Party lawmaker Kim Jong-dae, who recently visited Washington, told reporters that North Korea has "tens of thousands of facilities related to nuclear and missile development, while there are around 10,000 underground tunnels and storage facilities in the Mt. Baekdu area."

"Realistically, the U.S.-North Korea summit should discuss nuclear arms reduction rather than complete dismantlement," he added.

Mac Thornberry, head of the U.S. House Armed Services Committee, told Fox New that he is "very skeptical" that North Korea will completely dismantle its weapons of mass destruction and advised the U.S. to "prepare for the worst."

But others warned that North Korea could face a grim future if it attempts to fool the U.S.

Hardline U.S. lawmaker Lindsey Graham said in a radio interview that North Korea played "every president before — Clinton, Bush, all of them" but warned that Pyongyang would regret it if it tries to dupe the Trump administration since this would mean the "end of the North Korean regime."

Annual Report

Bulletin of the Atomic Scientists

For more than seven decades, a dedicated network of board members, advisors, foundations, and donors have sustained the *Bulletin of the Atomic Scientists*. We extend our deepest gratitude to the board leaders, individuals, and institutions whose continued partnership is key to our efforts. 2017 Annual Report The 2017 Annual Report reflects continued growth for the *Bulletin*, sustained by readership growth and a determined commitment to meet people where they are. From official March for Science events and museum exhibits in Chicago and Shanghai, to new partnerships with sites that cater to younger audiences like *TeenVogue* and NowThis Media, the *Bulletin* was on the front lines of taking science and rational, evidence-based policy to a public that is eager to make sense of it all. If the *Bulletin* publishes the brightest and most distinguished minds in science and public policy, it is due to the fact that our readers are equal to the task. As Lee Francis, chair of our governing board puts it: “Even in the most trying days of 2017, the Bulletin has

been buoyed by a growing readership and a spirit that reflects a keen awareness of the risks and the steady resolve to reduce them." Indeed.

Turkey probed over shipment of Israeli-made electronic equipment to Iran: report

Source: https://www.i24news.tv/en/news/international/174897-180517-turkey-probed-over-shipment-of-israeli-made-electronic-equipment-to-iran-report

May 17 – Turkey is reportedly under investigation by the United Nations over a shipment of Israeli-made electronic equipment to Iran in violation of a Security Council resolution which prohibits the transfer of nuclear-related products to the Islamic Republic.

A report by Israel's *Yedioth Ahronoth* published Thursday said that the probe was initiated **after the United Arab Emirates seized a shipment of CSP 180-300 electronic capacitors from Turkey to Iran in July 2017.**

Israel was subsequently asked to investigate the matter after it was discovered that the equipment had been manufactured by Celem Power Capacitors, a leading Jerusalem-based electronics firm, the report said.

The company, one of the largest manufacturers of electronic capacitors in Israel, was reportedly unaware that their products had been destined for Iran, claiming that the equipment was sold to a Turkish company following a thorough background check and after receiving full payment for the products in advance of shipping.

"We will prove that we sold [the equipment] to Turkey to an orderly company. We are not selling to enemy countries. Most of our sales are to Europe and the US, but Turkey is not an enemy state and there is no reason not to trade with it," Celem said in response to the report, according to *Yedioth*.

"If the shipment actually arrived in Iran, the Turkish buyer cheated us," the company added.

A description of the CSP 180-300 capacitor from Celem's website

A description of the CSP 180-300 capacitor from Celem's website lists it as a "high frequency conduction-cooled capacitor" with "induction heating, resonant circuits, medical imaging, heat treatment,electric vehicle charging, IPT, high frequency inverters, plasma applications, and wireless power transfer" among its standard applications.

Its transfer to Iran violates Security Council Resolution 2231 (2015) which prohibits the sale of nuclear-related products and technologies to Tehran, *Yedioth* reported.

The report comes amid a diplomatic stand-off between Turkey and Israel which has seen both countries expel the others' diplomats in tit-for-tat moves, while Erdogan and Israeli Prime Minister Benjamin Netanyahu trade back and forth barbs.

The rift, sparked by the killing of 60 Palestinians during clashes with Israeli forces on the Gaza border on Monday, threatened a fragile 2016 reconciliation deal ended a dispute over the deadly storming of a Turkish ship by Israeli commandos.

Turkey has in the past been accused of attempting to assist Iran in bypassing nuclear sanctions.

On Wednesday, Mehmet Hakan Atilla, a banker at Turkey's state-controlled Halkbank, was sentenced to 32 months in prison after he was convicted earlier this year for his role in a sanctions-evasion scheme led by wealthy Turkish-Iranian gold trader Reza Zarrab, who himself has pleaded guilty to fraud, conspiracy and money laundering charges.

Zarrab, who has not yet been sentenced, testified during Atilla's trial that he bribed Turkish officials, and that parts of the scheme -- which aimed help Iran spend oil and gas revenues abroad using fraudulent transactions through Halkbank -- were personally signed off by Turkish President Tayyip Erdogan during his tenure as Prime Minister.

Erdogan has dismissed the case as based on evidence fabricated by supporters of U.S.-based Muslim cleric Fethullah Gulen, his arch-rival, whom he also accuses of having orchestrated a failed coup attempt against him in 2016.

Turkey and Iran, despite a long-standing reciprocal distrust, are striving to develop pragmatic relations with each other, particularly over Syria where the two are backing opposite sides of the country's eight-year civil war.

Turkey was critical of US President Donald Trump's decision earlier this month to withdraw from the 2015 nuclear deal between Iran and world powers, saying it feared the decision could cause "instability" and open up "new conflicts".

Force that protects U.S. nuclear weapons loses explosives on North Dakota road, offers $5,000 to get them back

Source: https://www.washingtonpost.com/news/checkpoint/wp/2018/05/15/force-that-protects-u-s-nuclear-weapons-loses-explosives-on-north-dakota-road-offers-5000-to-get-them-back/

May 15 – **The Air Force is offering $5,000 for leads on the whereabouts of a box of explosive grenade rounds that its personnel accidentally dropped on a road in North Dakota while traveling between two intercontinental ballistic missile sites** — the facilities scattered across the U.S. heartland that stand ready to launch nuclear warheads at a moment's notice.

Airmen from the 91st Missile Wing Security Forces team were traveling on gravel roads May 1 in North Dakota when the back hatch of their vehicle opened and a container filled with the explosive ammunition fell out, according to a statement from Minot Air Force Base.

On May 11, the Air Force sent more than 100 airmen to walk the entire six-mile route where the grenades were probably lost, according to a statement from the local Mountrail County sheriff. But two weeks after it was lost, the box of explosives still hasn't been found.

The missing ordnance is a belt of linked grenades for the MK 19 automatic grenade launcher, Sheriff Kenneth G. Halvorson said in the statement shared with The Washington Post. "This ammunition is specific to that launcher and will not operate in any other launching device without catastrophic failure," he said.

The security forces of the 91st Missile Wing are responsible for protecting the intercontinental ballistic missile silos that Minot Air Force Base operates across the Great Plains.

The weapons are manned by specially trained airmen known as missileers, who sit in the underground launch centers in the middle of North Dakota fields 24 hours a day and wait in the event of a presidential order to launch the weapons of mass destruction. Associated security forces operate from a building above ground at each launch center to protect the missileers and their equipment

down below. The security forces are armed with weapons such as the MK 19 to fend off any attack on the installations and protect the nuclear warheads.

The 91st Missile Wing Security Forces team dropped a box of ammunition while traveling on gravel roads in North Dakota.

The Air Force said its Office of Special Investigations does not consider the incident a criminal matter and is seeking public assistance in ensuring the safe return of the explosives. The office has offered the number for an anonymous tip line for any information about the missing grenade rounds and a $5,000 reward for any information leading to their recovery.

Air Force Lt. Col. Jamie Humphries, a spokesman at Minot Air Force Base, said in a statement that the ammunition was in a green metal container weighing 42 pounds and is considered safe so long as the container remains intact.

Humphries warned that any damage to the container, however, could result in an explosion. If anyone locates the box and finds the ammunition in a damaged state, the area should be evacuated immediately, the statement said.

"We are hoping to get contacted by someone soon with information that leads to the can's return," Humphries said.

In September 2017, airmen from the 91st Missile Wing Security Forces team competed against other airmen in the Road Warrior exercise at Camp Guernsey, Wyo. (90th Missile Wing Public Affairs)

He added that the incident remains under investigation and that he couldn't speculate on whether any disciplinary action would be taken against the airmen who lost the explosives.

According to the statement from the sheriff, people living in the area were contacted by law enforcement authorities immediately and asked to keep an eye out for any explosives that have turned up on their property.

The sheriff's office also contacted many of the oil field vendors that operate in the area, as well as farmers, asking them to forward along any information about the box of grenade rounds, the sheriff said, describing the ammunition as very dangerous.

The sheriff's office wasn't notified until three days after the airmen lost the explosives, according to his statement. Agents from the Office of Special Investigations met with him a week after the incident to outline the status of their investigation and request assistance, resulting in a warning to the public.

Detecting & Preventing Nuclear/Radioactive Materials

By Ian Pleet

Source: https://www.domesticpreparedness.com/preparedness/detecting-preventing-nuclear-radioactive-materials/

May 16 – This case study from a 2015 deployment to the U.S. Marine Corps (USMC) Combined Arms Training Center (CATC) Camp in Fuji, Japan, demonstrates effective ways to detect and prevent unwanted nuclear and radioactive materials from being brought aboard an overseas USMC installation. The author was deployed as the emergency manager (EM) with the collateral duty of being the chemical, biological, radiological, nuclear, and high-yield explosive (CBRNE) protection officer (CPO). Upon arrival, the commanding officer also appointed him to serve as the alternate antiterrorism officer, with full support from his contracting company, Camber Corporation.

The immediate challenges for the EM/CPO involved establishing peer networks and conducting a mission assurance assessment to determine protection needs for the CATC. The first step was to reach out to the emergency managers at other bases in the Kanto Planes: Camp Zama, Atsugi Naval Airfield, Yokota Air Base, and Yokosuka Naval Station. If one of the bases faced an emergency, they may need assistance from the other installations. If one of their EOCs was activated, the EM/CPO would stand up the CATC's EOC as well. Networking also involved reaching out to fellow emergency managers and CPOs aboard Marine Corps Base Okinawa and asking the base fire chief, who was bilingual, to accompany when visiting the base fire department at the Takigahara Garrison, which was located literally across the street from the CATC.

The other key challenge for the EM/CPO was to protect the CATC from radiological threats as well as to be able to assist the host nation, Japan, respond to and mitigate a radiological threat, should leaders ask for assistance. The U.S. Marines assigned to the CATC helped during operation Tomodachi following the earthquake and tsunami in 2011 and the goal was

for the CATC to be ready to respond if Japan needed help again. A combination of training, equipment, and exercises were used to accomplish this goal.

Established Practices

Prior to arrival of the EM/CPO, there was not a consistent emergency management presence aboard the CATC for a variety of reasons. The commanding officer and the other stakeholders –explosive ordnance disposal (EOD) officer, provost marshal (similarly to a civilian chief of police), safety officer, and base fire chief – were not used to working with a proactive emergency manager. The installation emergency management plan was outdated and had not been exercised regularly.

Every military base has a cache of CBRNE equipment including bomb suits, atmospheric meters and monitors, chemical protective outer garments, respiratory protection, and CWA detectors assigned to it based on the threats identified in its hazard and vulnerability assessment. However, in the CATC's case in 2015, its cache of CBRNE equipment was stationary, nicely stored on shelves. After the EM/CPO had time to assess the situation and meet with stakeholders, a plan was established to issue out the CBRNE equipment to better protect the CATC. The equipment was assigned to specific personnel who were responsible for training on it and maintaining it to ensure it was ready at all times.

New Practices

Because the security forces are the primary deterrent for CBRNE threats, they were issued personal handheld radiation detectors to be worn while on duty. If the handheld detectors alarm, the base fire department would respond and utilize several different radiation detectors to confirm (or deny) the initial radiation alarm and identify specific radioactive isotopes. If further analysis were needed, the CPO, the safety officer, and the EOD officer would determine the best course of action. The EOD unit assigned to the CATC were already issued the regular suite of radiation detectors as well as the established reach-back capabilities to request further analysis, personnel, and assets to respond to and mitigate any radiological threat. Fixed radiation detectors were also placed at the entry control points to screen vehicles and personnel entering and leaving the CATC.

Coordinating with Marine Corps Installation Command, a semi-annual schedule was established for its Regional CBRNE Equipment Training Team to visit the CATC. Its cadre of instructors provided the security forces (both U.S. and local Japanese) 40 hours of CBRNE training, which included interactive, classroom lectures, hands-on practice with the CBRNE meters, monitors, and detectors, as well as functional exercises. It was important for the CPO to be present during the classes and help design the exercises. Because they taught both U.S.

Marines and local nationals, an interpreter also accompanied the Regional CBRNE Equipment Training Team.

Monthly exercises – both tabletop and functional – were established to include radiological threats, like radiological dispersal devices. The EOD unit served as a "red cell" and helped create realistic, safe, and functional exercises to test and evaluate the CATC's response to all-hazards threats, like suspect mail received in the mailroom. With the support of Marine Corps Installation Command and a newly established network, there was buy-in from the commanding officer and other stakeholders to mature the emergency management plan and heighten the security posture of the CATC in Fuji.

The CATC Since 2015

Since departing in 2015, the changes made are still in place. Fortunately, the succeeding CPO from Marine Corps Base Okinawa continues to evolve the program. The lessons learned from this were to establish a network of peers and empower first responders by equipping and training them.

*In 2015, **Ian Pleet** served as the installation emergency manager and CBRNE protection officer for the U.S. Marine Corps Combined Arms Training Center (CATC) Camp Fuji, Japan. Since his return from Japan, he has been accepted into the EMI's Emergency Manager Basic Academy train-the-trainer course and looks forward to sharing his experiences with the next generation of emergency managers. He currently works as an emergency manager for the U.S. Department of Defense and is contract CBRN Operations instructor for the State Department's Global Antiterrorism Assistance (GATA) Program.*

Scientists successfully vitrify three gallons of radioactive tank waste

Source: http://www.homelandsecuritynewswire.com/dr20180517-scientists-successfully-vitrify-three-gallons-of-radioactive-tank-waste

May 17 – In a first-of-its-kind demonstration, researchers at the Department of Energy's Pacific Northwest National Laboratory have vitrified low-activity waste from underground storage tanks at Hanford, immobilizing the radioactive and chemical materials within a durable glass waste form.

Approximately three gallons of low-activity Hanford tank waste were vitrified at PNNL's Radiochemical Processing Laboratory in April. The laboratory-scale demonstration is an important step toward the eventual treatment of millions of gallons of hazardous waste generated during past plutonium production at Hanford.

"This was the first time low-activity Hanford tank waste has been vitrified in a continuous process, very similar to the treatment process that will be used at Hanford, rather than as a single batch," said Albert Kruger, glass scientist with DOE's Office of River Protection. "The experience from this test will help us as we prepare for full-scale operations."

Researchers at PNNL performed the work in partnership with Hanford tank operations contractor Washington River Protection Solutions and ORP.

To vitrify the material, researchers mixed the liquid waste with glass-forming materials and pumped it, at a controlled rate, into the melter. Approximately 5 inches in diameter, the melter sits inside a furnace that keeps the glass forming materials within it at 2100°F. A half-pound of glass poured from the melter every half hour, and the test produced approximately 20 pounds of glass.

"This successful test confirms the science and engineering approach," said Will Eaton who led the test for PNNL. "Seeing actual Hanford low-activity waste being converted to glass is really exciting. It ties together 20 years of work from the design and construction of the Waste Treatment Plant to the research and testing that has supported that effort."

PNNL says that the vitrification test was the most recent in a series that

used the PNNL-designed test platform to mimic the key processes to be used in the Direct Feed Low-Activity Waste system being constructed at Hanford. DFLAW will remove solids and cesium from tank waste and send the resulting low-activity waste to the Waste Treatment Plant for vitrification inside large melters.

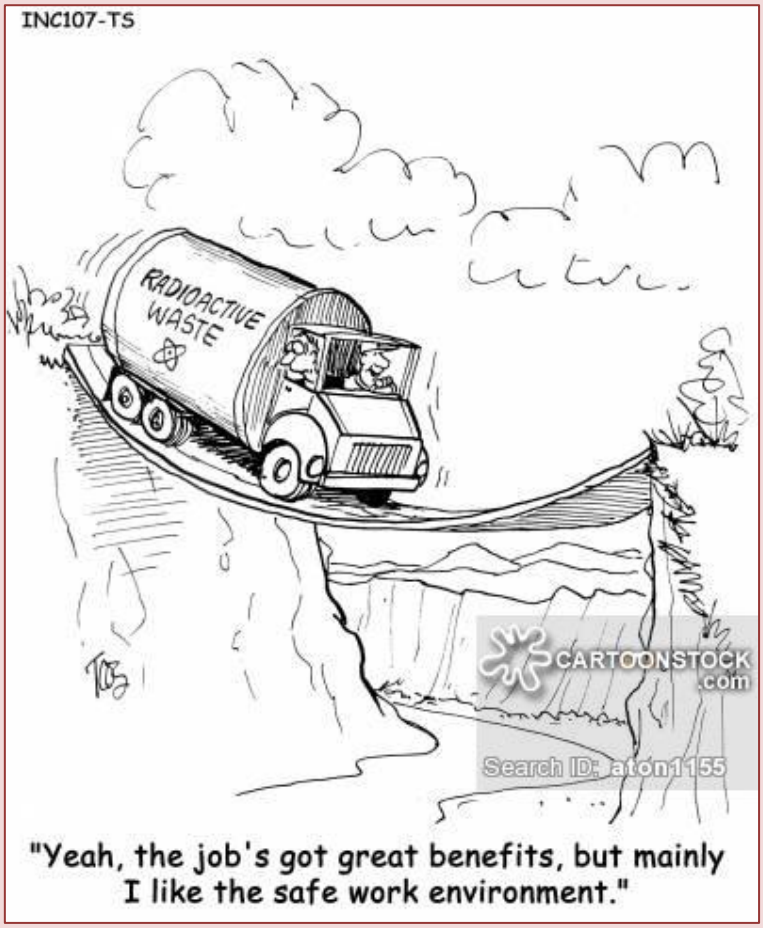
In tests leading up to the vitrification, the original high-level tank waste was pretreated inside a PNNL hot cell. There, researchers used a filter and ion exchange columns to remove solids and cesium, leaving a low-activity solution containing dissolved waste constituents.

Off-gases generated during the vitrification process produced a liquid condensate which will be concentrated and grouted later this spring in another related test. The grouted material will be analyzed to see if it meets disposal requirements.

A second laboratory-scale vitrification test is planned later this year using approximately two gallons of waste from a different Hanford tank. Pretreatment of that waste will test different filtration and ion exchange methods.

"Being able to run real tank waste instead of simulant through these tests provides valuable input for validating and refining our approach to the treatment of low-activity waste," said Kris Colosi, the WRPS project manager. "It's another important step toward the removal and disposal of a large portion of Hanford's tank waste."

PNNL, which is located near the Hanford site, developed the liquid-fed ceramic waste melter technology in the 1970s and it has become the standard for waste vitrification in this country and elsewhere around the world. Numerous melter tests have been conducted in the decades that followed, including both small- and large-scale simulant tests and pilot-scale tests with high-level radioactive waste.



ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

EXPLOSIVE NEWS

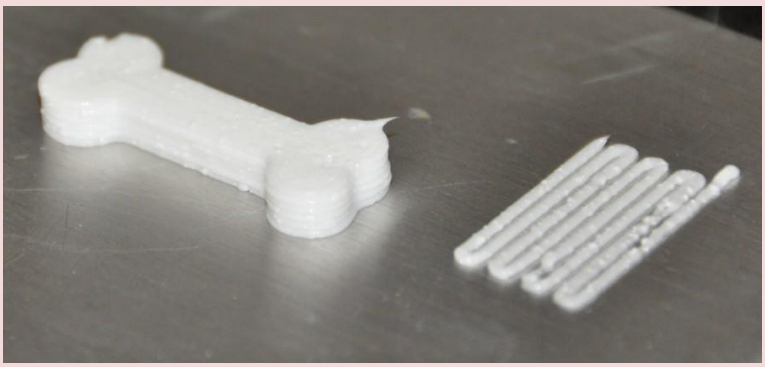
Improving K-9 training

Source: http://www.homelandsecuritynewswire.com/dr20180502-improving-k9-training

May 02 – Additive manufacturing (AM) has gone to the dogs, thanks to Lawrence Livermore National Laboratory's (LLNL's) new approach to K-9 training materials. The process prints 3D objects that contain trace amounts of nonreactive explosives, resulting in several advantages for K-9s and their handlers. Chemist John Reynolds leads a team of LLNL scientists and engineers who recently received patents for this method and application.

Known by many names — bomb dogs, sniffer dogs, explosives detection canines or K-9s — these animals are valued for their reliability, trainability and highly sensitive noses. Their portability enables real-time detection in a range of national security scenarios. K-9s can detect explosives, residues, fillers and post-blast evidence.

K-9s learn to distinguish scents and targets through intensive training, which can take years at considerable expense. Reynolds has come to know the K-9 community through his work with explosives and associated safety measures. "It's surprising how difficult this training is. Very few dogs have the aptitude for it," he said.



Proof-of-concept training aid containing 8 percent of the explosive HMX in a silica substrate. The low concentration makes the object safer to handle when testing a dog's scent sensitivity.

According to Reynolds, this community needs materials with better quality and more variety. "We have the technology to make sophisticated training aids," he said, citing LLNL's long history of AM research and development combined with the expertise of the Energetic Materials Center. Materials chemist Alex Gash added, "Our job is to provide innovative, technically sound solutions to current problems. We can improve the existing training products."

LLNL notes that conventional training aids are usually presented to the dog as a powder or gel, which does not reinforce shape recognition. Simple mixing techniques do not uniformly distribute explosive material throughout the object, so the concentration level is harder to control. Simulating improvised explosives is even more problematic because mixing fuel and oxidizers together render the object unstable, unsafe and short-lived. Reynolds points out, "Training aids are mainly limited to stable explosives, but the real world is not."

K-9s are tested with explosive concentrations below 10 percent of a training aid's weight, and dogs' noses are sensitive enough to pick up more than just the active material. AM can uniformly and precisely disperse the explosive throughout the substrate at low concentrations. Controlled dispersion also allows fabricators to eliminate any interfering materials. "The K-9 should respond to the explosive itself, not the matrix," Gash said. "With a low-volatility matrix, the dog won't train on the wrong signature."

Feedstocks are dyed red and blue in this laminate structure to show one type of alternating composition. Training aids that simulate improvised explosives can be printed without mixing reactive components.

With this ability to fine-tune ingredients, researchers can combine explosives with an assortment of substrates, such as plastic or clay, to simulate real-world conditions. AM's flexibility makes many combinations possible for both traditional and improvised explosives training. "We can train dogs for a broader swath of explosive threats," Gash said.

AM also makes training aids safer, particularly for simulating improvised explosives. Fuel and oxidizer layers can be sandwiched between inert layers to prevent a reaction. Gash explains, "Printing two materials without mixing them yields a more stable product that still gives an accurate signature to the animal." Stable, low-concentration training aids can be handled, stored and transported as non-hazardous materials.

The team is using multiple AM techniques, such as direct-ink writing and powder-bed binding, to optimize mixtures, stability and strength. For example, lattice structures such as base-cement, which were previously not used in the field, can now be made into training aids.

Additional AM benefits include the ability to print on demand (potentially in the training field with a portable printer), scale up and create any size or shape. Although some of the team's proof-of-concept objects resemble Milk Bones, more realistic shapes, such as cell phones and hand grenades, are possible.

The project's next step is securing sponsors for rigorous testing with K-9s and handlers. Ultimately, the goal is to gain approval from agencies like the Department of Homeland Security and the Transportation Security Administration to use this next generation of training aids in the field. Beyond explosives, AM technology could produce aids for dogs learning to detect narcotics, chemical weapons or other illicit materials.

Drugs laboratory or bomb laboratory?

By Marc Wesselius

Sourcce: https://www.cbrneportal.com/drugs-laboratory-or-bomb-laboratory/

May 01 – Times are changing and threats involving explosives are more potent than ever. Public authorities have long been aware of the presence of homemade explosives (HMEs). The knowledge of how to construct HMEs has been widely distributed by anarchist organizations and has thus been known to criminals and terrorists long before the invention

of the Internet. Though homemade explosives have always embodied danger, they were previously only found in small quantities in the Netherlands. More often than not such detonative offences involved an adolescent chemistry student unable to resist the temptation of manufacturing his very own bomb.

The technology of manufacturing HMEs was picked up by known terrorist organizations which in their turn informed their supporters of this fairly easy and rather ideal way of committing attacks. Recently, however, it appears that the practice no longer limits itself to small quantities. Terrorists now produce HMEs in vast quantities, something a rational person would never think of doing due to the very high risks involved in the manufacturing.

The unexpected discovery of large quantities of reactive substances such as Triacetone triperoxide (TATP) or Hexamethylene triple oxide diamine (HMTD) is now a risk that every first responder (police units and fire brigades) could face. Because it is very difficult for a first responder to recognize the difference between a bomb laboratory and a drug laboratory, a new problem arises; correctly identifying the lab in question. This remains the problem of the first responder and therefore he or she must be able to make the correct assessment.

▶▶ Read the rest of this article at source's URL.

Mark Wesselius *is the Coordinating Team Leader for Explosives Safety and the Chief Inspector of Police of the National Police Unit of Rotterdam for the Netherlands.*

Family of Suicide Bombers Attacks Churches in Indonesia

Attackers came from a single family; first time children involved in carrying terrorism in country

Source: https://www.wsj.com/articles/bomb-attacks-rock-three-indonesia-churches-1526177568

May 13 — **A family of suicide bombers, including children, killed at least seven people and injured dozens in attacks at churches in Indonesia** on Sunday, police said, the latest in a wave of Islamic State-inspired violence in the world's largest Muslim-majority nation.

The attacks on Indonesia's Christian minority come amid a rise in extremist violence and security lapses in a Southeast Asian nation where supporters of Islamic State have been seeking to wage large-scale attacks. It was the first time children have been involved in waging a terrorist attack in Indonesia, and the country's deadliest act of terror in almost a decade.

Police sources said **seven churchgoers and security personnel died in near-simultaneous morning bombings at three churches in Surabaya, Indonesia's second-largest city,** on the island of Java.

National Police Chief Tito Karnavian said the attackers came from a single family that had spent time in Syria in support of the terrorist group Islamic State, and whose head was the leader of a terrorist cell in Surabaya. All six family members died in the bombings, police said.

Mr. Karnavian said that in one of the attacks, the family's mother and two daughters, ages 9 and 12, were killed when they detonated one or more bombs at the entrance to a church. He said he believed all three had bombs wrapped around their waists.

In another attack, he said two sons, ages 16 and 18, drove a motorcycle onto the grounds of a church and detonated a bomb. The biggest explosion was at a third church, where police believe the father detonated a car bomb.

Motorcycles burned after a blast Sunday at one of three Christian churches targeted by a family of suicide bombers in the city of Surabaya in East Java, Indonesia. Photo: antara foto/Handout Surabaya Government/Reuters

Dozens of people were injured and taken to hospitals. Police said they defused bombs at Santa Maria Catholic church.

The Middle East-based terrorist group Islamic State claimed responsibility for what it called "three martyrdom operations."

President Joko Widodo called the attacks "barbaric" and said he would "uproot the cells entirely."

Police also put Jakarta, the capital, on high alert. Terrorism experts warned of more attacks, with extremists rallying followers ahead of the Muslim fasting month of Ramadan, which begins this week.

The bombings come amid a wave of bloodshed largely targeted at police.

Last week, inmates killed five police officers in a 36-hour siege of a terrorist-detention center in Jakarta.

Islamic State claimed responsibility for the revolt, the second uprising at the prison since Aman Abdurrahman, the de facto leader of Islamic State supporters in Indonesia, was transferred there last year to stand trial on charges of inciting followers to wage attacks. Those include one in Jakarta in January 2016 that was the first here to be linked to Islamic State and left four bystanders and four terrorists dead.

Early Sunday morning, police in western Java shot dead four suspected terrorists in a gunfight. They said the men were members of a pro-Islamic State group and had carried out paramilitary training with a plan to attack the Jakarta detention center.

There are indications that "several sleeper cells have started waking up," said Setyo Wasisto, a police spokesman. "We suspect that there's a command from Nusakambangan for them to act," he added, referring to a maximum-security prison that houses some of the country's highest-risk inmates.

"The killing of five police officers is seen by these terror cells as an invitation for them to do the same," said Al Chaidar, a terrorism analyst from Malikussaleh University.

Islamic State is believed to use child soldiers in its heartlands of Iraq and Syria, and The Wall Street Journal reported in 2014 that ISIS religious schools in Aleppo and Deir Ezzour

had recruited children. Last year, the terror group published a video of a toddler shooting dead a prisoner in Syria.

Members of an Indonesian bomb squad surveyed the site of a Sunday morning attack at a church in Surabaya, Indonesia. A police source said the attackers included children carrying bombs. Photo: juni kriswanto/Agence France-Presse/Getty Images

Hundreds of Indonesians have traveled to the Middle East in recent years to support Islamic State, and authorities worry that their influence and possible return could lead to new attacks, a concern shared by Indonesia's neighbors in Southeast Asia. Last year, Islamic State-linked militants took control of the southern Philippine town of Marawi for several months.

How assault vehicles destroy IEDs without locating them

Source: https://www.wearethemighty.com/how-assault-vehicles-destroy-ieds

For ground troops, the improvised explosive device threat is considered one of the deadliest defensive components ever to hit the battlefield. Enemy forces have placed countless IEDs anywhere, including alleyways, open terrain landscapes, and along transportation routes.
With all the different mine-defeating technologies allied forces have available, many homemade explosives still manage to still go undetected at times.

Assault Breacher Vehicle
Crammed with 7,000 pounds of explosives, this mode of transportation can destroy nearly any hazard the enemy might plant.
The ABV uses its weaponry to destroy a preselected area of enemy terrain within seconds — much faster than foot patrol.
"The ABV can clear a route faster than dismounted patrols because it doesn't actually have to find the IED," Lance Cpl. Jonathan Murray stated.
The vehicle is tailor-made to find and destroy IEDs that protect the enemy's stronghold. Along with its superior armor, the ABV fires a mine-clearing line charge known as an MICLIC.
The MICLIC is as a 350-foot-long "sausage link" that contains nearly one-ton of C-4 explosives that can clear a surface area of a football field in a single blast. Once a MICLIC is fired off by the operator, they will send out an electrical charge that will completely detonate the line and everything in its path.

The massive explosion that follows will set off any IED with the surrounding sector 45-feet wide, making it safer for troops and local nationals to walk. As the ABV maneuvers through the enemies' backyard, the vehicle can also detonate the IEDs with a plow system mounted in the front.
The plow has the ability to dig up the lethal mines before our brave service members have a chance to step on it — saving lives.

UK airports to add explosive detection dogs to screen cargo

Source: http://nationalpost.com/pmn/news-pmn/uk-airports-to-add-explosive-detection-dogs-to-screen-cargo-2

May 06 — British officials say dogs trained to detect explosives are being deployed at airports to screen cargo for possible devices.
The Department of Transport said Sunday that each dog has been trained for 12 months to be able to detect small traces of explosives. They will be based in airport cargo sheds to screen large volumes of freight as one additional layer of protection.
Aviation minister Elizabeth Sugg says the use of the dogs "will bolster our existing rigorous security methods."
Dogs are already deployed at U.K. airports — including London's sprawling Heathrow Airport — to aid police in identifying criminals and preventing drug transport and other illegal activities.

EDITOR'S COMMENT: I thought that dogs were part of the screening methodology for years. Well, better late than sorry!

Terrifying arsenal of weapons - including IEDs - seized from city gang targeted in raids

Source: https://www.liverpoolecho.co.uk/news/liverpool-news/terrifying-arsenal-weapons-including-ieds-14609343

May 03 – A terrifying arsenal of weapons - including two Improvised Explosive Devices - have been discovered by police in a gangland investigation which led to a series of raids this morning.
The crudely made IEDs, believed to have been stashed for use against criminal rivals, were among a haul of 13 guns and more than 200 rounds of ammunition during a 12 month probe.
Three more guns were discovered this morning when search teams raided suspected associates of an underworld network that stretched across the country from its Speke base.

Tipped off by those forced to endure the antics of the gang across the region, Merseyside Police launched Operation Bombay.
Undercover work was mixed with high profile visible operations - including searches of woods and open land surrounding Speke - as detectives gathered intelligence on those thought to be linked to the gang suspected of being involved in the supply of Class A and Class B drugs, a business by the ownership of illegal guns.

Suicide Bombings: Boko Haram adopts new tactics

Source: https://www.premiumtimesng.com/news/headlines/268745-suicide-bombings-boko-haram-adopts-new-tactics.html

May 17 – The Nigerian military says the Tuesday attack that claimed the lives of at least three operatives of the Civillian-JTF in Konduga town of Borno State was possible because Boko Haram used an aged man who disguised as a weak and feeble traveller.
The spokesman of the military operation in the North-east, Operation Lafiya Dole, Onyema Nwachukwu, said members of the Civillian-JTF on a stop and search duty in Konduga were deceived by the old man whom they allowed to inch too close to their post for a check of the content of the bag he was carrying.

It has been a usual practice of the Boko Haram to deploy mostly teenage boys and girls in carrying out suicide bombing attacks.

But unknown to the vigilante members, the aged man was actually a Boko Haram member on a mission to carry out attack in Konduga, a community 35km from Maiduguri.
He detonated the explosive devise contained in the bag, which resulted in killing himself and three of the Civilian-JTF operatives.
"The elderly man pretending to be weak and feeble was being searched by men of the Civilian Joint Task Force, when he detonated a suicide vest contained in a bag he was carrying," Mr Nwachukwu said.
"Unfortunately three Civilian Joint Task Force members paid the supreme price in the incident. The wounded have been evacuated for medical attention.
"Our hearts go out to those who lost their lives as well as those injured in the callous attack."
Mr Nwachukwu, an army colonel, said the Konduga incident "points to the variation in the tactics of the Boko Haram terrorists in their uncanny resolve to deceptively infiltrate communities and towns to mindlessly attack vulnerable and soft targets.
"Aside using women and children, the terrorists are now engaging the aged in suicide bombing as witnessed in this recent incident."
He warned members of the public to cast their net of suspicion beyond looking for dirty and scraggy looking individuals as suspected suicide bombers.
"They (Boko Haram) have also been detected to now appear clean and well dressed to look unsuspicious and enable them gain access to targets marked for suicide attack. Some of the terrorists have also been found to now conceal their suicide vests by wearing it on the thigh rather than the waist to appear less bulky and evade detection when searched.
"In view of these developments, members of the public are please urged to be vigilant and discerning as they go about their normal daily routines and activities."
Meanwhile, Mr Nwachukwu said a combined force of the Operation Lafiya Dole and the Cameroonian Defence Forces "have killed 15 Boko Haram

insurgents in separate encounters in Southern Lake Chad Basin.

"Troops neutralised the insurgents whilst conducting operations to clear remnants of Boko Haram insurgents in the Lake Chad Islands and surrounding villages of northern Borno yesterday.

"Troops dislodged the insurgents from their hideout after a fierce battle, killing 11 insurgents in Gomaran village of Southern Lake Chad Basin."

"In two other separate encounters with the fleeing insurgents in Firgi and Moula, both in Bama and Dikwa Local Governments Areas of Borno State, troops also ambushed and neutralised 4 Boko Haram insurgents who were fleeing troops ' onslaught in the northern fringes."

He added that the "clearance operations also led to the recovery of one single barrel gun, one Dane gun and one locally made pistol. Other items recovered from the dislodged insurgents include 4 Motorcycles, motorcycle spare parts, 2 tricycles, 6 pumping machines, and 2 power generating sets. Additionally, the valiant troops captured 2 Boko Haram flags, a pair of camouflage uniform, a pair of combat boots, a camera, a bag of mechanical tools and medications."

"Four men, 33 women and 16 children were rescued by the troops from the insurgents' hideouts . The rescued hostages are currently being profiled for subsequent hand over to officials of the Internally Displaced Persons Camp for documentation and administering."

Three families were behind the ISIS-inspired bombings in Indonesia's Surabaya, police said

Source: https://edition.cnn.com/2018/05/13/asia/indonesia-attacks-surabaya-intl/index.html

May 15 – A spate of deadly, ISIS-inspired bombings that rocked Indonesia's second-largest city in 24 hours were carried out by three families -- including their young children -- who targeted churches and the police, authorities said.

In the latest attack on Monday morning, a family of five rode two motorcycles to the front gate of Surabaya's police headquarters before detonating explosives, injuring 10 people.

On Tuesday, police identified the couple as Tri Murtiono and his wife Tri Ernawati, who carried out the attack accompanied by their sons, aged 18 and 14, and their 7-year-old daughter. CNN had previously reported that the girl was eight, per police statements.

She was riding as a passenger on one of the bikes and was thrown clear of the explosion, police spokesman Frans Barung Mangera said. A video of the scene showed her staggering through the rubble before a bystander picked her up and carried her to safety.

The bombing came one day after a family of six, including four children, detonated explosives at three churches, killing 12 people and injuring at least 40.

The father, identified by police as Dita Oepriarto, was said to have driven his wife Puji Kuswat and their two daughters, aged 9 and 12, to the Indonesian Christian Church. The trio went inside and detonated a bomb.

Oepriarto then drove the van to the Pentecostal Central Church, where, from inside the vehicle, he detonated another bomb, police said.

Around the same time the couple's two teenage sons, aged 16 and 18, drove motorcycles to the Santa Maria Catholic Church, where they also detonated bombs. All members of the family died in the attacks, which ISIS claimed responsibility for via its Amaq News Agency in what it called "a martyrdom operation."

Later Sunday, in what police also described as a terror incident, a mother and her 17-year-old daughter were killed in the Surabaya suburb of Sidoarjo when a bomb handled by the family's father detonated prematurely. Police found the father of the family in a house holding a detonator and shot him, police spokesman Barung Mangera said.

The family's 12-year-old son took his two younger sisters to the Bhayangkara Police Hospital, he added.

A damaged motorcycle is seen outside the Surabaya Centre Pentecostal Church in Surabaya on May 14.

Tito Karnavian, Indonesia's top-ranking police officer, told reporters Monday that police were working on the assumption that the attacks followed a directive from ISIS Central Command to avenge the imprisonment of the former leaders of Jamaah Ansharut Daulah (JAD), an Indonesian jihadi group that supports ISIS.

Indonesia, the world's most populous Muslim country, has struggled in recent months with a rise in Islamist militancy, which has come as ISIS has been squeezed out of its heartland in Syria and Iraq.

Karnavian also told reporters Monday that none of the families involved in the attacks had recently traveled to Syria, but Oepriarto had close links with someone who had recently returned from Syria who may have inspired him to carry out the attacks.

"These attacks are the nightmare scenario that's been anticipated since Indonesians affiliated with ISIS have returned from the Middle East," said Greg Barton, Chair in Global Islamic Politics at Deakin University in Australia.

Families linked

In an exclusive interview with CNN, Oepriarto's father said his son was close friends with the man involved in the explosion in the suburb of Sidoarjo on Sunday evening.

"He's never spoken about it, but I know my son is close friends with Anton," Raden Doddy Oesodo said, referring to the man who died in the affordable housing complex in Sidoarjo after a bomb detonated prematurely.

"Anton was my son's buddy in high school. Anton is my son's junior within the JAD organization. My son, his wife and Anton were part of the same JAD membership," he said, adding that his son was introduced to JAD in high school.

Oesodo described Oepriarto as "reclusive" and "private," but said he never spoke about martyrdom or traveling to Syria. "I've never heard him talk about jihad, but my son often disagrees with government policies."

Sitting in his home, Oesodo held a family photo of Oepriarto and his three other children and spoke about his love for his family.

"I love my grandchildren very much. They died because of their father's ideology," Oesodo said.

"I want to apologize to Surabaya residents who have become a victim due to my son's actions. I apologize from deep within my heart, especially to those who died because of him."

'Opening salvo'

Formed in 2015, the group linked to the attacks, Jamaah Ansharut Daulah (JAD), is a jihadi group that supports ISIS, according to Jakarta officials.

Its leader, Aman Abdurrahman, was scheduled to appear at a court hearing last week, but it was postponed after a deadly riot broke out at the jail where Aman is being held in Depok, West Java, according to a report in the Jakarta Post.

Police now believe the riot at the Mobile Brigade Detention Center was initiated by a convict acting on the ISIS Central Command's instruction.

The militant group is part of a "second wave" of terrorist groups to be active in Indonesia, according to Hugo Brennan, senior Asia analyst at Verisk Maplecroft, a risk consultancy firm.

"The first wave was linked Al Qaeda from 2001 and were involved in the Bali attacks. Indonesian security forces dealt with them fairly effectively.

"Then in 2014 there was an uptick in violence as groups linked to ISIS became active, stoked by online propaganda, militants who traveled to the Middle East and fighting in the Philippines. The attacks yesterday are part of a pattern ... but (are among) the more sophisticated, and as it involved children, heinous."

Barton at Deakin University said the Surabaya attacks could be the "opening salvo of a new, more sophisticated campaign," and added that the timing -- just before Ramadan, which begins May 15 -- "bears the hallmarks of ISIS," which has used the holy month in the past to launch high profile attacks.

"This is the first Ramadan since ISIS-linked Indonesians have returned" from Syria, he said.

Indonesia has a long history with terrorist groups, particularly the al-Qaeda affiliated group Jemaah Islamiyah, which claimed responsibility for 11 attacks between 2000 and 2010, including the deadly 2002 Bali bombings that left more than 200 people dead and hundreds injured, many of them tourists.

According to Wawan Purwanto, the information and communication direct of Indonesia's National Intelligence Agency, around 930 Indonesians have traveled to Syria and Iraq to fight alongside ISIS since 2013.

Of those, around 400 had returned to Indonesia while 100 are known to have died in battle. Exact numbers are uncertain because immigration officials in Iraq and Syria don't have a record of them entering those countries, Wawan said.

The United Nations Secretary-General condemned the three terrorist attacks on the Surabaya churches. Through his spokesman, Stephane Dujarric, Secreatry General Antonio Guterres said that he was "appalled at reports that children were used to participate in the attacks," and offered his condolences to the families of the victims.

"(The Secretary General) reiterates the support of the United Nations to the Government and people of Indonesia in their efforts to fight and prevent terrorism and violent extremism, including through the promotion of pluralism, moderation and tolerance," the statement said.

More than 82% of Indonesia's roughly 261 million people follow Islam. Almost 10% of the population is Christian.

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

CYBER NEWS

How cybercriminal spend their illicit gains

Source: http://www.homelandsecuritynewswire.com/dr20180424-how-cybercriminal-spend-their-illicit-gains

Apr 24 – A University of Surrey Senior Lecturer in Criminology has teamed up with virtualization technology company Bromium to produce "Into the Web of Profit," a research study revealing the socio-economic and spending differences among cybercriminals.

Bromium, a specialist in application isolation using virtualization-based security, have announced the findings of an independent, academic study into how much money cybercriminals are earning, and what they spend it on.

The findings are part of a larger 11-month study titled Into the Web of Profit, commissioned by Bromium and written by Dr. Mike McGuire, Senior Lecturer in Criminology at the University of Surrey. It draws on first hand interviews with convicted cybercriminals, data from international law enforcement agencies, financial institutions, and covert observations conducted across the Dark Web.

Surrey says that research in the report reveals how income and spending are almost cliché. While cybercriminals do not have to pay taxes on their income, their annual earning level might push them into some of the higher brackets.

- **High earners make up to $2m/£1.4m – almost as much as a FTSE250 CEO**
- **Mid-level criminals make up to $900,000/£639,000 – more than double the U.S. presidential salary**
- **Entry level hackers make $42,000/£30,000 – significantly more than the average U.K. graduate.**
- **Data gathered through first-hand interviews with 100 convicted or currently engaged cybercriminals, combined with Dark Web investigations, reveals that:**
- **15 percent of cybercriminals spend most of their money on immediate needs – such as buying nappies and paying bills**
- **20 percent of cybercriminals focus their spending on bad habits – like buying drugs or paying prostitutes**
- **15 percent of cybercriminals spend to attain status, or to impress romantic interests and other criminals – for example, buying expensive jewelry**
- **30 percent of cybercriminals convert some of their revenues into investments– such as property or financial instruments, and other items that hold value such as art or wine**
- **20 percent of cybercriminals spend at least some of their revenue on reinvestments in further criminal activities – for example, buying IT equipment.**

The report notes a growing market catering to cybercriminals by allowing them to buy things with virtual currency. Sites such as White Company, Bitcoin Real Estate, and de Louvois offer luxury products priced in Bitcoin, which is becoming a concern for financial analysts.

McGuire said: "The range of spending habits among cybercriminals was fascinating. A lot of cybercriminals spend their money on increasing their status, whether that be with peers or romantic interests. One individual in the U.K., who made around £1.2m per year, spent huge amounts of money on a trip to Las Vegas, where he claimed to have gambled $40,000 and spent $6,000 hiring sports cars so that they could "arrive in style" to casinos and hotels.

Another U.K. cybercriminal funneled his proceeds into gold, drugs, expensive watches and spent £2,000 a week on prostitutes. It's alarming how easily cybercriminals are able to spend their illicit gains – there is an ever-growing market that is almost tailor-made for cybercriminals to make these ostentatious purchases with little to no regulation or oversight."

— Read more in Michael McGuire, "Into the Web of Profit: Tracking the Proceeds of Cybercrime" (paper presented at the RSA Conference, San Francisco, 20 April 2018). Register to download the full report: learn.bromium.com/rprt-web-of-profit.html

Cyber criminals earn $1.5 trillion through Amazon, Facebook and Instagram exploitation

Source: https://www.independent.co.uk/life-style/gadgets-and-tech/news/cyber-criminals-facebook-amazon-instagram-earnings-terrorism-trafficking-money-laundering-tech-a8313801.html

May 01 – The exploitation of companies like Amazon, Facebook, and Instagram has caused a $1.5 trillion boom in cyber crime, according to new research.

The study by Dr Michael McGuire, senior lecturer in criminology at the University of Surrey, explored methods by which a new breed of opportunistic criminals are using major technology platforms for drug dealing, money laundering, human trafficking and even terrorism.

"What is astounding is just how much cyber criminals are profiting from these platforms," Dr McGuire told *The Independent*. "It's an incredibly lucrative economy — $1.5 trillion is actually a pretty conservative estimate."

Gadgets and tech news in pictures

The research follows revelations that UK data firm Cambridge Analytica collected personal information from 87 million people after an online quiz was used to take advantage of Facebook's data and security settings.

According to Dr McGuire, Cambridge Analytica is "just the tip of the iceberg" when it comes to the manipulation of social media firms and other technology companies.

"It's more of a question of which platforms aren't being misused," Dr McGuire said. "AirBnb and Uber are being used to move money around, Instagram has become a hotbed for illicit drug dealing, while eBay and Amazon are being used to peddle counterfeit goods and bypass local tax laws."

The study refers to this new model of cyber crime as "platform criminality," explaining how large criminal organisations are profiting from this burgeoning cyber economy.

The $1.5 trillion profits obtained through these platforms are equivalent to the GDP of Russia, the study notes.

"The findings of Dr McGuire's research provide shocking insight into just how widespread and profitable cyber crime has become," said Gregory Webb, the CEO of Bromium, the cyber security firm that commissioned the study.

"The platform criminality model is productising malware and making cyber crime as easy as shopping online… We can't solve this problem using old thinking or outmoded technology. It's time for new approaches."

The companies involved are yet to be approached with the study's findings, though Dr McGuire hopes his research will bring their attention to the issue.

"Approaching these companies is the next step," Dr McGuire said. "A lot of them are aware of the issue but it's operating at such a scale that it's difficult to see what they will do about it.

"They need to come down from their pedestals and engage with criminology experts in order to have meaningful dialogues that will lead to meaningful results."

Dr McGuire is set to present the findings of the study at the RSA Conference in San Francisco on Friday, 20 April.

Against cyber terrorism: Europol shut down one of the dangerous sites

Source: http://micetimes.asia/against-cyber-terrorism-europol-shut-down-one-of-the-dangerous-sites/

May 04 – The website Webstresser.org was considered one of the world's largest services on the implementation of the customized DDoS attacks.
Europol reported on the results of international operations for site closure **WebStresser, which gave everyone the opportunity to order a DDoS attack on the Internet by paying €15 per month.**
This was reported on the website of the organization.
It is noted that on 24 April the resource managers arrested in the international operation Power Off – the arrests were made in the UK, Croatia, Canada and Serbia.
Webstresser.org was considered one of the world's largest services on the implementation of the customized DDoS attacks. At the close it was 136 thousand registered users.
Over the past few years with WebStresser was made more than 4 million attacks. Objectives have become critical online services, banks, government resources, and servers of the gaming industry.

What to Expect in 3rd Generation Cybersecurity?

Source: https://i-hls.com/archives/82805

May 02 – China's first- and second-generation cybersecurity systems relied on blacklists and whitelists to screen out potential threats, but hackers can always find a way to get around such lists, and attackers can also hide their presence. AI and big data-support are ready for a role in the development of the country's third-generation cybersecurity defense system, evaluates China's leading cybersecurity company, **360 Enterprise Security Group**.

"A cybersecurity system that monitors online behavior will be more efficient. Based on big data and AI behavioral analysis, the third-generation system will be able to identify an attack through intelligence on threats. Behaviors that go against the baseline set up by the system will be reported and warnings will be given," said Qi Xiangdong, the company chairman. He noted that the baseline can be adjusted to mark out abnormal behaviors that differ from usual ones.
The new defense system, like the previous ones, will mainly serve businesses and institutes rather than individuals. Hence, it will only look for abnormal activity targeting those institutes. "It will not put personal privacy at risk or damage personal information," Qi stressed, according to en.people.cn.
For example, if a user usually visits a certain company website only once a day, then its baseline will be identified as breached if the website is viewed over 1,000 times a day.

Hackers Shut Down Gas Pipeline Infrastructure Through Third Party

By Thomas Pore

Source: https://www.hstoday.us/subject-matter-areas/cybersecurity/hackers-haunt-pipelines-as-silent-shut-off-valve/

May 08 – All operations on the natural gas pipelines for four different U.S. energy companies were running smoothly until the moment they were inexplicably shut off. It is a moment that sends panic down the pipelines and through the teams operating them.
Oneok Inc., with pipelines in Texas and the Rocky Mountains region, Energy Transfer Partners LP, Boardwalk Pipeline Partners LP, and Chesapeake Utilities Corp.'s Eastern Shore Natural Gas were shut down temporarily in March within a week of each incident. This calamity was traced to a third-party provider: Latitude Technologies unit of Energy Services Group, which got hit by a cyberattack on their communication systems.
These attacks being investigated by Homeland Security come on the heels of a U.S. government warning that hackers were conducting cyberattacks on the U.S. power grid and

other targets. It was also a wake-up call to pipeline and critical infrastructure operators that nation-state and other attackers are continuously probing critical infrastructure networks for weaknesses. One of the most serious malware to hit critical infrastructure systems last year was discovered by FireEye, who named it Triton because it targeted Schneider's Triconex plant safety systems. This virus is capable of disrupting industrial processes.

In the wake of these increasing attacks, the National Institute of Standards and Technology recently released an update to its cybersecurity framework for organizations that gives additional instructions for managing the supply chain cybersecurity, which poses significant vulnerabilities. NIST is expected to release a roadmap for improving critical infrastructure cybersecurity later this year.

Evolving Security

The ramping up of hostilities around the world combined with now various connections to the Internet for critical SCADA systems, combined with the ability to jump air-gap systems, has now provided a widespread threat landscape for attackers.

For decades, critical infrastructure operators have attempted to prevent breaches with a security strategy focused on perimeter defense or relayed on air-gapped systems. Technologies like firewalls, antivirus, intrusion prevention systems (IPS), network access control (NAC), and access control lists (ACLs) were leveraged in an effort to secure systems and were, for the most part, very successful. However, the last five years has brought significant change with new technologies that are propelling the industry at light speed. Combining the massive growth of attack surfaces driven by the Internet of Things (IoT), coupled with the increasing sophistication of malware and a seemingly infinite number of attack vectors, has led to a point where breaches are inevitable.

Critical infrastructure facilities must continue their efforts of prevention, but it is imperative that they also evolve their strategy to include technology, people, and processes dedicated to incident response.

Detection alone is not enough. Knowing there is a problem is just the first step. When the security team receives an alarm, they must be able to identify what the breach was, determine root cause, mitigate, and return to normal. This process requires forensic data that delivers context extending to network traffic associated with the event. Network Traffic Analysis (NTA) platforms incorporating artificial intelligence and historical forensic data are key to this shift in security strategies.

Effective incident response processes require four key capabilities that come from a combination of people and deployed technology:

1. The ability to collect data on network traffic that goes far beyond syslogs. Teams must centrally collect information that spans all seven layers of the OSI model (physical all the way to application data).
2. Security teams must be able to quickly correlate and navigate all of that data in a way that delivers context and insight.
3. The team should have a documented response process, including advisory guidelines for specific types of attacks, to guide them through the investigation.
4. There should be pre-defined automation mechanisms for dynamic mitigation. Advances in artificial intelligence will make this process more precise and efficient over time.

Critical infrastructure facilities are directly in the crosshairs of well-funded, sophisticated nation-state hackers. NIST is providing the guidance, but critical infrastructure operators themselves must be on the leading edge of security, going beyond strategies focused only on prevention and embracing the need for people, processes, and technologies dedicated to incident response. It is imperative that they be prepared to quickly react to inevitable breaches to avoid the catastrophic effects that are all too real.

Thomas Pore *is an expert in network behavior and cyber threat intelligence analysis. He is a regularly quoted as a cyber security resource for global media outlets and is an adjunct professor teaching ethical hacking. Pore is currently Director of IT and Field Engineering at Plixer. His responsibilities include establishing, planning and implementing the company's IT and security policies and procedures, leading the Professional Services team and driving product features and roadmap. He established, and is responsible for, the Malware Incident Response and Advanced NetFlow Training programs offered throughout the USA. Pore regularly travels the world meeting with customers, helping them optimize threat detection strategies and incident response solutions.*

Cascading Consequences: Electrical Grid Critical Infrastructure Vulnerability

By George H. Baker & Stephen Volandt

Source: https://www.domesticpreparedness.com/resilience/cascading-consequences-electrical-grid-critical-infrastructure-vulnerability/

May 09 – If there were a prolonged nationwide, multi-week, or multi-month power failure, neither the federal government nor any state, local, tribal, or territorial government – acting alone or in concert – would be able to execute an effective response. This bleak outlook results from understanding that so many critical infrastructures depend on electricity. As such, effective recovery cannot be expected through top-down assistance alone. Without electric power, the goods and services essential to protect life and property would be at risk by day three or perhaps longer depending on preparedness levels. Consequently, it is vital that citizens, households, communities, businesses, and governments be as informed and prepared as possible.

Citizens of the United States are dependent on secure and reliable electric power for their current way of life. **If electric power were not available for weeks, months, or even a year, then cascading impacts would degrade multiple critical infrastructures, for example:**

- Water supply and wastewater treatments;
- Telecommunications and the internet;
- Food production and delivery;
- Fuel extraction, refining, and distribution;
- Financial systems;
- Transportation and traffic controls;
- Government, including public works, law enforcement, and emergency services;
- Hospitals and healthcare;
- Supply chains; and
- Other critical societal processes.

Loss of life could be catastrophic. Life itself would change.

The recently published InfraGard community preparedness guide, *Powering Through: From Fragile Infrastructures to Community Resilience (*hereafter *Powering Through)*, states that no post-industrial society has yet experienced a widespread and prolonged electric blackout. Thus, nations that develop resilience and recovery plans for long-term, wide-area electric power blackouts are in uncharted territory. Although there may be unforeseeable points of failure, cascading effects, and barriers to recovery, plans can still be made for prevention, mitigation, adaptation, and recovery. Imperfect plans, thoughtfully developed, are far better than no plan at all.

This article examines the national power grid and the most significant threats to it. Of particular note, Dr. George Baker developed and others helped refine an important matrix of impacts from five threats to the grid and other key infrastructures. Threats evaluated include:

- Coordinated physical attacks;
- Cyberattacks against industrial control systems and/or other cyber-enabled technology;
- An electromagnetic pulse (EMP) generated by detonation of one or more nuclear warheads in the upper atmosphere over the United States;
- An EMP caused by a coordinated attack using radio frequency weapons; and
- A severe solar storm caused by an Earth-directed coronal mass ejection (CME).

Some human-caused threats might utilize a natural disaster to mask and extend infrastructure damage.

High-Impact Risks to the Electric Grid & Other Critical Infrastructures

There are two types of hazards: *naturally occurring events*, such as a solar geomagnetic storm, a pandemic, or other random events; and *acts of human volition*, such as a human-caused electromagnetic pulse (EMP) attack, a coordinated cyberattack, or a coordinated set of physical attacks on critical grid equipment or related critical infrastructures. This article, drawn from *Powering Through*, presents a summary of the risks associated with

dependencies on technologies that are increasingly vulnerable to the "triple threat" of cyber, solar geomagnetic storms (GMD), and electromagnetic pulse (EMP) weapons (see Table 1).

Table 1. Potential Impacts on Critical Infrastructure Affecting the Electric Grid

Equipment at risk	EMP (nuclear)	Solar storm	Cyber	Physical attack	Radio frequency weapons
Transformers	R	R	R-Y	R	R
Generator Stations	R	G	R	R	R
SCADA/Industrial Controls	R	R	R	R	R
Utility Control Centers	R	R	R	R	R
Telecommunications including cellphones	R	R	R	Y	Y
Radio Emergency Communications	R	P	Y	Y	Y
Emergency SATCOM Communications	R	P	Y	Y	Y
Internet	R	R	R	Y	Y
GPS	R	P	Y	Y	Y
Transportation	R	Y	Y	Y	Y
Water	R	Y	R-Y	Y	Y

Legend: Red = direct permanent effects. Yellow = Cascading effects if no backup power. Pink = temporary effect (0.5-36 hours) assuming backup power. Gray = direct effects uncertain. Red-Yellow = potential permanent effects plus cascading effects.

Comments From *Powering Through* on Equipment at Risk

Transformers – Transformers are vulnerable to EMP, solar GMD, or physical attacks. Because unprotected relays supporting transformers can be rapidly opened and closed, transformers may be damaged or destroyed via remote manipulation. Radio frequency weapons can be used to disable substation controls, but are unlikely to affect the transformers themselves directly unless targeted substation supervisory control and data acquisition (SCADA) systems cause secondary damage. If these are attacked and disabled, then the time to replace high-voltage and ultra-high-voltage transformers is likely to be lengthy, and often dependent on overseas manufacturers. There are smaller transformers, designed to serve the residential and small business consumer, that are generally less vulnerable, more easily transportable, and manufactured in the United States. Hence, these transformers might be replaced relatively quickly.

Generator Stations – Unless protected, grid generators at electrical power stations may be disabled by an EMP. Generator control electronics are highly susceptible to EMP. If there is a severe solar storm, there is evidence that the generators themselves could be harmed. Cyber, physical, or radio frequency weapon attackers may target grid generator stations.

SCADA/Industrial Control Systems (ICS) – These industrial control devices regulate the operation of machinery, breakers, and transformers. SCADA systems are vulnerable to EMP and radio frequency weapons (RFWs). Solar GMD could debilitate SCADA operations if SCADA electronics are connected to long landlines. Since they are accessible from the internet, they may be targeted in cyberattacks. They also may be targets of physical and RFW attacks.

Grid Control Centers – Control facilities vary in size and are the hubs for grid communication and SCADA networks. They provide important situational awareness for directing both normal grid operation and grid reconstitution following a blackout. Because of

their long-line interfaces, they are highly susceptible to EMP and GMD effects. If communications lines going into or out of the center were disabled, SCADA functions would be disabled. A cyberattack could target the SCADA devices used in the control center. The facilities could be targets for physical and RFW attacks.

Cellphones – Although many individual cellphones may be unharmed, the phones depend on cell towers interconnected with the local and long-haul telecommunications networks, which are vulnerable to EMP, GMD, RFW, cyberattacks, and physical attack.

Radio Emergency Communications – Some of the emergency radio systems – such as the Federal Emergency Management Agency, National Radio System – continue to work if they are hardened. However, in an EMP, public radio stations and their power sources may not be hardened and may fail. In a solar storm, this communication may be temporarily disabled by atmospheric conditions, but could return in hours to days. The other threats would not affect radio systems if the attack were focused on the grid.

SATCOM – The military's Military Strategic and Tactical Relay, MILSTAR system is EMP protected and will continue to operate. Some additional military portable UHF SATCOM radios that link through high-orbit geo-stationary satellites may also continue to function. Unhardened ground stations may fail in an EMP environment. Commercial satellite phones rely on satellite and ground stations that are likely to fail under EMP stress.

Internet – An EMP would disable key elements of the internet and users' IT equipment. A cyberattack on the grid taking out the generators, SCADA devices, and control centers would also have a cascading effect on internet data centers depending on the capacity and longevity of their back-up power resources. A solar storm can damage long-haul internet interconnects including both metallic and fiber optic links (the latter due to the vulnerability of optical fiber regeneration equipment). Physical or RFW attacks targeting grid assets would disable local internet equipment within Endpoint Group data centers and substation control facilities, but leave the larger internet intact.

Transportation – Railroad signals and highway traffic signals could be directly damaged by an EMP and cause significant delays. Controls and communications elements that use rails for transmitting communications signals are in great jeopardy if not protected and tested. A solar storm should not disable these transportation items if backup power is available for the duration of the grid failure. Likewise, a cyberattack or RFW attack on the grid would not disable transportation systems if backup power is available. In a widespread grid blackout, standard operating procedures to close ports safely could result in delays in prioritized reopening of U.S. ports that are essential for throughput of disaster relief supplies. Chemicals or liquefied natural gas facilities within ports could benefit from backup power capabilities that prevent hazardous chemical releases due to loss of external power. In turn, preventing these chemical releases could avert extended port shutdowns after regional grid blackouts and help to re-establish priority supply chains and accelerate lifesaving and recovery operations.

Water – Because water purification and wastewater purification plants are controlled by SCADA devices, these could be disabled by EMP. Backup emergency diesel generators and solar panels are also vulnerable to E1 pulses (the first of three electromagnetic pulses created by an EMP) unless the generators and the solar panel inverters and controllers are EMP-protected. A cyberattack or RFW attack on the grid would not directly disable the water/wastewater systems if protected backup power were available. Nevertheless, if electric substations continue to be exempt from cyberprotection standards for "high-impact" grid assets, adversary takeover of substation controls could disable aqueduct pumps and locks, as well as other water and wastewater pumps and motors that provide essential water pressure and that process and manage wastewater products.

Probability

Powering Through states:

> *The likelihood of natural event hazards is generally independent of efforts to prevent, mitigate, or recover from such events. Solar storms cannot be deterred, though the consequences can be mitigated. In contrast, the likelihood of volitional acts may be affected by both preventive measures and by the deterrent effects of initiatives to mitigate and recover.*

Powering Through continues:

> *Severe solar geomagnetic storms have been recorded over recent millennia, but their impact on electrical systems has been measured with increasing accuracy only since the August-September 1859 Carrington event. Various models in the past decade estimate the probability of severe solar geomagnetic storms – of the magnitude of the Carrington event or the May 1921 New York Central Railroad storm – as approximately 8% to 12% per decade.*

It is very important to examine the consequences of a long-term power outage and not to concentrate on the probability.

In more than seven decades since nuclear weapons were employed in World War II, a high-altitude electromagnetic pulse (HEMP) attack has not occurred. EMP-optimized atmospheric testing occurred before a Limited Test Ban Treaty, a ban on testing in outer space, the atmosphere, or underwater, took effect in 1963. Deterrence of nuclear weapon use has been successful to date. However, the past may also be a prologue.

Even if most nation states are deterred, not *all* nation states (including failed states) and all subnational groups will be deterred if EMP vulnerabilities are not addressed and diminished. There is no credible way to assign a probability to HEMP attack or to ground-based or cruise missile radiofrequency weapons employment that may not violate the Environmental Modification Convention. However, it is reason for concern that approval for asymmetrical warfare, including a HEMP attack, is found in foreign military literature.

With these diverse hazards in mind, it is essential to recognize that government entities at the federal and state levels cannot protect critical infrastructures by themselves. Public-private partnerships will be necessary, and planning concepts and suggestions for broader audiences must extend beyond government.

Readiness Gap

The authors have considered various scenarios that range from two to three weeks without power on a regional basis, to continent-wide loss of power for over one year. It is certainly possible for an adversary or solar weather to disrupt electrical power for longer than a year. Accepting this possibility is the first major step in readiness planning. Aiming for readiness that can address a one-year outage is daunting; however, that effort will do much to provide for limited-term outages of up to two-three months. Recent events in Puerto Rico caused by Hurricane Maria make it obvious how challenging it can be to restore electrical power even with the remainder of the nation providing assistance.

As of 26 September 2017, 95% of the island was without power and, due to the cascading effects of power loss, less than half the population had tap water and 95% had no cellphone service. Two weeks after the hurricane, 89% of the population was still without power, 44% without water service, and 58% without cell service. One month after the hurricane, there was only slight improvement as 88% of the population lacked power, 29% lacked tap water, and 40% lacked cell service. Three months after the hurricane, 45% of the population still had no power (1.5 million people) and 14% had no tap water; cell service was returning, with over 90% of service restored and 86% of cell towers functioning.

Powering Through observed:

> *On its Ready.gov website, the U.S. Department of Homeland Security advises the American public to store food and water for at least three days. As useful as that is for a starting point, high-impact events must also be considered. Many who assume that the government will provide support as soon as day four may think that they do not need to plan for extended emergencies at all.*

In the West now, they are encouraging their citizens to be prepared for two weeks. This is significantly better than three days.

Powering Through continues to illustrate that:

> *In the event that a widespread failure of electrical power, which takes down critical infrastructures for a much longer duration, sufficient relief, whether from government and/or other sources, probably will not be available. Depending on the duration of the infrastructure failure, consequences for unprepared citizens could go well beyond economic loss to include sickness and death from dehydration, disease, pollution, exposure, starvation, fire, and civil unrest. Consequences for the nation could include a breakdown of coherent central government (local, state, and federal), leading to possible loss, at least temporarily, of effective sovereignty: the full right and power of governing bodies to govern*

themselves without outside interference. There could also be unacceptable delays in recovery, resulting in extensive loss of life and property. All of these are unacceptable risks.

The U.S. House of Representatives has passed several bills that address U.S. electric power grid vulnerabilities. The Federal Energy Regulatory Commission sponsored research at Oak Ridge National Laboratories to characterize EMP effects on the national power grid. There are several indications that these threats are being taken seriously by federal officials. For example, the White House National Science and Technology Council's National Space Weather Strategy and National Space Weather Action Plan are strong indicators. In addition, the Defense Threat Reduction Agency has recognized the EMP effects on the national electric power grid in a request to strengthen the critical civil infrastructure on which military facilities in the United States depend for at least 98% of their electricity. The Department of Energy and Electric Power Research Institute issued a Joint Electromagnetic Pulse Resilience Strategy in July 2016. The Department of Homeland Security Office of Infrastructure Protection explicitly noted the EMP threat to the cyber industry in the public and more detailed "For Official Use Only" reports issued in 2016 by the Regional Resiliency Assessment Program. All of the foregoing initiatives validate the threat.

However, no plan or preparation exists at the national level that addresses long-term electrical power outages that span large regions or the continent. In such a case, there would be no neighboring state or region that could provide the depth of assistance required to promptly assist the general public, businesses, and local or state governments. Each region would be grappling with its own problems (see Figure 1).

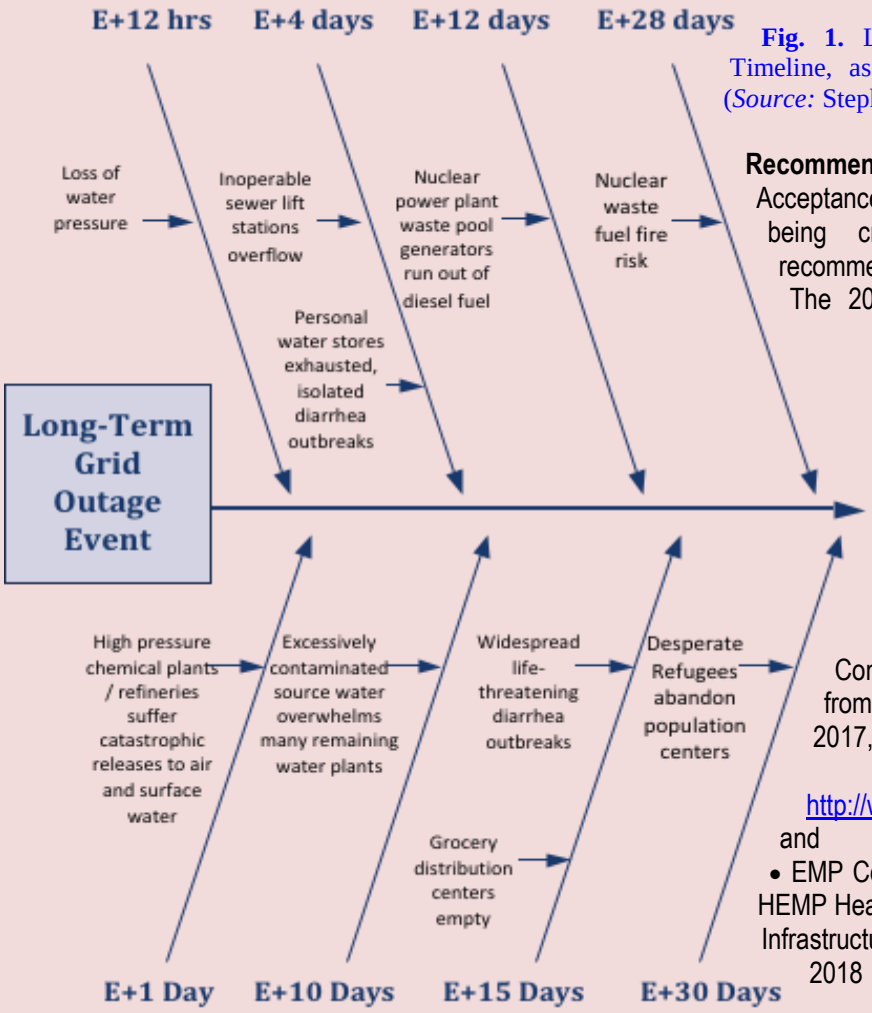


Fig. 1. Long-Term Power Outage Worst Case Timeline, as shown in *Powering Through*, p. 166 (*Source:* Stephen Volandt, Auroros Incorporated).

Recommendations

Acceptance of the threats presented in this article as being credible is the first step in any recommendation. For example, Section 1913 of The 2018 National Defense Authorization Act addresses EMP specifically. Additionally, The Congressional EMP Commission has been granted permission to publicly release two reports regarding EMP:

- EMP Commission, Volume I, Assessing the Threat from EMP Attack – Executive Report, July 2017, publicly released April 2018 and available at: http://www.dtic.mil/dtic/tr/fulltext/u2/1051492.pdf; and
- EMP Commission, Volume II, Recommended E3 HEMP Heave Electric Field Waveform for the Critical Infrastructures, July 2017, publicly released April 2018 and available at: http://www.dtic.mil/dtic/tr/fulltext/u2/1051494.pdf

Overall, a strategy to protect and rapidly restore lifeline sectors – including water, electricity, food, medical and emergency services, and telecommunications – offers the potential to maximize "shelter in place" capabilities and minimize uncoordinated evacuations.

Uncoordinated evacuations have the potential to escalate threats to public safety, protection of supply chains, and equitable distribution of life-essential goods and services.

As stated in the *Powering Through* preparedness guide:

> *The United States needs to augment the planning and investments that are essential to cope with extended duration catastrophes. Whole community participation in both planning and recovery must be the new norm, and this vital process needs to start now and continue. The fundamental criterion for success should be prepared individuals and communities capable of surviving long-term infrastructure failure, while at the same preserving families, assisting others in their communities, and defending the nation.*

The White House National Science and Technology Council in October 2015 issued the National Space Weather Strategy and the National Space Weather Action Plan, calling for the "whole of community" to plan for a severe solar storm and noting that other threats could cause similar effects. In 2016, the Department of Energy and the Electric Power Research Institute issued a Joint Electromagnetic Pulse Resilience Strategy for the national electric power grid. Also in 2016, the Defense Threat Reduction Agency recognized the operational importance of grid survivability in the event of an EMP, and requested proposals to strengthen the private sector and military critical infrastructure upon which defense missions depend. The Department of Homeland Security Office of Infrastructure Protection specifically noted the EMP threat to the telecommunications industry in a 2016 report prepared for the Regional Resiliency Assessment Program. Finally, the 2018 National Defense Authorization Act calls out the vulnerability of military bases caused by their dependence on the electrical power grid instead of relying on locally produced electricity. The foregoing documentary findings validate the threat and underscore the urgent need for infrastructure planning and protection. Assessments are still needed for households, communities, and organizational readiness to manage the risks described in this article.

InfraGard, more formally the InfraGard National Members Alliance is a nonprofit consisting of more than 50,000 volunteers committed to assessment and protection of critical infrastructures throughout the United States. InfraGard sponsored the December 2016 publication of Powering Through: From Fragile Infrastructures to Community Resilience, an Action Guide Powering Through, Version 1.0, which was researched and prepared by InfraGard's Electromagnetic Pulse Special Interest Group (EMP-SIG) volunteers. Powering Through examines actions that could be taken now to be more resilient, protect life and property during grid outages, and prepare for expedited recovery. Most of the content of this article is taken from this action guide, which is available at: https://www.amazon.com/Powering-Through-Infrastructures-Community-Resilience/dp/0998384402

Dr. George H. Baker, *is a professor emeritus at James Madison University, where he directed the JMU Institute for Infrastructure and Information Assurance. Previously, he led the Defense Nuclear Agency's Electromagnetic Pulse (EMP) program, directed the Defense Threat Reduction Agency's assessment arm, and served as a senior scientist for the Congressional EMP Commission. He is a member of the Foundation for Resilient Societies' board of directors. He holds an M.S. in Physics from University of Virginia, and a Ph.D. in Engineering Physics from the U.S. Air Force Institute of Technology. Currently, he is CEO of BAYCOR, LLC – a consulting company primarily devoted to preparedness for and protection against major electromagnetic threats to critical infrastructures including nuclear EMP, solar storms, and radio frequency weapons.*

Stephen Volandt, *vice president of Auroros Inc., currently serves as a vice-chair of the FBI's InfraGard Electromagnetic Special Interest Group (EMP-SIG). He has over 30 years of experience leading projects that assess and transform critical operations with focus on capability portfolio management and cascading consequence management. He has led teams for the FBI, Headquarters Army, and Headquarters Marine Corps to address enterprise-wide operations and systems improvement. His experience spans operations in austere locations, weapons of mass destruction neutralization, nuclear terrorism, cybersecurity, and infrastructure readiness and protection. His current passion is the establishment of vibrant, resilient, and self-sustaining communities.*

Significant contribution to this article was provided by:

William R. Harris *is an international lawyer specializing in arms control, nuclear nonproliferation, energy policy, and continuity of government. He is a member of the board, secretary, and a principal investigator involved in reliability standard development for critical infrastructures for the Foundation or Resilient Societies. He formerly served as a space operations lawyer for reconnaissance and communication systems of the United States government. He served as a senior (legal) advisor to the Commission on Electromagnetic Pulse (EMP) in January-December 2017. Since September 2017, he has been a vice chair of the EMP Special Interest Group of InfraGard, a nonprofit committed to protection of critical infrastructures. He holds a B.A. from Harvard College and a J.D. from Harvard Law School.*

Mary D. Lasky *is the chairman of the InfraGard Electromagnet Pulse Special Interest Group (EMP SIG). She is the lead editor and author of "Powering Through: From Fragile Infrastructure to Community Resilience" an action guide on being prepared if there is grid failure. She is a Certified Business Continuity Professional (CBCP). She has been the program manager for business continuity planning for the Johns Hopkins University Applied Physics Laboratory (JHU/APL). She is a past president of the Community Emergency Response Network Inc. (CERN) in Howard County, Maryland. She is a past president of the Central Maryland Chapter of the Association of Contingency Planners (ACP). At APL, she has held a variety of supervisory positions in Information Technology and in business services.*

Twitter users likely to spread falsehoods during disasters

Source: http://www.homelandsecuritynewswire.com/dr20180514-twitter-users-likely-to-spread-falsehoods-during-disasters

May 14 – We know that Twitter is littered with misinformation. But how good are the social media platform's most active users at detecting these falsehoods, especially during public emergencies?

Not good, according to new University at Buffalo research that examined more than 20,000 tweets during Hurricane Sandy and the Boston Marathon bombing.

Buffalo says that the study, published last week in the journal *Natural Hazards*, looked at four false rumors — two each from the marathon and hurricane, including an infamous falsehood about the New York Stock Exchange flooding.

Researchers examined three types of behavior. Twitter users could either spread the false news, seek to confirm it, or cast doubt upon it. Researchers found:

- 86 to 91 percent of the users spread false news, either by retweeting or "liking" the original post.
- 5 to 9 percent sought to confirm the false news, typically by retweeting and asking if the information was correct.
- 1 to 9 percent expressed doubt, often by saying the original tweet was not accurate.

"To the best of our knowledge, this is the first study to investigate how apt Twitter users are at debunking falsehoods during disasters. Unfortunately, the results paint a less than flattering picture," says the study's lead author Jun Zhuang, associate professor in the Department of Industrial and Systems Engineering in UB's School of Engineering and Applied Sciences.

Even after the false news had been debunked on Twitter and traditional news media outlets, the study found that:

- Less than 10 percent of the users who spread the false news deleted their erroneous retweet.
- Less than 20 percent of the same users clarified the false tweet with a new tweet.

"These findings are important because they show how easily people are deceived during times when they are most vulnerable and the role social media platforms play in these deceptions," says Zhuang, who is conducting similar research concerning Hurricane Harvey and Hurricane Irma.

On a more positive note, the study found that while Twitter users are likely to spread false news during disasters, Twitter and other media platforms move quickly to correct the misinformation.

Additionally, Zhuang says it's important to note that the study does not consider Twitter users who may have seen the original tweets with false news and decided to ignore them.

"It's possible that many people saw these tweets, decided they were inaccurate and chose not to engage," says Zhuang, who was recently awarded a $392,000 National Science

Foundation (NSF) grant to work on additional studies, including understanding what factors prompt Twitter users to ignore certain posts during emergencies, and the best ways to debunk false news.

— Read more in Bairong Wang and Jun Zhuang, "Rumor response, debunking response, and decision makings of misinformed Twitter users during disasters," Natural Hazards (11 May 2018).

Facebook says it took down 2 million terrorism posts in 2018

Source: https://www.upi.com/Facebook-says-it-took-down-2-million-terrorism-posts-in-2018/1271526406870/

May 15 – **Facebook said Tuesday it took down nearly 2 million posts related to terrorist propaganda this year before users reported them.**

The social media network took action against 1.9 million posts containing Islamic State, al-Qaida and related terrorism propaganda before users reported them in the first quarter of this year, Facebook said in a report.

Some 99.5 percent of the terrorism-related content was flagged by artificial intelligence technology.

CEO Mark Zuckerberg previously mentioned flagging of this content at his Senate hearing in April.

"Today, as we sit here, 99 percent of the ISIS and al-Qaida content that we take down on Facebook, our AI systems flag before any human sees it," Zuckerberg said at the hearing.

The number of terrorism-related posts are up 73 percent -- from 1.1 million terrorism-related posts last quarter, the Verge reported.

However, the enforcement component is also up with 99.5 percent of the posts flagged compared to 97 percent the previous quarter.

Increased enforcement was due to improvements in data technology including "using photo-matching" to match photos "previously marked as disturbing," the report said.

The report is the company's first publication of its enforcement numbers against violations of its community standards. These violations include graphic violence, adult nudity, terrorist propaganda, bullying, hate speech and fake accounts. The report covered the period from October to March.

Other findings in a release from Facebook showed that the company took down 21 million posts for adult nudity. It also took down or applied warning labels to 3.5 million posts of graphic violence, and removed 2.5 million hate speech posts, 837 million spam posts and 583 million fake accounts in the first quarter of this year.

An estimated 3 to 4 percent of Facebook accounts were fake accounts, the company said.

"We have a lot of work still to do to prevent abuse," Zuckerberg said. " It's partly that technology like artificial intelligence, while promising, is still years away from being effective for most bad content because context is so important."

Facebook says it has more than 2 billion users.


ICI
International
CBRNE
INSTITUTE
CBRNE-Terrorism Newsletter
W
O
M
D
EMERGENCY
RESPONSE

Washington well-prepared for major medical care emergencies

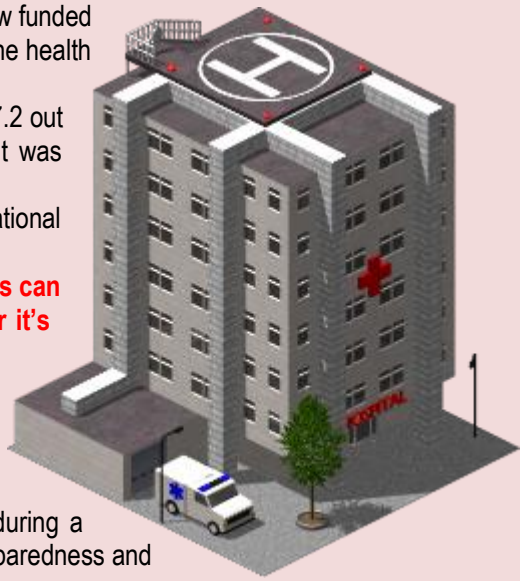
Source: http://www.heraldnet.com/northwest/washington-well-prepared-for-major-medical-care-emergencies/

Apr 24 – Washington is well-equipped to detect emerging diseases, deliver medical supplies, and coordinate a health response to an emergency, according to a federal index of state emergency preparedness released last week.

The index, created by the Centers for Disease Control and Prevention and now funded and managed by the Robert Wood Johnson Foundation, assesses how well the health system in each state could respond to a disaster.

For 2017, Washington was on par with the rest of the nation, with a score of 7.2 out of 10. The national average was 7.1, up from 6.4 in 2013, the first year it was measured.

Idaho scored a 6.7, improving from 6.4 in 2016, but still putting it below the national average.



Why measure health preparedness? The obvious reason is that disasters can send a lot of people to hospitals within a short period of time, whether it's hundreds of burn victims or dozens of people with gunshot wounds.

But even when that doesn't happen, disasters disrupt medical care and supplies by knocking out power or forcing evacuations. That prevents people from getting to pharmacies for needed medications or clinics for dialysis treatment.

Because of that, the most important thing for health care providers to do during a disaster is "stay in business," said Michael Loehr, the chief of emergency preparedness and response for the Washington Department of Health.

"The number one thing we want hospitals to do is treat patients," he said. The best way to prepare for that is by working across a broad group of providers and agencies, he said.

"If you try to go it alone, you're absolutely destined to fail," Loehr said.

The index was created as part of a federal effort to improve emergency response after Hurricane Katrina, said Anna Wood, a researcher at the University of Kentucky and the deputy director of the preparedness index. Before then, most federal planning for health emergencies was focused on responding to bioterrorism.

"The capabilities and the resources that had been invested in bioterrorism were not necessarily as transferable to a natural disaster as folks would like it to be," Hoover said.

Gaps in Israel's Civilian Preparedness in Emergency

Source: https://i-hls.com/archives/82645

Apr 22 – The IDF has been gradually reflecting the concept that Israel's next conflict will take place in two fronts: In the military front, the IDF forces will be operated in the defensive and mainly offensive spheres in order to achieve the swiftest victory. In the civilian front, the public will be called to produce a reasonable functioning sequence vis a vis the massive attacks on both population concentrations and critical infrastructure. The Home Front Command's national exercise "Steadfastness" was held between March 11-15, 2018 as part of the IDF commands exercise. In a recent Insight series publication by INSS, Meir Elran and Karmit Padan raise doubts concerning the preparedness of the civilian front in emergency, and reflect several gaps in both the State and IDF levels, that should be taken into account in order to improve the insufficient preparedness of the civilian population for the next high-intensity conflict scenario, considered realistic.

The exercise dealt with the multi-front conflict, but the emphasis was on the combined Syrian-Lebanese northern front, and the threat posed by Hizballah was presented as the major threat regarding the civilian front. The exercise was presented as directed to advance the cooperation among the Home Front Command, the emergency and rescue agencies and the police and to improve the public's readiness to war. However, the article claims that the extent of the information that the exercise directors chose to share with the population was, in fact, very poor.

In order to materialize the deterrence concept, Israel must present a reasonable functioning sequence, so the exercise allowed to examine the essence and quality of the dialogue between the civilian and military fronts and map the gaps existing in the Home Front Command. However, as result of the classified character of the event, the incorporation of civilians was very limited. The participation of civilian organizations such as government ministries, local authorities and social entities was also restricted. The article authors raise the question whether the information should have been classified in the first place. The same approach has been also reflected by the government and military directed and consistent policy to refrain from agitating the public regarding the evaluation of the extent of the developing threat. Will knowing the threats in advance enhance the public preparedness or rather it will act correctly even if surprised?

Another challenge reflected in the national home front exercise related to the cooperation and coordination among the systems of the State's organizations in an emergency. The recent exercise did not demonstrate the complete array of possibilities of cooperation between the IDF, through the Home Front Command, and the civilian systems, including the National Emergency Authority. According to INSS article, this reflects a severe systemic failure. With the lack of legislation and regularization agreed upon by the various state organizations, particularly the National Emergency Authority and the Home Front Command, there is no leading actor responsible for the Israeli civilian front. Under the current circumstances, the result might be non-coherent functioning and a severe blow to the civilian front preparedness, especially in an extreme emergency scenario.

From heat to terrorism to quakes, doctors prepare for all eventualities ahead of Tokyo 2020 Olympics

Source: https://www.japantimes.co.jp/news/2018/01/26/national/science-health/heat-terrorism-big-one-doctors-prepare-eventualities-ahead-tokyo-2020-olympics/#.WvKF4n--nIU

January 2018 – Japanese doctors are preparing for the widest-possible range of medical contingencies they may face during the 2020 Olympics and Paralympics in Tokyo, from the provision of general first aid to major responses to anticipated sweltering weather or a possible terrorrist attack.

Organizers estimate that some 7.8 million people will flock to Olympic venues during the games, and 2.3 million will be in and around Tokyo for the Paralympics.

With such huge numbers expected, the Japanese medical community has put together a consortium of groups to prepare responses to everything from simple medical procedures to full-scale disaster triage.

The consortium began its evaluation in spring 2016, assuming the worst possible outcomes while preparing for the most likely, with the Tokyo summer heat an ever present consideration in all scenarios.

The consortium is made up of the Tokyo Medical Association and other national medical societies that specialize in emergency medicine, trauma injuries, burns and poisoning.

The central government also launched a group to coordinate responses within the Ministry of Health, Labor and Welfare in 2017, headed by Hiroyuki Yokota, a Nippon Medical School professor.

On their agenda so far has been an examination of medical arrangements for past large-scale sports events held in major cities — including the London Olympics and Paralympics in 2012 — and an assessment of the patient and treatment capacities of facilities around venues slated to host events in 2020.

The group will also formulate manuals for general and specialist doctors to help them cope with a large number of patients in the event of accidents or attacks during the games, they said.

Naoto Morimura, a University of Tokyo professor who will be responsible for compiling the manuals, said the consortium's goal is "to not only recommend preparations for the games, but also to present a vision of emergency medical care for disasters in the capital thereafter."

"We hope to make this an opportunity to strengthen cooperation among relevant parties and make it conducive to future efforts," Morimura said, alluding to possible disasters in or around Tokyo, with a major earthquake directly beneath the metropolitan area topping the list of concerns.

In October the Japanese Association for Acute Medicine hosted a symposium during its general assembly in Osaka to share information about the most critical issues.

Many emergency physicians taking part in the symposium raised concerns about the difficulty of securing hospitals, doctors and volunteers to manage so-called code blues — emergency situations where a person goes into cardiac arrest — according to participants.

Noting that private doctors and medical practitioners are seemingly unfamiliar with issues affecting athletes and spectators at events like the Tokyo Marathon, an official from the Tokyo Medical Association introduced a plan to shore up and improve preparations.

After evaluating the medical response to incidents like the 2005 terror attack in London and the 2013 Boston Marathon bombing, one doctor advised the symposium about the importance of effective and efficient transport of victims and to ensure plans involve quickly transferring them to a number of hospitals — rather than overwhelming just one with a flood of serious cases.

Among issues raised by participating doctors was the shortage of emergency medical care centers and ambulances in Tokyo, as well as the possible neglect of medical treatment for regular residents when all focus turns to the games.

The consortium will encourage the Tokyo Olympic and Paralympic organizing committee to secure necessary personnel and funding, and to submit a final set of proposals in line with the results of its study.

With the games being held in the hottest and most humid period during Tokyo's summer, heatstroke and heat exhaustion are serious concerns for medical officials.

For example, between July 24 and Aug. 9, when the Olympics will be held, the average highs in Tokyo were 34.6 degrees in 2015, 31.6 in 2016 and 31.3 in 2017.

A government survey conducted in summer 2016 found temperatures may become unsafe for athletes and spectators at some venues.

Yasufumi Miyake, a member of a panel set up within the organizing committee to study measures that can be taken to combat the heat, said it is necessary to take precautions against heat-related illnesses.

"We plan to formulate responses by planning for the different people concerned, whether they are foreigners, the elderly, children, people with disabilities or games staff. (We will take into consideration) how many of them gather at each place and their movements, from stations and bus stops near Olympic venues to ticket checks, security checks and venue entrances," said Miyake, a Teikyo University emergency medicine professor.

Arrangements will be made to install sunshades and fans, and water will be readily available to people everywhere.

For road race events like the marathon and cycling, in which spectators will line the capital's streets, convenience stores and vending machines may be utilized in the battle against the heat, Miyake said.

"As many patients suffering from heat-related illness tend to have only mild symptoms, we hope to give them first-aid treatment on the spot as much as possible," he said.

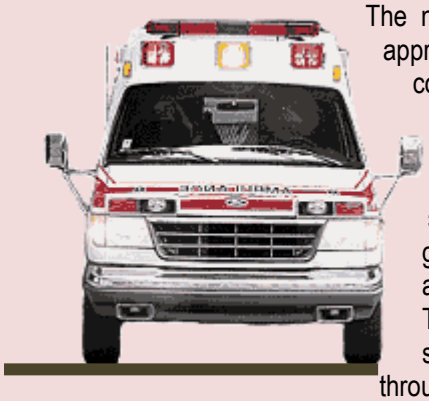
Miyake suggested that gymnastic halls and other buildings near event venues should be used as first-aid centers, to allow people to cool down and to provide them with necessary medical attention so they won't need to be transported to hospitals.

EDITOR'S COMMENT: Problem with "code blues"? In that case, it might sund stupid to ask for CBRN preparedness…

New Application Will Alert When Emergency Vehicle is Approaching

Source: https://i-hls.com/archives/82873

May 07 – A new service, Responder-to-Vehicle (R2V), protects first responders and motorists by delivering real-time alerts to drivers and connected cars via smartphone apps and in-vehicle systems when emergency vehicles are nearby and on-scene. HAAS Alert, a startup whose mission is to make roadways safer, is one of the first applications approved for use on FirstNet (US First Responder Network Authority).



The new alert service warns motorists and cars when emergency vehicles are approaching and on-scene. It reduces the potential for dangerous and costly collisions involving emergency vehicles and apparatuses. It sends real-time notifications to distracted drivers providing them ample time to yield.

After passing FirstNet's rigorous App Review Process, the solution can now be found in the App Catalog which is exclusively for public safety entities that subscribe to FirstNet services. It features apps for the first responder community, giving public safety a dedicated location to find meaningful new, solutions, according to the company announcement.

The company said their availability in the FirstNet App Catalog indicates their strong commitment to providing cellular-enabled safety alerts to drivers throughout the United States.

HAAS Alert service is already integrated with and delivers proactive safety notifications to Waze users. Integration with other popular navigation apps and in-car systems with major automotive brands is also on the way. Within the next couple of years, HAAS Alert will be sending real-time alerts to millions of drivers on a daily basis.

"Through our work with first responders, we heard their need for innovative applications to assist with their lifesaving mission. FirstNet is helping to address these needs, and we are pleased to welcome HAAS Alert's app to the FirstNet App Catalog," said Mark Golaszewski, Director of Technology and Innovation, First Responder Network Authority.

Electric-Car Era Threatens Firefighters With New Road Risks

Source: https://www.bloomberg.com/news/articles/2018-05-15/electric-car-era-threatens-firefighters-with-new-roadside-risks

May 15 – Firefighters doused the blazing Tesla Inc. Model X's battery pack, and then company engineers removed about one-quarter of its power cells before the vehicle was deemed safe to tow off of a California freeway.

That didn't prevent the powerful and highly flammable lithium-ion battery cells from reigniting. The car caught fire twice more within 24 hours of the March 23 fatal crash, and again six days later, according to a safety bulletin from the fire department in Mountain View.

Fires on electric vehicles are rare, but the volatile chemistry of their batteries and the need for special training on how to extinguish them raises new safety questions as automakers are poised to dramatically increase production. Techniques for putting out burning gasoline-fueled vehicles could make worse a blaze in a battery powered one.

"We're in uncharted waters here," said Donald Sadoway, a professor of materials chemistry at the Massachusetts Institute of Technology. "When you start putting 70 kilowatt-hour packs in a car, it's very different than what happens in a cellphone."

The growing popularity of lithium-based batteries that power everything from personal electronics to bicycles has periodically been marred by outbreaks of fires. Blazes in e-

cigarettes, laptops and even battery packs on one of the most sophisticated jetliners in the world, the Boeing Co. 787, have led to government restrictions and frightening headlines.
The U.S. National Transportation Safety Board has opened investigations into two recent Tesla fires, along with an earlier blaze last year. The agency charged with setting vehicle safety standards, the National Highway Traffic Safety Administration, on Thursday announced it was also gathering information on the most recent episode, on May 8 in Fort Lauderdale, Florida. Swiss police are also examining a fatal Tesla crash last week that triggered a fire.

Emergency personnel at the scene of a Tesla crash on U.S. Highway 101 in Mountain View, California on March 23. Source: KTVU via AP Photo

The issue isn't new. NHTSA also has conducted reviews of battery fires in the past, including a General Motors Co.'s Chevrolet Volt that caught fire in 2011, several weeks after the agency conducted crash tests on the vehicle. Other manufacturers whose cars have been involved in fires include the former Fisker Inc. and Mitsubishi Motors Corp.

Heat and Sparks

The components of lithium-ion rechargeable batteries make them inherently fire-prone.
Unlike gasoline, which needs a spark before it ignites, lithium cells contain their own ignition systems: large stores of energy that are transformed into heat and sparks when they short circuit. They also contain solvents that are powerful fuel for fires as well as oxidized metals that can feed oxygen to a blaze, complicating efforts to extinguish it.
"This is a perennial problem with lithium-ion batteries," said Prashant Kumta, a University of Pittsburgh engineering professor who has studied battery chemistry.
While the battery industry has made huge strides in ensuring cells can perform safely during normal operation and recharging, there is little that can be done once cells are torn apart in a violent collision, Kumta said. In a phenomenon known as thermal runaway, a short-circuiting battery produces ever more heat, which creates a chain reaction of fire and more heat production in adjacent cells, he said.
"It's basically like a fire cracker," he said. "You have one battery that catches fire, then the next one catches fire and pretty soon they're all on fire."

Comparing Risks

There were 174,000 fires on all motor vehicles in the U.S. in 2015, killing 445 people, according to the most-recent data from National Fire Protection Association.
The attention paid to the relative handful of Tesla fires compared to the thousands of other automobile fires has rankled the carmaker. The risk of a gasoline-powered car catching fire was more than four times higher than a Tesla Model S, company Chairman Elon Musk said in a 2013 blog post.
"You are more likely to be struck by lightning in your lifetime than experience even a non-injurious fire in a Tesla," Musk said. The company didn't respond to a request for comment on the recent episodes.
In a 2011 press release, prompted by the Chevrolet Volt fire, the NHTSA said it did not believe electric cars were more susceptible to blazes than other cars.
After that fire, NHTSA conducted a series of tests on Volt battery packs. Out of six simulations of various types of accidents, two of the batteries caught fire, according to the agency's report. A search of crash records at the time found no evidence of other fires.

However, there is little government data on the occurrence of electric-vehicle fires, making it difficult to document the extent of the problem, said Jason Levine, executive director of the advocacy group Center for Auto Safety.

"One of several troubling things about these fires is a real lack of usable, quantifiable data that would help everyone involved," Levine said.

Not only is it difficult to compare electric vehicles to gas-powered ones, it's also impossible to compare the likelihood and severity of fires on Teslas with those on other lithium-battery-powered cars such as the Chevrolet Bolt, Nissan Motor Co. Ltd.'s Leaf and BMW's i3, Levine said.

One fact that is not in dispute is the intensity of fires that occur in large lithium-ion battery packs.

Like Fireworks

Firefighters in Indianapolis who responded on Nov. 3, 2016, to a crash of a Model S that hit a tree and a building at high speed encountered what looked like a fireworks display as battery cells exploded and shot into the air, according to video shot by a news crew. The crash killed both people in the car.

In the Fort Lauderdale Tesla crash, two teenagers died and a third was injured when the car struck a concrete wall and burst into flames, according to police. Video of the scene shows fire engulfing the Model S (photo below).

"NTSB has a long history of investigating emerging transportation technologies, such as lithium-ion battery fires in commercial aviation," NTSB Chairman Robert Sumwalt said in a statement announcing the agency was opening an investigation.

When the Model X in Mountain View slammed into the side of a concrete highway barrier, the front of the car was sheared off, damaging the battery pack located under the floor. About half of the car was on fire when crews arrived, said Chief Juan Diaz. It took about two minutes to extinguish the blaze, he added.

The driver, Walter Huang, was killed.

Mountain View is located in Silicon Valley, where electric vehicles are common and firefighters trained for battery fires at Tesla's nearby factory in Fremont in 2014, the chief said. Still, the case illustrates how fire departments may need more training on the unique issues created by battery fires.

The fire crews used water mixed with chemicals that create a foam designed to snuff out gasoline fires, according to Diaz and photos of the scene.

However, foam isn't recommended by the National Fire Protection Association for batteries. NFPA guidelines call for using copious amounts of plain water on battery fires, as much as thousands of gallons. The water helps cool the battery, which is key to halting a fire.

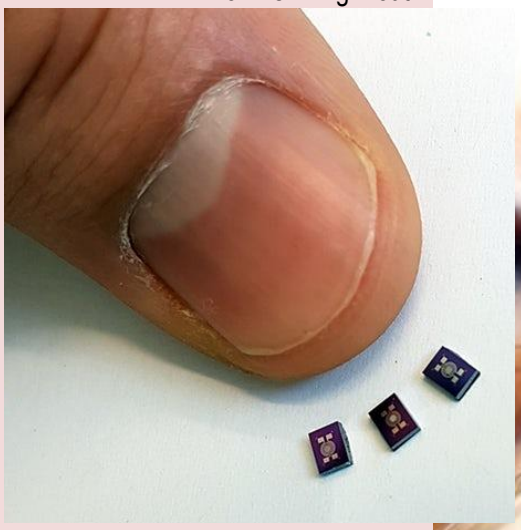
Concerned that the battery was continuing to generate heat and worried about the risk of electrical shock, the firefighters called in Tesla engineers -- which may not be possible if accidents aren't located as close to the company's factory. They removed about 25 percent of the battery's cells, Diaz said.

Fire crews accompanied the tow truck that brought the car to a salvage yard because the battery continued to pop and hiss as gas vented from the power pack, Diaz said. It didn't reignite on the trip, but it caught fire again two more times within the next 24 hours and again six days later, Diaz said.
A crew had to drain the remnants of the battery of any electrical charge before it became safe, he said.
Scientists are working on promising lithium-ion battery formulations that will reduce the chances of fire and there may be ways to make battery cases more impact resistant, said John Warner, a consultant who is president of the National Alliance for Advanced Technology Batteries International, a trade group.
But until then, there needs to be more education for firefighters and other emergency workers, Warner said.
"It is a relatively new technology from what the firefighters have dealt with in the past," he said. "I think there's been some very good work done. Has it reached every fire department in the United States? I'm not sure it has."

Scientists develop the smallest, cheapest electronic nose for search and rescue

Source: https://newatlas.com/electronic-rescue-nose/54653/

May 17 – Scientists from ETH Zurich have developed what they claim is the "smallest and cheapest" electronic nose for sniffing out



people, designed with earthquake and avalanche rescue in mind. The nose is an array of sensors to detect various substances which, when found together, would provide the crucial "chemical fingerprint" showing the presence of human life.
The array builds on the team's previous work on building sensors to detect acetone, ammonia and isoprene which are all by-products of human metabolism and which leave our bodies either as we breath, or through our skin. Separate research has shown that these chemicals can accumulate quickly where a human is trapped.
The new "nose" combines these sensors with commercially-available ones which detect carbon dioxide and moisture, which could also indicate the presence of a person. It could be fitted to a handheld device, or to a robot or drone for reaching inaccessible locations. The team's own sensors are made from metal-oxide films with a high surface area, which makes them sensitive to trace concentrations of the target chemicals.
"The combination of sensors for various chemical compounds is important, because the individual substances could come from sources other than humans," lead author Andreas Güntner explains in a press release. "CO2, for example, could come from either a buried person or a fire source."

Though the team's sensors are the fraction of the size of your fingernail, they're shown to be as sensitive as suitcase-sized spectrometers which are much more expensive.

"Our easy-to-handle sensor combination is by far the smallest and cheapest device that is sufficiently sensitive to detect entrapped people," lead researcher Sotiris Pratsinis says in the same release. "In a next step, we would like to test it during real conditions, to see whether it is suited for use in searches after earthquakes or avalanches."

The team tested its array on people enclosed in a plethysmographic chamber, which is usually used to detect changes in volume in the body, or an organ. The scientists would next like to test it in a real-world simulation of earthquake conditions.

Though trained dogs are great at finding people trapped in snow or rubble, they come with certain disadvantages. They're not always located near to disaster areas, so travelling to where they're needed uses precious time, then once on the scene they need to take breaks from time to time. These disadvantages could be overcome with their device, the scientists say. The chances of survival drop enormously in the first hours after an earthquake strikes.

Though electronics are used in earthquake searches, they tend to be microphones and cameras rather than sensors. The researchers' device could prove more adaptable – locating those who are unconscious as well as those able to make noise. The research points out that 780,000 people have died due to earthquakes over the last 10 years. The team suggests the device could also be used to expose human trafficking.

The nose joins similar technology developed to detect nerve gas, Chron's disease, explosives and narcotics, and prostate cancer.

The team's research was published in the journal *Analytical Chemistry*, and can be read online.

Sniffing Entrapped Humans with Sensor Arrays

By Andreas T. Güntner† , Nicolay J. Pineau†, Paweł Mochalski‡, Helmut Wiesenhofer‡, Agapios Agapiou§, Christopher A. Mayhew‡, and Sotiris E. Pratsinis*†

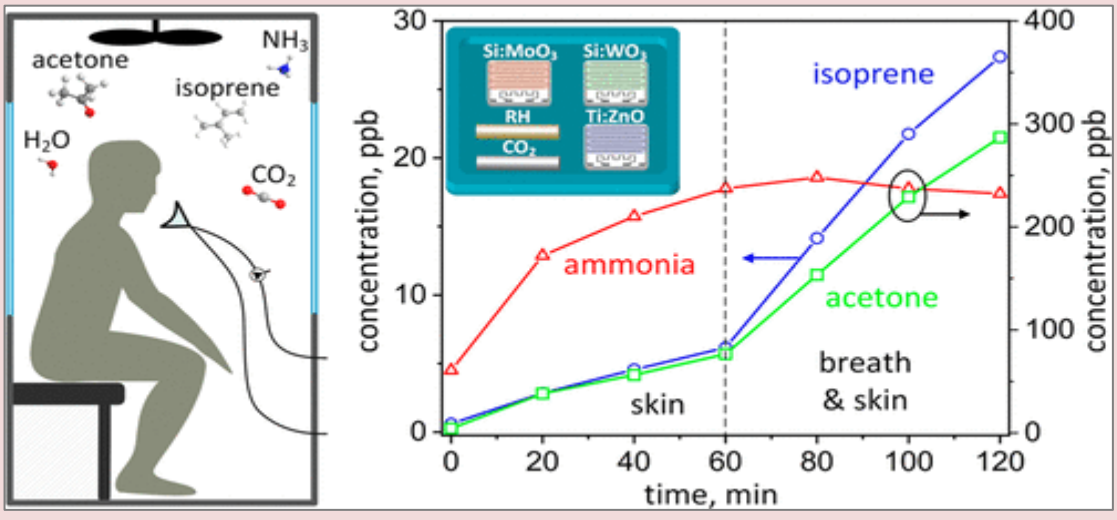
† Particle Technology Laboratory, ETH Zurich, Zurich CH-8092, Switzerland

‡ Institute for Breath Research of the University of Innsbruck, Dornbirn AT-6850, Austria

§ Department of Chemistry, University of Cyprus, P.O. Box 20537, Nicosia CY-1678, Cyprus

Anal. Chem., 2018, 90 (8), pp 4940–4945; **DOI:** 10.1021/acs.analchem.8b00237

Source: https://pubs.acs.org/doi/10.1021/acs.analchem.8b00237



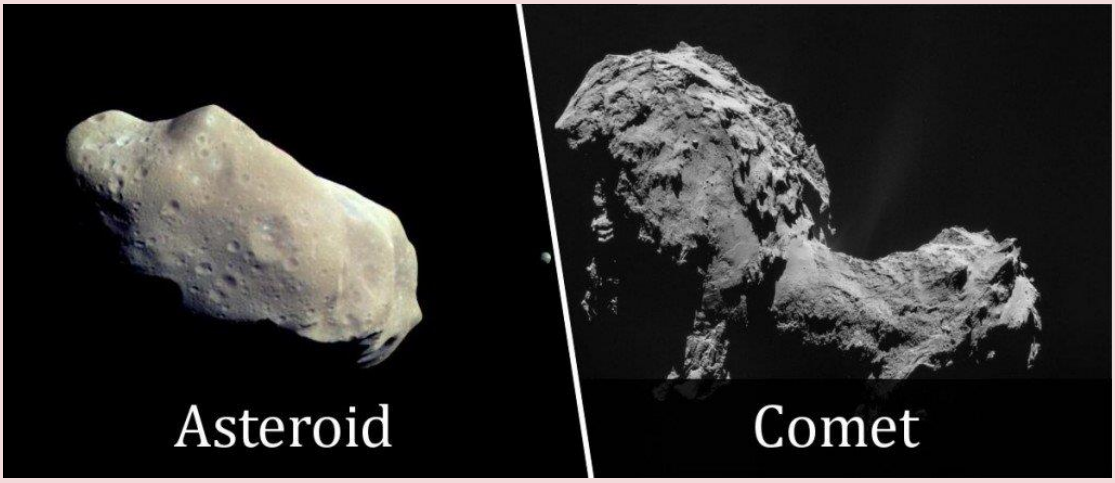
Earthquakes are lethal natural disasters frequently burying people alive under collapsed buildings. Tracking entrapped humans from their unique volatile chemical signature with hand-held devices would accelerate urban search and rescue (USaR) efforts. Here, a pilot study is presented with compact and orthogonal sensor arrays to detect the breath- and skin-emitted metabolic tracers acetone, ammonia, isoprene, CO_2, and relative humidity (RH), all together serving as sign of life. It consists of three nanostructured metal-oxide sensors (Si-doped WO_3, Si-doped MoO_3, and Ti-doped ZnO), each specifically tailored at the nanoscale for highly sensitive and selective

tracer detection along with commercial CO_2 and humidity sensors. When tested on humans enclosed in plethysmography chambers to simulate entrapment, this sensor array rapidly detected sub-ppm acetone, ammonia, and isoprene concentrations with high accuracies (19, 21, and 3 ppb, respectively) and precision, unprecedented by portable sensors but required for USaR. These results were in good agreement (Pearson's correlation coefficients ≥0.9) with benchtop selective reagent ionization time-of-flight mass spectrometry (SRI-TOF-MS). As a result, an inexpensive sensor array is presented that can be integrated readily into hand-held or even drone-carried detectors for first responders to rapidly screen affected terrain.


IOI
International
CBRNE
INSTITUTE
CBRNE-Terrorism Newsletter
W
O
M
D
ASYMMETRIC
THREATS

The threat of asteroids and comets

Source: http://www.homelandsecuritynewswire.com/dr20180516-the-threat-of-asteroids-and-comets



May 16 – In 1994, astronomers watched in awe as the comet Shoemaker-Levy 9 crashed into the planet Jupiter, creating massive fireballs exploding with the force of six million megatons of TNT—equivalent to 600 times the world's nuclear arsenal.

What would have happened if it had hit Earth instead of Jupiter?

"It would be the biggest destruction that mankind has ever seen," said Mel Stauffer, University of Saskatchewan geological sciences professor emeritus. "It wouldn't matter where it hit, it would affect all mankind."

The subject of Hollywood movies, the reality of asteroid and comet strikes is more science, than science fiction. Most researchers believe the likelihood of a massive object colliding with Earth in our lifetime is small, but the planet has been hit before and will certainly be hit again.

USask says that Stauffer has spent a lifetime collecting the evidence, searching for meteorites, shatter cones (rock violently fractured around the rim of impact craters) and tektites (pulverized rock liquified by the superheated temperature of an impact and blasted into the atmosphere before raining down to the surface).

Stauffer said on average the Earth gets hits by a one-metre-wide asteroid about once a year, although, most burn up in the atmosphere or crash into remote regions or our vast oceans. Two of the most alarming recent events occurred in the Siberian region of Russia, including the 2013 asteroid air burst near Chelyabinsk that was reported in the journal Nature to be a house-sized object 20 metres in diameter, releasing the energy equivalent of 440,000 tonnes of TNT.

"It went just past a couple of villages, including Chelyabinsk, and because it was breaking the sound barrier and exploding into pieces, the shock wave broke windows that blew up in people's faces, so about 1,500 people were hospitalized from cuts," said Stauffer. "It was the second largest event that we have been able to accurately measure."

In 1908, what is believed to have been an asteroid exploded over a sparsely populated area of Siberia, flattening 80 million trees over 2,000 square kilometres of forest in what is called the Tunguska event. More than 1,000 research papers have been filed on that blast, with supercomputer simulations projecting the object to have been 60 to 190 metres wide and to have exploded with a force of up to 15 megatons of TNT (1,000 times more powerful than the atomic bomb dropped on Hiroshima in 1945).

Chelyabinsk and Tunguska are the most recent examples of what can happen when an asteroid or comet enters a collision course with the planet. The Earth Impact Database documents 168 asteroid craters of at least one kilometre in diameter, a list that includes the 130km Sudbury impact—the third largest in the world—1.8 billion years ago, and the 150km Chicxulub crater in Mexico's Yucatan Peninsula created 65 million years ago that has been linked to the extinction of the dinosaurs.

The database includes six impact craters in Saskatchewan two kilometres or larger—Viewfield, Gow Lake, Maple Creek, Elbow,

Deep Bay and Carswell (the biggest at 39km wide)—dating between 75 million and 395 million years ago, as well as the 25km Victoria Island crater in the Arctic that U of S geological sciences professor Brian Pratt helped discover in 2012 while exploring the area for Natural Resources Canada.

"It was exciting," said Pratt, who co-authored a paper on the find in the research journal Meteoritics and Planetary Science. "We were flying in a helicopter and we could see the rocks looked strange. So, we landed and walked about 30 yards to the first outcrop of tilted rocks and right away we saw shatter cones. We both looked at each other and said, 'This is a meteorite impact!' That's what creates shatter cones, so we knew exactly what we were dealing with."

Pratt estimates that impact occurred between 130 million and 450 million years ago and likely had wide-ranging effects.

"It could have been a shallow sea when it hit, or it could have hit land, we just don't know for sure," he said. "If it hit land, there would have been an awful lot of debris in the atmosphere that would have affected climate, probably creating a cooling period."

While major asteroid strikes are rare in terms of Earth's 4.5-billion-year geological history, even another Tunguska-sized impact would have a devastating effect on a populated area. In the 1990s, Stauffer was a member of the national Meteorite and Impacts Advisory Committee which called on the Canadian Space Agency and the National Aeronautics and Space Administration (NASA) in the United States to identify near-Earth objects (NEOs) and track potential threats to the planet.

"They didn't do anything right away, but a few amateur astronomers did and NASA finally took heed and started their program, which I guess I can claim a tiny, tiny bit of credit that our group put the bug in their ear," Stauffer said.

To date, NASA has documented 18,043 NEOs in our solar system, including 1,900 that are at least 140 metres in diameter and have orbits near enough to Earth to be classified as potentially hazardous asteroids. But thousands remain undetected. On April 18 an asteroid labelled 2018GE3, estimated at up to 100 metres in diameter, escaped detection by NASA until just a few days before passing halfway between the Earth and moon (192,000km) at a speed of 106,000km per hour.

"There are lots of asteroids and comets in our solar system and it's impossible to predict the trajectories of all of these objects, but we need to try," said Daryl Janzen, a U of S sessional lecturer in physics who discusses NEOs in his Astronomy 104 class.

Identifying threats is the first step, with the United Nations recently endorsing establishment of the International Asteroid Warning Network for world-wide collaboration to defend Earth from potential impacts. While NASA's official position is that no known asteroid is projected to collide with the planet this century, NASA is preparing for a 2021 space mission designed to demonstrate a kinetic-impact technique to nudge an object off of a collision course with Earth.

"There is an extremely low probability of the planet coming into contact with one of these large near-Earth objects in our lifetime, but there is really good evidence that it happened in the past and led to mass extinction on the planet," said Janzen. "So, although the probability is low, it's important to discover as many NEOs as we can, so that if one does enter into a collision course with Earth, we can try to do something about it."


ICI
International
CBRNE
INSTITUTE
CBRNE-Terrorism Newsletter
W
O
M
D
BUSINESS
CONTINUITY
OPEN FOR
BUSINESS
AS USUAL
Business Interruption
Disaster Event

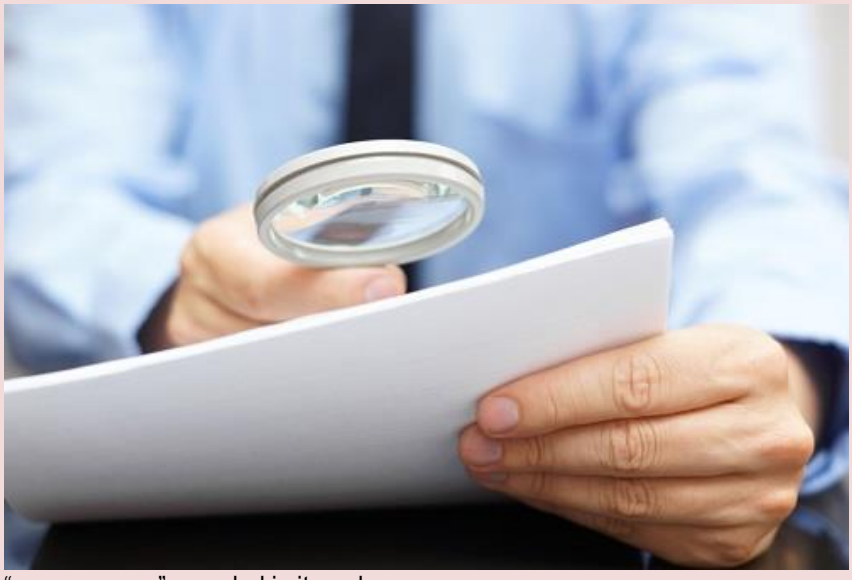
Pool Re reveals latest report, looks at Salisbury nerve attack

By Lucy Hook

Source: https://www.insurancebusinessmag.com/uk/news/kidnap-ransom-terrorism/pool-re-reveals-latest-report-looks-at-salisbury-nerve-attack-99194.aspx

Apr 30 – Pool Re has today published its latest Terrorism Frequency Report, which looks at terrorism trends and reinsurance in advanced markets spanning the 25 years since its foundation – including recent attacks such as in Salisbury.

The report, which coincides with the government-backed reinsurance pool's quarter-century anniversary, provides "an insight into the shifting nature of the terrorist threat," looking at the frequency of attacks, the changes in methodology, and the financial impact of the property damage caused.



It also reviews recent terrorist attacks across the globe, including an assessment of the attack against Sergei and Yulia Skripal in Salisbury, and the "coverage gap" revealed in its wake.

The IRA's mainland bombing campaign and the events that led to Pool Re's foundation are discussed in an article written by Andrew Silke, the newly-appointed Pool Re and Cranfield University professor of terrorism, risk management and resilience, and the implications for the insurance market and counter-terrorism police as a result of the intensified threat posed by modern extreme right-wing terrorism are reviewed in the report.

Pool Re's chief executive Julian Enoizi said that the scheme and threat which Pool Re was established to mitigate has "changed markedly" in the 25 years since its creation.

"We have sought to continuously evolve our proposition and to learn from our experience of terrorism risk in an effort to develop analytical and actuarial tools," he said.

"By assessing the libraries of data available, in collaboration with our academic partners, from a (re)insurance standpoint and then distilling this information we aim to provide a resource which will enable the market to retain ever more of this risk. The analyses in this report are a significant step towards that goal."

Enoizi said that events which point towards an emerging risk must also be analysed, pointing to the Salisbury attack.

"The losses being suffered by businesses in Salisbury are highly unusual. CBRN has historically been excluded from all commercial property and business interruption insurance policies as it was thought that the sheer magnitude of the potential losses would exceed the ability of insurance and reinsurance companies to meet claims. However, the disturbing event in Salisbury shows that these types of attack can be localised and could be deployed by criminal or terrorist actors," the CEO said.

"They have highlighted the macro consequences of a micro CBRN event. This should prompt debate within our industry. Consideration should be given to whether the perceived wisdom around certain perils needs to be reassessed and whether now is the time to address other risks, for which underwriters also do not provide cover."

Nerve agent attack raises business interruption concerns

By Matthew Lerner

Source:http://www.businessinsurance.com/article/20180430/NEWS06/912320935/Salisbury-UK-Nerve-agent-attack-raises-business-interruption-concerns-Pool-Reins

Apr 30 – The nerve agent attack in Salisbury, U.K., purportedly perpetrated by the Russian government as revenge on a former spy, according to reports, raises some interesting points about insurance coverage and exclusions, according to a report from Pool Reinsurance Co. Ltd. Monday.

Although the attack was "the first offensive use of a nerve agent in Europe since the Second World War," the resulting loss of foot traffic and commercial activity in the areas surrounding the attack's location may shine light on coverage gaps, Pool Re says in its latest Terrorism Frequency Report issued Monday.

"There are certain eventualities that are invariably excluded by all commercial insurance policies, two examples of which are war and the use of CBRN [chemical, biological, radiological, nuclear]," said an analysis by Stephen Coates, chief underwriting officer, and Camilla Scrimgeour, analyst.

Local attractions and business have seen traffic fall off drastically or been closed altogether.

Salisbury Cathedral, the report said, saw foot traffic drop by 40% in the week immediately after the incident and a month after the attack, the visitor rate was still down 20% and income was down 24%.

Two restaurants where the Russian agent dined with his daughter, who was also exposed to the nerve agent, remained closed as of the writing of the report, the analysis said.

The unprecedented nature of the interruption to business in Salisbury raises some interesting issues for business interruption (BI) insurance policies," the analysis said, adding "Traditional commercial property and business interruption policies do not offer such cover."

Limited coverage for such CBRN events is available in the stand-alone terrorism market, the report said. "CBRN coverage is available within terrorism policies backed by Pool Re, and on a more limited basis in some other terrorism covers."

The incident shines a light on a scenario always considered low probability that may warrant new attention.

"Since it seems possible that techniques, thought formerly to be restricted to nation states and deployed during a conflict, may be used by others in a more restricted and localized manner, it may be useful for insurers and reinsurers to consider if their historical perspectives on certain scenarios should be re-examined," the report said.

Salisbury attack exposes business interruption protection gap, reports Pool Re

By Matt Sheehan

Source: https://www.reinsurancene.ws/salisbury-attack-exposes-business-interruption-protection-gap-reports-pool-re/

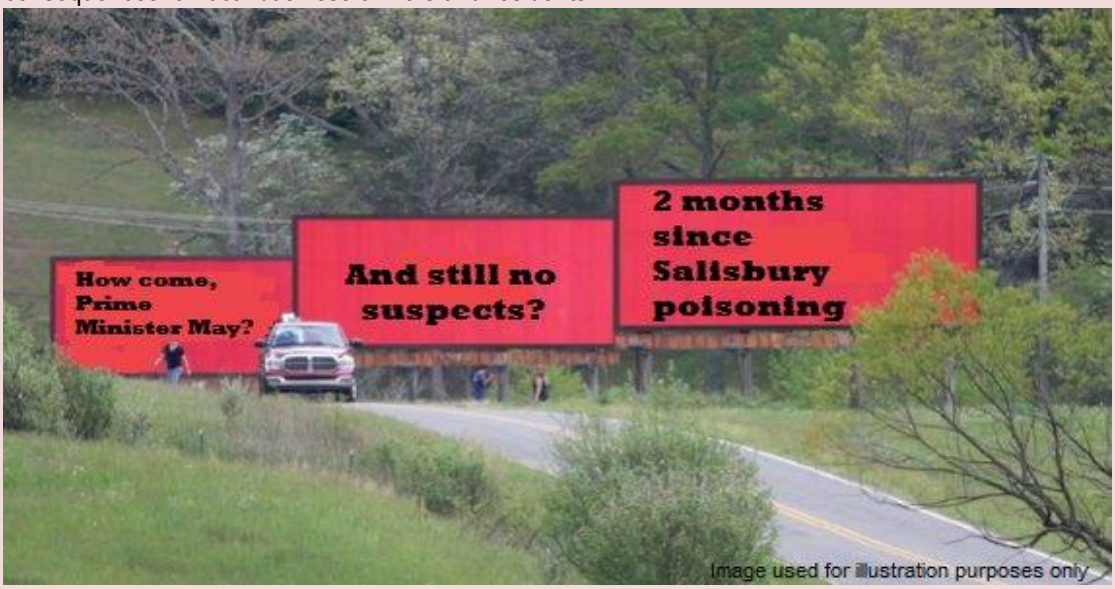
May 03 – **Pool Re, the UK's government-backed terrorism reinsurer, has reported that the losses suffered by Salisbury businesses in the wake of the nerve agent attack against Sergei and Yulia Skripal have exposed an oversight in the way re/insurers cover terrorism risks.**

The company's latest Terrorism Frequency Report, which coincided with the 25th anniversary of the Pool Re's foundation, noted that affected business owners are unlikely to be able to claim these business interruption (BI) losses on their existing insurance policies.

BI policies have traditionally been triggered by damage events like fire or storm, but have in many cases now been extended to cover other causes of interruption like closure of an area due to a crime scene or infectious disease.

However, BI policies have deliberately excluded risks related to war and the use of Chemical, Biological, Radiological, Nuclear (CBRN) due to the sheer magnitude of potential losses, which would be more appropriately funded by other means, such as Government.

The Salisbury incident, whilst unlikely to be declared a terrorist attack itself, shows that CBRN attacks can be localised and deployed by criminal or terrorist actors, and can have far-reaching financial consequences for local business owners and residents.



Julian Enoizi, Chief Executive Officer (CEO) of Pool Re, said: "The losses being suffered by businesses in Salisbury are highly unusual. They have highlighted the macro consequences of a micro CBRN event. This should prompt debate within our industry.

"Consideration should be given to whether the perceived wisdom around certain perils needs to be reassessed and whether now is the time to address other risks, for which underwriters also do not provide cover."

Although CBRN coverage is available within terrorism policies backed by Pool Re, traditional commercial property and business interruption policies do not offer such cover.

Pool Re's report, which assessed terrorism trends in advanced markets from 1990 to 2016 through the lens of reinsurance, also found that the nature of terrorist attacks have changed more generally.

It observed that, during the 1990s, when the IRA represented the most notable threat to UK terrorism reinsurers, attacks were designed to maximise financial and economic losses, whereas modern attacks focus on maximising loss of life.
Thus, while the annual average number of terrorist attacks in the 2010s is 63% lower than in the 1990s, the yearly average deaths are 30% higher.
Similarly, the proportion of attacks using improvised explosive devices (IEDs) was found to have fallen by 20%, while deaths from firearms rose 18%, and vehicles now account for 18% of terror-related fatalities.
The study also considered the growth of domestic, extreme right-wing (XRT) terrorist attacks, and their implications for the re/insurance market and counter-terror police.
Enoizi added: "We have sought to continuously evolve our proposition and to learn from our experience of terrorism risk in an effort to develop analytical and actuarial tools.
"By assessing the libraries of data available, in collaboration with our academic partners, from a (re)insurance standpoint and then distilling this information we aim to provide a resource which will enable the market to retain ever more of this risk."

Salisbury potential

Source: http://www.professionalsecurity.co.uk/news/case-studies/salisbury-potential/

May 16 – A 'micro CBRN event' as recently in Salisbury brings potential for extensive financial losses, due to business interruption, says the underwriting body Pool Re in its latest 'terrorism report'. Pool Re noted that the March 4 poisoning of Sergei and Yulia Skripal is unlikely to be certified as a terrorist attack by the UK Government.
Ed Butler CBE DSO, Head of Risk Analysis at Pool Re, said: "Despite it not being a terrorist incident, Pool Re has closely monitored this incident as it has highlighted a number of CBRN [chemical, biological, radiological and nuclear] post-incident and insurance lessons learned that we will feed into our CBRN modelling work. The use of even a very small amount of nerve agent and its resultant contamination can have a macro impact on businesses and the local economy." He recalled as a young Army officer in the Cold War, training for nerve agents being used as 'area denial weapons' against NATO military. "The threat we faced on the inner German border was as much about perception as actual capability and, as has been clearly seen in Salisbury, the psychological impact that nerve agents can have on local populations is far greater than the reality. It might be some time before Salisbury is deemed to be fully open for business and the strategic question of 'how clean is clean enough' is answered. Pool Re will analyse the economic losses, and its CBRN modelling."
The authorities in Wiltshire are promoting 'business as usual' in the cathedral city.
Pool Re summed up that not all CBRN losses are the same, and the Salisbury incident may provoke a wider debate around whether some elements are capable of coverage within traditional insurance policies. The UK Government has declared that the Novichok agent used in the Salisbury attack was of a type made in Russia.
Andrew Silke, the new Pool Re/Cranfield University Professor of Terrorism, Risk Management and Resilience, has written a guest article on the IRA's mainland bombing campaign and the forming of Pool Re, 25 years ago.

For the full 14-page report, visit https://www.poolre.co.uk/wp-content/uploads/2018/04/Terrorism-Frequency-Report-April-2018.pdf.

About Pool Re

Pool Re is the UK's terrorism reinsurance pool, providing underwriting over £2 trillion of exposure to terrorism risk in commercial property across the UK mainland.