Dedicated to Global First Responders

CBRNE NEWSLETTER TERRORISM

July 2017

www.cbne-terrorism-newsletter.com


ICI
International
CBRNE
INSTITUTE
CBRNE-Terrorism Newsletter
W
O
M
D
DIRTY R-NEWS

First Strike Final Hour Review – Not The Best Strategy

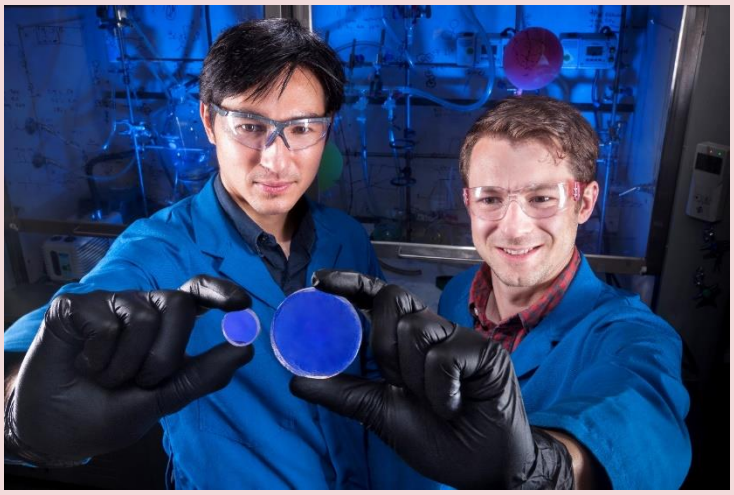
Source (video): http://wccftech.com/review/first-strike-final-hour/

Scintillating discovery at Sandia Labs

Source: http://www.homelandsecuritynewswire.com/dr20170630-scintillating-discovery-at-sandia-labs

June 30 – Taking inspiration from an unusual source, a Sandia National Laboratories team has dramatically improved the science of scintillators — objects that detect nuclear threats. According to the team, using organic glass scintillators could soon make it even harder to smuggle nuclear materials through America's ports and borders.

The Sandia Labs team developed a scintillator made of an organic glass which is more effective than the best-known nuclear threat detection material while being much easier and cheaper to produce. Organic glass is a carbon-based material that can be melted and does not become cloudy or crystallize upon cooling. Successful results of the Defense Nuclear Nonproliferation project team's tests on organic glass scintillators are described in a paper published this week in *The Journal of the American Chemical Society*.



Sandia National Laboratories researcher Patrick Feng, left, holds a trans-stilbene scintillator and Joey Carlson holds a scintillator made of organic glass. The trans-stilbene is an order of magnitude more expensive and takes longer to produce. (Photo by Randy Wong)

Sandia Labs material scientist and principal investigator Patrick Feng started developing alternative classes of organic scintillators in 2010. Feng explained he and his team set out to "strengthen national security by improving the cost-to-performance ratio of radiation detectors at the front lines of all material moving into the country." To improve that ratio, the team needed to bridge the gap between the best, brightest, most sensitive scintillator material and the lower costs of less sensitive materials.

Inspiration from light-emitting diodes lead to performance boost

Sandia Lab says that the team designed, synthesized and assessed new scintillator molecules for this project with the goal of understanding the relationship between the molecular structures and the resulting radiation detection properties. They made progress finding scintillators able to indicate the difference between nuclear materials that could be potential threats and normal, non-threatening

sources of radiation, like those used for medical treatments or the radiation naturally present in our atmosphere.

The team first reported on the benefits of using organic glass as a scintillator material in June 2016. Organic chemist Joey Carlson said further breakthroughs really became possible when he realized scintillators behave a lot like light-emitting diodes.

With LEDs, a known source and amount of electrical energy is applied to a device to produce a desired amount of light. In contrast, scintillators produce light in response to the presence of an unknown radiation source material. Depending on the amount of light produced and the speed with which the light appears, the source can be identified.

Despite these differences in the ways that they operate, both LEDs and scintillators harness electrical energy to produce light. Fluorene is a light-emitting molecule used in some types of LEDs. The team found it was possible to achieve the most desirable qualities — stability, transparency and brightness — by incorporating fluorene into their scintillator compounds.

Pushing past crystals and plastics

The gold standard scintillator material for the past 40 years has been the crystalline form of a molecule called trans-stilbene, despite intense research to develop a replacement. Trans-stilbene is highly effective at differentiating between two types of radiation: gamma rays, which are ubiquitous in the environment, and neutrons, which emanate almost exclusively from controlled threat materials such as plutonium or uranium. Trans-stilbene is very sensitive to these materials, producing a bright light in response to their presence. But it takes a lot of energy and several months to produce a trans-stilbene crystal only a few inches long. The crystals are incredibly expensive, around $1,000 per cubic inch, and they're fragile, so they aren't commonly used in the field.

Instead, the most commonly used scintillators at borders and ports of entry are plastics. They're comparatively inexpensive at less than a dollar per cubic inch, and they can be molded into very large shapes, which is essential for scintillator sensitivity. As Feng explained, "The bigger your detector, the more sensitive it's going to be, because there's a higher chance that radiation will hit it."

Despite these positives, plastics aren't able to efficiently differentiate between types of radiation — a separate helium tube is required for that. The type of helium used in these tubes is rare, non-renewable and significantly adds to the cost and complexity of a plastic scintillator system. And plastics aren't particularly bright, at only two-thirds the intensity of trans-stilbene, which means they do not do well detecting weak sources of radiation.

For these reasons, Sandia Labs' team began experimenting with organic glasses, which are able to discriminate between types of radiation. In fact, Feng's team found the glass scintillators surpass even t he trans-stilbene in radiation detection tests — they are brighter and better at discriminating between types of radiation.

Another challenge: The initial glass compounds the team made weren't stable. If the glasses got too hot for too long, they would crystallize, which affected their performance. Feng's team found that blending compounds containing fluorene to the organic glass molecules made them indefinitely stable. The stable glasses could then also be melted and cast into large blocks, which is an easier and less expensive process than making plastics or trans-stilbene.

From the lab to the ports

The work thus far shows indefinite stability in a laboratory, meaning the material does not degrade over time. Now, the next step toward commercialization is casting a very large prototype organic glass scintillator for field testing. Feng and his team want to show that organic glass scintillators can withstand the humidity and other environmental conditions found at ports.

Sandia notes that the National Nuclear Security Administration has funded the project for an additional two years. This gives the team time to see if they can use organic glass scintillators to meet additional national security needs.

Going forward, Feng and his team also plan to experiment with the organic glass until it can distinguish between sources of gamma rays that are non-threatening and those that can be used to make dirty bombs.

Russia offers expertise that will take Emirati nuclear engineers to top of their game

Source: https://www.thenational.ae/uae/na28-nuclear-ld-az-1.1208

3 November 2015 -- Abu Dhabi, UAE: Flag day at the Barakah plant. The Emirates Nuclear Energy Corporation (ENEC) today raised the UAE flag at Unit 1 of Barakah NPP. Courtesy ENEC

July 01 – Emirati nuclear engineering students could soon undergo training at Russian Training and education is important for countries looking to develop their own nuclear power, according to Valery Karezin, head of human resources at Rosatom, Russia's atomic energy body.

"Training is key. If the country is a newcomer the most important challenge is the creation of its own programme for personnel training," said Mr Karezin.

The UAE has collaborated with several countries to gain experience from their nuclear programmes.

In October last year the Emirates Nuclear Energy Corporation and Korea Electric Power Corporation signed a joint venture agreement which Mohammed Al Hammadi, Enec's chief executive, said would bring the country's 40 years of experience to the UAE.

A few months earlier Japanese professors were flown into the country to hold workshops for Emirati students and share lessons learnt from the Fukushima disaster in 2011.

Speaking at the atomic energy forum AtomExpo in Moscow, Mr Karezin said there are plans for Russia to work with the UAE in nuclear education.

"Until recently we did not have any close cooperation but there will be," he said.

"Russian and Emirati universities will work in the exchange of students. We are open for universities as part of a programme to help boost the UAE's nuclear power sector.

discussions and we're waiting for a decision from our universities to start this."

He said areas where staff need more training include nuclear infrastructure, operators, engineers, research and development staff who help support the project.

At the Barakah power plant, Emirati trainees spend hundreds of hours during the two-year Energy Pioneers programme learning how to deal with potentially catastrophic scenarios in a simulator.

A strong grasp of maths and physics means nuclear engineering students are not short of job opportunities.

"A recent study found that nuclear majors have the lowest unemployment rate. I was surprised as there are few 'nuclear engineering' jobs but those with nuclear backgrounds can go into many other sectors such as finance, management, environmental, medical and industrial research and applications," said Dr Anthony Hechanova, head of advanced energy engineering technology at Abu Dhabi Polytechnic.

The programme he heads at Abu Dhabi Polytechnic is tailored to prepare young people to operate, maintain and manage a nuclear plant.

"This is what we call career technical education," Dr Hechanova said.

"The skills and expertise are very different than those of an engineer, who can design mechanical and electrical systems while the technical workforce has to operate and maintain these systems and keep them and the workforce safe. This requires a vastly different knowledge and skillset."
Nuclear specialists are at the cutting edge of technologies, he said.
"In the UAE, the advent of commercial nuclear power production is a game changer in this fossil fuel rich region," he said.
"The importance of diversification will be felt every time the price of oil and gas fluctuates. Nuclear power will allow fossil resources to be preserved and the wealth of the nation and sustainability of the Earth to be extended and expanded."
Lady Barbara Judge, former head of the UK Atomic Energy Agency, said countries would generally train their staff locally, although the UK, the US and Russia, along with France, Japan have the most expertise. "With new nuclear countries like the UAE, they are training many at home as well as sending many abroad" she said. "Once the nuclear education programme is fully up and running, then they'll train most at home. I am very impressed by the excellence of the education programme that the UAE has created."

Retrospective Imaging and Characterization of Nuclear Material

Health Physics. 113(2):91–101, AUG 2017
By Robert B. Hayes and Sergey Sholom
Source: https://insights.ovid.com/crossref?an=00004032-201708000-00001

Modern techniques for detection of covert nuclear material requires some combination of real time measurement and/or sampling of the material. More common is real time measurement of the ionizing emission caused by radioactive decay or through the materials measured in response to external interrogation radiation. One can expose the suspect material with various radiation types, including high energy photons such as x rays or with larger particles such as neutrons and muons, to obtain images or measure nuclear reactions induced in the material. Stand-off detection using imaging modalities similar to those in the medical field can be accomplished, or simple collimated detectors can be used to localize radioactive materials. In all such cases, the common feature is that some or all of the nuclear materials have to be present for the measurement, which makes sense; as one might ask, "How you can measure something that is not there?" The current work and results show how to do exactly that: characterize nuclear materials after they have been removed from an area leaving no chemical trace. This new approach is demonstrated to be fully capable of providing both previous source spatial distribution and emission energy grouping. The technique uses magnetic resonance for organic insulators and/or luminescence techniques on ubiquitous refractory materials similar in theory to the way the nuclear industry carries out worker personnel dosimetry. Spatial information is obtained by acquiring gridded samples for dosimetric measurements, while energy information comes through dose depth profile results that are functions of the incident radiation energies.

After nuclear midnight: The impact of a nuclear war on India and Pakistan

By Karthika Sasikumar
Bulletin of the Atomic Scientists. Volume 73, 2017 - Issue 4
Source: http://www.tandfonline.com/doi/full/10.1080/00963402.2017.1338009

During the past decade, computer models have predicted that the physical impacts of a nuclear exchange between India and Pakistan, or even a single strike on a large city, would be devastating. The social, economic, and political impacts – although less well known – would also be crippling and would reverberate throughout the world. Efforts to use "Armageddon estimates" to scare the people of India and Pakistan have thus far not significantly reduced the risk of nuclear weapons use in this turbulent region. However, the increasing penetration of television and social media may give members of the public a better grasp of the scale of potential devastation. Combined with educational efforts

targeted at media elites, increased public awareness of the consequences of a nuclear attack may help to reduce the pressure on political leaders to exercise the nuclear option.

Indian nuclear forces, 2017

By Hans M. Kristensen and Robert S. Norris

Bulletin of the Atomic Scientists. Volume 73, 2017 - Issue 4

Source: http://www.tandfonline.com/doi/full/10.1080/00963402.2017.1337998

India continues to modernize its nuclear arsenal, with at least four new weapon systems now under development to complement or replace existing nuclear-capable aircraft, land-based delivery systems, and sea-based systems. India is estimated to have produced enough plutonium for 150–200 nuclear warheads but has likely produced only 120–130. Nonetheless, additional plutonium will be required to produce warheads for missiles now under development, and India is reportedly building two new plutonium production facilities. India's nuclear strategy, which has traditionally focused on Pakistan, now appears to place increased emphasis on China.

Indian nuclear forces, 2017.

Type	NATO designation	Number of launchers	Year deployed	Range[i] (kilometers)	Warhead x yield (kilotons)	Number of warheads
Aircraft						
Vajra	Mirage 2000H	~16	1985	1,850	1 × bomb	~16
Shamsher	Jaguar IS/IB	~32	1981	1,600	1 × bomb	~32
Subtotal:		~48				~48
Land-based ballistic missiles						
Prithvi-2	n.a.	~24	2003	350[ii]	1 × 12	~24
Agni-1	n.a.	~20	2007[iii]	700+	1 × 40	~20
Agni-2	n.a.	~16	2011[iv]	2,000+	1 × 40	~16
Agni-3	n.a.	~8	2014?	3,200+	1 × 40	~8
Agni-4	n.a.	n.a.	(2018)	3,500+	1 × 40	n.a.
Agni-5	n.a.	n.a.	(2020)	5,200+	1 × 40	n.a.
Subtotal:		*~68*				*~68*[v]
Sea-based ballistic missiles						
Dhanush	n.a.	2	2013	400	1 × 12	2
K-15	(Sagarika)	(12)	(2017)	700	1 × 12	(12)
K-4	n.a.	n.a.	?	~3,000	1 × ?	n.a.
Subtotal:		*(14)*				*(14)*
Total						**~118 (130)**[vi]

[i]Range listed is unrefueled combat range with drop tanks.

[ii]US NASIC has estimated the range as 250 kilometers (155 miles) but we assume the range has probably been increased to about 350 kilometers (217 miles) as stated by the Indian government.

[iii]Agni I first began induction with the 334th Missile Group in 2004 but did not become operational until 2007.

[iv]Agni II first began induction with the 335th Missile Group in 2008 but did not become operational until 2011.
[v]The missile and warhead inventory may be larger than the number of launchers, some of which can be reused to fire additional missiles. This table assumes an average of one warhead for each launcher.
[vi]The number in parenthesis includes 12 warheads possibly produced for the first SSBN, but not yet operational, for a total stockpile of roughly 130 warheads.

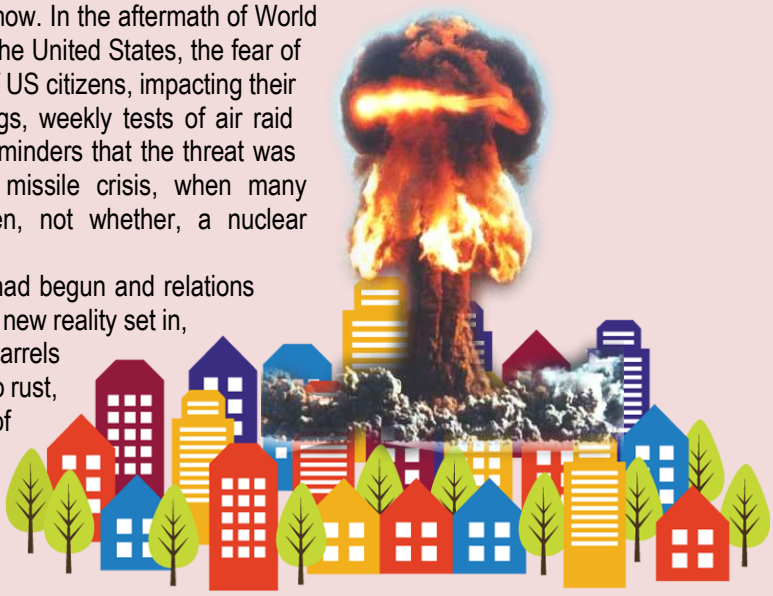
US cities are not medically prepared for a nuclear detonation

By Jerome M. Hauer

Bulletin of the Atomic Scientists. Volume 73, 2017 - Issue 4

Source: http://www.tandfonline.com/doi/full/10.1080/00963402.2017.1338003

It's been more than five decades since concern about a nuclear conflagration was as prominent a focus for world leaders as it is again now. In the aftermath of World War II, during the Cold War between Russia and the United States, the fear of nuclear attack was front and center in the minds of US citizens, impacting their daily lives. Fallout shelter signs on office buildings, weekly tests of air raid sirens, and drills by school children were stark reminders that the threat was real. Anxiety peaked during the 1962 Cuban missile crisis, when many Americans believed it was a question of when, not whether, a nuclear confrontation with Russia would occur.



Less than three decades later, though, glasnost had begun and relations had thawed between the two archenemies. As this new reality set in, so did complacency about planning for the worst. Barrels of supplies stored in fallout shelters were allowed to rust, and their contents deteriorated to the point of uselessness. The ensuing period of cooperation between the superpowers, for all its benefits, also left us with a form of amnesia. The United States is now completely unprepared to manage the aftermath of a nuclear detonation.

The case for preparedness

Some would argue that the possibility of any type of nuclear attack is so low that expending energy to discuss the threats, much less plan for an attack, is a fool's errand. It is true that the probability of a nuclear detonation on US soil is low; on the other hand, it could happen. We know that North Korea has constructed and tested nuclear devices, and that its leader, Kim Jong-un, has verbally threatened the United States and US allies. We know that Pakistan's stockpiles of highly enriched uranium, or HEU – the critical component needed to make an improvised nuclear device or nuclear bomb – are not especially secure, and a change in regime could leave the material in the hands of leaders who support terrorism. We know we lack the ability to prevent HEU from being smuggled into the United States. We know that it is quite possible to obtain 55 kilograms of HEU, the amount required to build a 10-kilotons (kt) nuclear bomb, which is around the size of the "Little Boy" dropped on Hiroshima in 1945. As remote as the possibility may be, the use of a nuclear device in a major city would have long-term catastrophic consequences. It would be irresponsible in every sense, knowing that a nuclear strike by a terrorist group or hostile nation is possible, not to plan for such an event.

What we're up against

There are four types of potential nuclear incidents that require some level of preparation: an accident or attack at a nuclear power plant, a dirty bomb, terrorist use of an improvised nuclear device, and an attack using a nuclear weapon executed by a foreign nation.

The first two types of events – an incident at a nuclear power plant and a dirty bomb – have received a greater level of planning attention than the others. An attack on a nuclear power plant or a catastrophic accident like the ones that occurred at Chernobyl in 1986 and Fukushima in 2011 would

have devastating short- and long-term effects. With that in mind, the Federal Emergency Management Agency (FEMA) and Department of Energy require that states with nuclear power plants practice notification, response, and evacuation plans. Zones requiring specific actions have been designated depending on communities' proximity to nuclear power plants. Fortunately, the track record of the US nuclear power industry has been reassuring in terms of planning for accidents.

The possibility of a dirty bomb attack has also received planning attention from US authorities, in part because it is seen as relatively likely on the spectrum of nuclear disasters. A dirty bomb is a rather simple device composed of a conventional explosive – much like the one used to blow up Oklahoma City's Alfred P. Murrah building in 1995 – laced with radiological materials called isotopes. Gaining access to radioactive isotopes is not as challenging as one might expect. Medical facilities use various types for diagnostic testing, and several industries require them. Certain isotopes, while difficult to come by, have a long half-life, and if used in a dirty bomb would contaminate the blast area and that around it with residual radioactive material for months or years. This would create a "hot zone" too dangerous to enter for any type of firefighting, rescue, or reconstruction activity. Additionally, radioactive particles dispersed in the air can be carried downwind in a "plume" and deposited far from the explosion. Planning for the aftermath of a dirty bomb will vary from city to city. Most cities have some level of preparedness for managing a mass-casualty event, but the problem of radiation contamination adds complexity. The majority of contamination can be handled by removing clothing and washing victims' skin. Once victims are removed from the area, the residual ground and building contamination is a less urgent problem, and decisions about clearing the area will likely be made by city authorities in conjunction with federal agencies.

The most devastating kind of incident would involve a nuclear weapon: Terrorists could acquire or build and detonate an improvised nuclear device in a major city, or – worse because the bomb would be bigger – a foreign nation could launch a nuclear attack.

In the first scenario, the device would likely be between 5 and 10 kt. A 10-kt bomb would release the same amount of energy as 10,000 tons of TNT. The kind of improvised nuclear device we are most likely to see is a "gun" type of bomb that would use an explosive to fire a mass of HEU through a tube at another mass of HEU, causing fission and the release of energy in an eruption of pressure, light, and heat. A 10-kt improvised nuclear device would destroy or significantly damage everything within a half-mile radius.

An attack by a government with a long-standing nuclear weapons program could be orders of magnitude worse. The strength of the explosion could range from something around 10 kt – the size of a nuclear bomb North Korea tested in 2013 – to measurements in the megatons, or hundreds of times greater. In a nuclear attack, the bomb will be dropped from an aircraft or delivered via missle. Unlike a bomb carried into a city on a truck, a bomb delivered by air can be detonated above a city rather than at ground level, causing a larger area of destruction and loss of life.

In the discussion that follows, I make the assumption – based on information from open-source material – that terrorists are unlikely to construct a device greater than 10 kt, and that a missile launched by North Korea would carry a warhead in the 10–15 kt range. These scenarios are both more likely than a multimegaton nuclear warhead being launched at the United States.

What to expect

For those who must think about planning for the aftermath, one of the starkest facts about a nuclear bomb attack is that on top of killing people on a vast scale, it will thoroughly destroy the capacity to respond.

When a nuclear bomb made with HEU detonates, it releases an enormous amount of energy of four different types. The blast releases 50 percent of its energy in the form of a pressure wave so powerful that it levels buildings. There is little chance for human survival within a quarter mile, and as the wave travels farther out and weakens, it can shatter glass within half to three quarters of a mile. Thirty-five percent of energy from the blast creates the blinding flash, emitting heat that incinerates all but concrete buildings (and melting glass and burning the contents even in those). Fires will be so numerous and radiation levels so high that firefighting will be impossible. Initial (or "prompt") radiation accounts for 5 percent of the energy. The remaining 10 percent is released in long-term fallout or residual

radiation, which can, when carried by wind, travel over long distances.

Should an improvised nuclear device detonate in New York City's Times Square, the initial blast will kill between 75,000 and 100,000 people in seconds. They will be incinerated so thoroughly that their ashes will be indistinguishable from the ashes of the buildings around them. Others will be crushed by falling buildings, struck by flying debris, or thrown by the pressure wave against buildings, the ground, or each other.

Another 100,000–200,000 people will be injured, some with burns from the heat of the blast, others by objects hurtling through the air. Many will be exposed to various levels of radiation that will cause suffering or death over weeks and months. The loss of city government, fire and police departments, and other emergency responders, coupled with demolished hospitals and destroyed water, sewage, power, and gas lines, means that repairs will take months or years even outside the contaminated "hot zone" and be impossible within it. The city will become a ghost town. As a result of the plume carrying radioactive particles downwind, hundreds of square miles may be unusable and need decontaminaion.

People will leave their homes in search of safe havens. With no radios to give them instructions, some will move into the path of the plume and be exposed to a higher dose of radiation than they would have received had they stayed home. Many of these evacuees will die from radiation exposure.

Chaos will prevail as millions of people try to evacuate the city without aid of communications systems, which will have been destroyed. They won't know where to go or where to receive medical care. Following a hurricane, people can reach shelters, medical teams, and sources of food and water that were deployed in advance. Following a nuclear attack, none of these assets will have been prepositioned prior to the explosion.

In the early 1980s, while living outside of Boston, I received a pamphlet in the mail instructing me to evacuate to a specific town should the worst happen. A reporter following this effort to prepare citizens traveled to several of the "host" towns to determine their readiness to receive all the evacuees. The reporter was startled to find townspeople who said the new arrivals wouldn't be welcome. Where would city evacuees go if an attack occurred today?

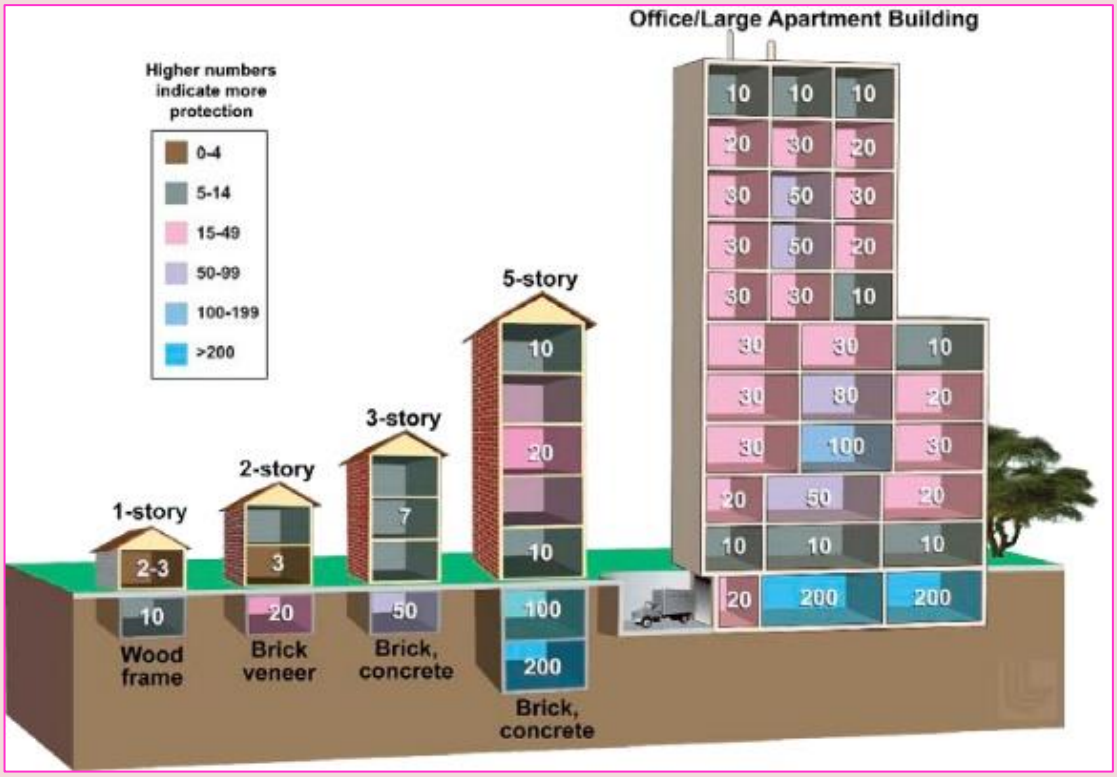
A massive medical challenge

From 2009 to 2010, as part of research I was doing for the Defence Academy of the United Kingdom, I conducted an end-to-end assessment of the medical capabilities of several countries and cities to respond to terrorist use of an improvised nuclear device. (It was similar to one I completed while serving as director of the Mayor's Office of Emergency Management in New York City, looking at the aftermath of biological and chemical attacks.) No city or country visited during this assessment was prepared to manage the aftermath of a nuclear detonation. Even taking into account just the medical needs of a large city following a nuclear attack, the results clearly showed that current planning efforts were not sufficient to manage the carnage.

Using New York City as a model, it's anticipated that several hundred thousand people will require some sort of medical evaluation or care. With the loss of hospitals and 35–50 percent of first responders, and health care personnel unable or unwilling to go to work, surviving hospitals will need to use every inch of space to treat only the most critically injured. Makeshift treatment centers or casualty collection points near the blast will be required to triage the injured. Ethical and moral issues will arise as the overwhelmed staff, short on supplies, is forced to decide who should receive treatment and who should be moved to end-of-life care, receiving morphine to ease their pain. The profound psychological impact on these healthcare workers and first responders cannot be overstated. Their task is essential, though: The ability to make some order out of the chaotic wave of people with different levels of injuries, from those with various kinds of physical trauma to those with psychological trauma to the "worried well," is a key to reducing morbidity and mortality.

Certain characteristics of nuclear attacks make them especially hard to prepare for. A nuclear blast causes an electromagnetic pulse that knocks out communication systems, some irreversably. Without the ability to communicate, coordination among medical personnel and other first responders will become nearly impossible. Assuming medical staff can get to where they need to be, demand for them will be extraordinary, but managers will have to rotate them to prevent exhaustion and reduce the psychological impact.

There will be an overwhelming number of patients. After triage, some will have to be transported. Hospitals will have to not only care for the injured but also control security and coordinate the flow of information to victims' families. Local, state, and federal governments



will have to rapidly set up alternate-care facilities close to the "hot zone." They will have to have plans for alternate standards of care, so that, for example, emergency medical technicians are allowed to perform tasks ordinarily reserved for paramedics or nurses, freeing paramedics and nurses to perform more advanced medical treatment than normally permitted. This last issue, the focus of numerous studies and reports, presents both legal and ethical challenges, many of which need to be resolved in state capitals, where the scope of practice for health care professionals is typically controlled. And planners should remember that just because an ethical issue is resolved in advance, doesn't mean that the decision will be followed in practice in the aftermath of a disaster. Sending an adult to end-of-life care may pull on the heartstrings, but sending a child to the same fate could prove to be too difficult for many medical personnel.

Beyond the difficult frontlines of triage, survivors of a nuclear explosion will have a variety of injuries, some well known to modern hospitals but others more difficult to diagnose and develop a plan for. Acute radiation syndrome, in particular, results from exposure to radiation and does not have to coincide with any other injury. It may be the only effect a survivor suffers, and it may not manifest soon after exposure. Acute radiation syndrome occurs when a significant portion of the body is exposed to a large dose of penetrating radiation in a short period of time. The nature of acute radiation syndrome depends on the dose. At lower doses, the only effect may be on the gastrointestinal system and bone marrow. At higher doses, bone marrow will stop producing infection-fighting white blood cells, platelets that assist in blood clotting, and red blood cells that carry oxygen. Larger doses also destroy the lining of the gastrointestinal system, causing diarrhea, vomiting, and an inability to swallow or digest food, requiring patients to receive nutrition and fluids intravenously. At the highest levels of exposure, the heart and nervous system are impacted and rapid progress toward death is certain. Some of the most difficult patients to manage are those with combined injuries – say, a penetrating wound from a shard of glass, requiring rapid surgical intervention, and also acute radiation syndrome.

Finally, a great moral and societal challenge will be managing the dead. Many victims will be in the "hot zone," where responders can't enter and radiation

levels may not be safe for years. Victims' families, though, will demand recovery of loved ones. Even where identifiable remains exist, the number of dead will be so large that months may pass before a family receives them. At some point in recovering bodies, a decision may have to be made to bury victims in mass graves. The United States has excellent systems in place to manage mass fatality incidents – but they have never been tested with several hundred thousand dead at one time.

Where do we stand?

These issues have not received enough attention from FEMA, the US government entity responsible for helping states plan for and respond to disasters. FEMA takes what emergency planners call an "all hazards" approach, meaning it addresses effects common to many different types of disasters. This lack of planning to deal specifically with a nuclear incident is a serious weakness.

That makes it all the more important for states and cities to have their own plans in place for worst-case scenarios. It's far easier to scale back a response if resources are not needed than to need them but not have them. While serving as Commissioner of Homeland Security and Emergency Services for New York State, I asked each of the 57 counties to plan for what they thought to be a worst-case scenario. (Scenarios varied from county to county.)

Where FEMA has lagged, the US Department of Health and Human Services has aggressively built up its capability to respond to a nuclear incident. It has medical response teams that are staffed and equipped to mobilize in response to an incident, support state and local governments, and, depending on what is needed where, either provide comprehensive health care infrastructure or augment existing hospitals and clinics. In the aftermath of Hurricane Sandy in 2012, these teams provided the only medical care available to some communities on Long Island, just east of New York City. They provided invaluable aid in evacuating Manhattan hospitals.

The Department of Health and Human Services has also committed significant resources to acquiring medical treatments for the survivors of a nuclear detonation. The Strategic National Stockpile, composed of 12 separate units at classified locations around the country, is also under the department's control, and capable of being dispatched to any city within 12 hours. In it are supplies to treat burn injuries, as well as cutting-edge therapeutics to aid in reversing the effects of radiation by stimulating bone marrow to produce platelets (which help stop bleeding) and white blood cells (which help prevent infection). Should respirators be needed, the Strategic National Stockpile can provide them, along with antibiotics, vaccines, and massive quantities of intravenous solutions. Many units from the stockpile will be needed to support a city in the aftermath of a nuclear detonation.

Cities far from the nuclear blast are also a potential resource. The federal government is sure to ask for help from far afield as soon as demand for medical resources exceeds local supply in a given area. Governors and mayors may be reluctant to release personnel, though, either for political reasons or out of concern that their cities and states may be targeted next. I believe most elected officials will rise to the occasion, and dispatch as much help as they can spare. But no number of simulated incidents can predict how political dynamics will shift following the real thing.

Over the course of the study I conducted in 2009 and 2010, several government officials said they were unable to take steps forward because the elected officials they reported to were unwilling to discuss the issue. Privately, many politicians used to worry that if they discussed nuclear terrorism, they would likely be ridiculed for fearmongering. In the last seven years, that concern has changed dramatically at the national level, with President Obama and other world leaders convening to address nuclear proliferation and nuclear terrorism. Silence at the local level continues, though. Among city and state governments, the only ones that I'm aware have some level of ongoing planning for nuclear disaster are New York (city and state), Washington state, Los Angeles, Boston, and Chicago. To a much lesser extent, several more cities are engaged as well. The state of Hawaii has asked the federal government for assistance in planning for a nuclear attack.

A path forward

In 1965, the folksinger Barry McGuire recorded the powerful lyrics "We're on the eve of destruction" in the song "Eve of Destruction." Perhaps that one-time hit should be resurrected to remind US leaders that we are not prepared for nuclear disaster. To those who say that preparing for such an incident makes an enemy more likely to strike

sooner, I would argue otherwise. It is highly unlikely that preparedness would factor into any decision to detonate a device on American soil. Plus, a terrorist group would find it challenging to gauge the level of US preparedness.

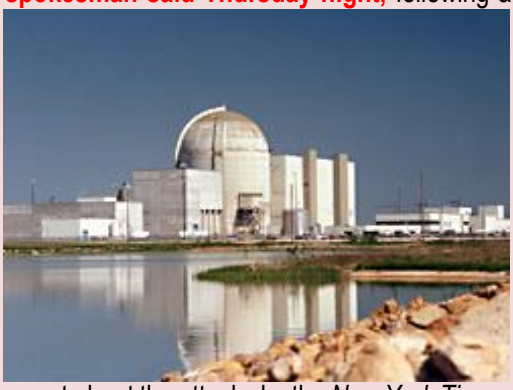
Realistically, no matter the level of preparedness, detonating a nuclear bomb in an American city would cause immediate and enormous loss of life, vast destruction, and trillions of dollars in damage. It would cripple the US economy and dramatically impact other nations' financial stability, for years if not decades. That is why it is our responsibility to educate the public. The reinvigoration of US civil defense programs should not be a matter of debate or concern over political impact. It needs to be mandated at every level of government so that the United States is prepared for a nuclear Armageddon.

__Jerome M. Hauer__ has served in cabinet positions at the local and state level and was an acting assistant secretary for the Office of Public Health Emergency Preparedness at the US Department of Health and Human Services. Hauer is an associate editor of the Journal of Special Operations Medicine and president of the Homeland Security Section of the Health Physics Society. He earned his doctorate at Cranfield University, has a master's degree from the Johns Hopkins School of Public Health, and holds a bachelor's degree from New York University. He is also an Adjunct Associate Professor at Georgetown University and Visiting Professor at the Cranfield University.

Russian hackers likely behind cyberattacks on U.S. nuclear operators: Experts

Source: http://www.homelandsecuritynewswire.com/dr20170707-russian-hackers-likely-behind-cyberattacks-on-u-s-nuclear-operators-experts

July 07 – **Attacks by hackers on Wolf Creek Nuclear Operating Corporation in Burlington, Kansas have had "absolutely no operational impact," the company's spokesman said Thursday night,** following a

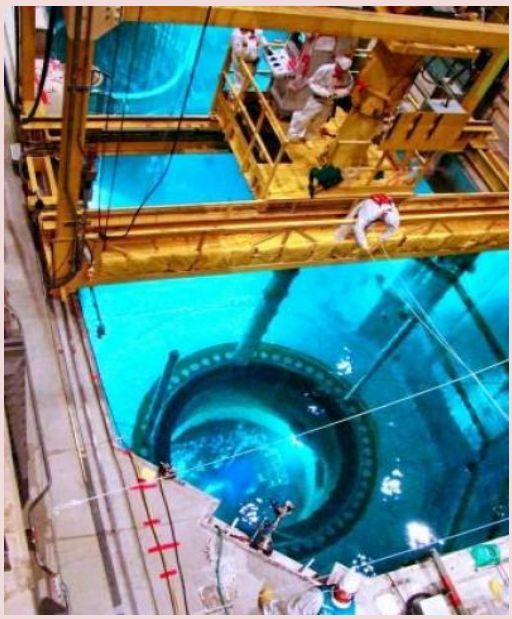


report about the attacks by the *New York Times*.

A report issued by DHS and the FBI concluded that hackers have targeted the nuclear corporation and other nuclear power operators since May, the *Times* reported (also see this detailed *Bloomberg*'s report).

Wolf Creek communications director Jenny Hageman said the facility's operational computer systems are separate from the corporate network.

"The safety and control systems for the nuclear reactor and other vital plant components are not connected to business networks or the internet," Hageman said. "The plant continues to operate safely."



The *Times* reported that the hackers sent emails with resumes which contained code allowing attackers access to senior employees' credentials and other network machines.

The source of the hacking is not clear, but *Bloomberg* reports that according to three people familiar with the continuing effort to eject the hackers

from the computer networks, the chief suspect is Russia.

The possibility of a Russia connection is particularly worrisome, former and current officials say, because Russian hackers have previously taken down parts of the electrical grid in Ukraine and appear to be testing increasingly advanced tools to disrupt power supplies.

Had the plant been successfully hacked, the attack would have to be reported to the Nuclear Regulatory Commission (NRC) which would have to inform the public, said John Keeley with the Nuclear Energy Institute.

CNet reports that DHS and the FBI said it was most concerned about the "persistence" of the attacks on choke points of the U.S. power supply. The language used by the two agencies suggests that hackers are trying to establish backdoors on the plants' systems for later use.

*Bloomberg*notes that those backdoors can be used to insert software specifically designed to penetrate a facility's operational controls and disrupt critical systems.

"We're moving to a point where a major attack like this is very, very possible," Galina Antova, co-founder of Claroty, a New York firm that specializes in securing industrial control systems Antova, told *Bloomberg*. "Once you're into the control systems — and you can get into the control systems by hacking into the plant's regular computer network — then the basic security mechanisms you'd expect are simply not there."

Industry experts and U.S. officials take the attacks on U.S. nuclear operators seriously, partly as a aresut of recent Russian government hackers' attacks on Ukraine's power infrastructure.

Scott Aaronson, executive director for security and business continuity at the Edison Electric Institute, an industry trade group, told *Bloomberg* that utilities, grid operators and federal officials were already dissecting the attack on Ukraine's electric sector to apply lessons in North America before the U.S. government issued the latest warning to "energy and critical manufacturing sectors."

The Russian cyberattacks in Ukraine did not cause long-term damage, but with each escalation, the hackers may be gauging the world's willingness to push back.

"If you think about a typical war, some of the acts that have been taken against critical infrastructure in Ukraine and even in the U.S., those would be considered crossing red lines," Antova said.

President Donald Trump signed an executive order on 11 May aiming to strengthening cybersecurity for federal and infrastructure networks, but critics say that funding cuts included in the administration's budget proposal leave the nation's nuclear reactors exposed. A 23 May news release issued by the Nuclear Energy Institute, said Trump's proposed budget does not sufficiently support the nation's existing reactors.

New technique detects radioactive material even after it is gone

Source: http://www.homelandsecuritynewswire.com/dr20170707-new-technique-detects-radioactive-material-even-after-it-is-gone

July 07 – **A new technique allows researchers to characterize nuclear material that was in a location even after the nuclear material has been removed** – a finding that has significant implications for nuclear nonproliferation and security applications.

"Basically, we can see nuclear material that is no longer there," says Robert Hayes, lead author of paper describing the work and an associate professor of nuclear engineering at North Carolina State University. "For example, we could identify and characterize a dirty bomb based on samples taken from a room the bomb was in a year ago.

"This is a valuable tool for emergency responders, nuclear nonproliferation authorities and forensics, because it allows us to get a rough **snapshot of the size of a radiation source, where it was located, how radioactive it is, and what type of radioactive material it is,"** Hayes says.

NCSU says that the technique takes advantage of the fact that **radioactive material changes the arrangement of valence electrons – or outer electrons – in insulator materials, such as brick, porcelain, glass – even hard candy**. Basically, radiation displaces electrons at defect sites in the crystalline structure of these materials.

By taking samples of multiple materials in a room, applying conventional radiation dosimetry techniques, and

evaluating how the electrons at those defect sites are organized, researchers can determine the presence and strength of any nuclear materials that were in that room.

"If the samples were taken at regular intervals in a grid pattern, the relative radiation dose profile can be used to triangulate where in the room the source was located, in three dimensions," Hayes says. "It can also provide a very rough idea of the physical size of the source, but that depends on various factors, such as how close the source was to the materials being sampled."

By taking a core sample of the insulating material, and measuring the radiation dose at various depths in the material, researches can also ascertain what type of radiation source was present. This is possible because different radioactive materials have characteristic distributions of gamma rays, X-rays, etc., and each type of energy penetrates materials with different strength.

"This is not extremely precise, but it does allow us to answer important questions. For example, distinguishing between different kinds of nuclear material such as naturally occurring, medical, industrial, and 'special' nuclear materials – the latter being used for nuclear weapons," Hayes says.

"This is a proof of concept," Hayes says. "We're now focused on exploring its detection limitations along with spatial and energy resolution, and how to make use of this approach moving forward.

"But this is a big deal for nuclear nonproliferation efforts, because it means you can't handle nuclear material in secret anymore," Hayes adds. "It means the world is now densely blanketed by low-resolution integrating gamma-ray spectrometers, so we can always go back and measure what was present. There's no hiding."

— Read more in Robert B. Hayes and Sergey Sholom, "Retrospective imaging and characterization of nuclear material," Health Physics113, no. 2 (August 2017): 91-101.

Norway 'shamed' over 'nuclear nod'

Source: http://www.newsinenglish.no/2017/07/10/norway-shamed-by-nuclear-nod/

July 10 – Opponents of nuclear weapons were claiming that Norway should be ashamed of itself, for once again failing last week to support a UN resolution to ban them. Another 123 countries had already agreed to negotiate a "legally binding instrument to forbid nuclear weapons."

Foreign Minister Børge Brende (left) and Prime Minister Erna Solberg are usually active supporters of UN resolutions, but not one involving a potential ban on nuclear weapons. Anti-nuclear activists call that a "shame for Norway." PHOTO: Statsministerens kontor

Norway instead joined the US, Russia, Great Britain, France and 33 other countries in voting against the negotiations proposal last December. China, India, Pakistan, Japan and South Korea abstained. When the proposal to actually ban nuclear weapons came up for a vote late last week, Norway had no intention of supporting it.

Norwegian officials have claimed that it couldn't even participate in the negotiations for the measure that won support over the weekend, claiming it would violate its obligations as a member of the NATO defense alliance.

That argument is firmly rejected by anti-nuclear activists in Norway and abroad. "It's a shame that Norway is not part of this," declared Erling Borgen a filmmaker and journalist who is also on the board of Norway's anti-nuclear organization *Nei to atomvåpen*.

Borgen told newspaper *Dagsavisen* that several international anti-nuclear activists have condemned Norway for its "hypocritical" stand on the proposed ban. They include, according to Borgen, "well-known activists" like Setsuko Thurlow, who survived the bombing of Hiroshima, and Abacca Anjain-Madison from the Marshall Islands, who was affected by nuclear testing in the Pacific.

"They call the Norwegian position on this a shame, and believe that the country that doles out the Nobel Peace Prize must reverse it," Borgen said.

Frode Ersfjord, who heads *Nei to atomvåpen*, said the proposed UN ban on nuclear weapons is the product of 71 years of negotiations. "The nine countries with nuclear weapons have fought hard to avoid this, precisely because it will immediately have a strong political effect," Ersfjord told *Dagsavisen*. The measure will prohibit any use of nuclear weapons, or nuclear physical explosions, along with the threat of using them.

The resolution will be open for signing from September 20, and Borgen claimed that then Norway must at least do so. "Norway has to wake up on this," he said, adding that he hopes it will become an issue in the upcoming parliamentary election campaign.

"We're living in frightening times politically, when many countries threaten use of nuclear weapons," Borgen said. "The nuclear weapons powers have had the podium for 20 years, now we're banking on a prohibition that in fact will stygmatize those who use nuclear weapons." He claims NATO is no hindrance to the UN measure, claiming there's no problem with being a member of NATO and opposing weapons of mass destruction.

Lab mistakenly ships radioactive material aboard commercial plane

Source: http://www.homelandsecuritynewswire.com/dr20170714-lab-mistakenly-ships-radioactive-material-aboard-commercial-plane

July 14 – **Employees at the Los Alamos National Laboratory have been fired and disciplinary action against other personnel was taken after small amounts of radioactive material were mistakenly shipped aboard a commercial cargo plane.**

Officials at the lab did not offer any details regarding disciplinary actions, except to say that those individuals involved in the mishap, including those in higher management, have been held to account.

Las Cruces Sun-News reports that Los Alamos has transferred responsibility for the shipment of some nuclear materials to another division within the lab and has imposed additional controls for making shipping labels to prevent similar problems in the future.

"Although these shipments arrived safely at their destinations and no one was hurt, this mistake, taken together with other mistakes in recent years, is unacceptable and is in the process of being addressed promptly and thoroughly," the lab said in a statement. "Our response to this incident is not business as usual."

In June, National Nuclear Security Administration (NNSA) launched an investigation after the lab admitted that procedures for shipping small amounts of "special nuclear material" to facilities in California and South Carolina were not followed.

The radioactive material had been packaged for ground transport, but by mistake was shipped via a commercial air cargo service.

U.S. regulations prohibit the shipment of radioactive material by air.

Nuclear experts say the mishap could have led to serious consequences. The rapid pressure changes during flights could have damaged the packaging, causing radiation to escape.

When the shipment arrived at its destination, it was immediately tested, but no contamination or loss of radioactive material were detected.

The *Sun-News* notes that the incident was the latest in a series of safety mishaps at Los Alamos – which is especially worrisome, as the lab is set to ramp up production of a key plutonium component for the U.S. nuclear weapons arsenal.
Federal regulators are in the process of reviewing the lab's recent safety record.
Lab officials say that improvements have been made at the lab's plutonium facility – the same facility where the atomic bomb was developed during the Second World War.
The lab said that the personnel actions and the changes to the shipping procedure are only the first steps in a broad campaign to improve safety measures.
Los Alamos National Security LLC manages the complex under a $2.2 billion contract which ends in 2018. Critics suggest putting the management contract up for bids would offer incentives to make even more changes at Los Alamos.

Will Trump Stop the 10 Chinese Companies Supplying North Korea's Nuclear Program?

Source: http://www.newsweek.com/2017/07/21/trump-stop-chinese-companies-supplying-north-koreas-nuclear-weapons-635538.html

July 13 – The **city of Dandong**, in China's northeastern Liaoning province, appears to be an embarrassing relic of the country's economic past. Old, run-down state-owned factories sit on the outskirts of a town full of dreary office buildings. There is none of the flash and glitz so prevalent in China's far more prosperous cities.

But Dandong is nevertheless one of the most important cities in China, because it sits just across the border from North Korea and is Pyongyang's economic lifeline. Nearly 85 percent of North Korea's global trade is with China, and much of that flows through Dandong. That includes the machinery, purchased in contravention of both U.S. and U.N. sanctions, needed to build nuclear weapons, as well as the missiles needed to deliver them. And, crucially, Dandong is also the source of the offshore financing from Chinese banks that Pyongyang needs to pay for its illicit weapons program.

That program took yet another step forward on July 4, America's Independence Day, when Pyongyang successfully tested a missile capable of reaching Alaska. This latest in-your-face provocation from North Korean leader Kim Jong Un came after President Donald Trump had signaled that his strategy for reining in the North—relying on China to use its clout with the Pyongyang regime—had failed. "At least we know China tried," Trump tweeted on June 20.

But the U.S. and some of its allies in East Asia privately acknowledge that they don't think Beijing tried hard enough. A recent White House policy review of U.S. strategy toward North Korea, completed late this spring, has emboldened those in the administration who believe Washington and its allies have the ability to increase the economic pressure on Pyongyang—but only by going after the Chinese companies that funnel money and dual-use technology (equipment that can have an innocent purpose but which the North can also use in its weapons program) to Pyongyang.

Doing so may be easier than most of the outside world understands if—and only if—Washington is willing to offend Beijing. While more than 5,000 Chinese companies do business with North Korea each year, trade between the two countries is dominated by just a handful of large companies, several of which are based in Dandong. In late June, the U.S. asked Beijing to go after 10 companies and individuals who, Washington believes, play an outsize role in China's trade with North Korea—including selling parts and machinery used in Pyongyang's weapons program.

Why wouldn't Beijing do all it could to crack down on its own companies playing such a significant role in the North Korean economy? U.S. and allied intelligence analysts are divided on the answer. Some believe that the heads of the big conglomerates doing business with Pyongyang—a long-standing Chinese ally—are politically connected in Beijing. With a once-every-five-years Communist Party congress coming up in the fall, President Xi Jinping and his political allies don't want to make more enemies of powerful businessmen, many of whom are already angry at China's anti-corruption drive. Other analysts simply believe that a nuclear North means a permanently divided peninsula, rather than one under Seoul's rule, and that Beijing will forever be happy with that arrangement because it wants no part of a united Korea allied with the U.S. on its border.

The U.S. told Beijing that if China hadn't made progress by the end of the summer in sanctioning the "Chi-NoKo 10," as one American official puts it, then the U.S. would do so unilaterally. And on June 30, the Trump administration signaled it was serious: It announced sanctions against the Bank of Dandong, accusing it of facilitating financing for the North's weapons program. On July 5, at the United Nations, Trump's ambassador, Nikki Haley, delivered a blunt message to Beijing: "We will look at any country that chooses to do business with this outlawed regime." That same day, the commander of U.S. forces in South Korea, General Vincent Brooks, said the U.S. and its ally were ready to go to war if necessary, to prevent nuclear proliferation in North Korea. "Self-restraint, which is a choice, is all that separates armistice and war," Brooks said.

The change in the administration's policy toward the North is striking. In the wake of Trump's summit meeting with Xi at Mar-a-Lago in April, the administration's attitude toward China had seemed to become unexpectedly warm. During the campaign, Trump bashed China relentlessly as a trade predator and a bad actor militarily in the South China Sea. The U.S. seemed to be girding for a full-blown cold war with Beijing. That changed after Mar-a-Lago. Trump said after meeting Xi that he understood that there was a long, complicated history between the two countries. He seemed implicitly to accept Beijing's premise that it was harder than the outside world believed to coerce Pyongyang to behave. And he deferred to Beijing to deal with its unruly ally.

The irony is that behind the scenes—in work being done by both intelligence agencies and private firms digging into the North's trade with Beijing—analysts were becoming convinced that Xi had played Trump, and that China, in fact, did have the means to curb Kim if it chose. Beijing has, over the years, portrayed the companies who do business with the North as rogue firms, small private traders who worked hard to stay in the shadows and thus were difficult to control. But a recent, detailed report by C4ADS, a research firm based in Washington, D.C., which often consults with the U.S. on security issues, buttresses those inside the administration pushing for a harder line with Beijing. It argues that Pyongyang's financing and procurement system for its weapons of mass destruction program

is "centralized, limited and vulnerable—and thus ripe for disruption."

Analysts in both the CIA and the U.S. Treasury Department have been arguing this for years. They note that sanctions in 2005 against a single Macau-based bank—Banco Delta Asia—infuriated Pyongyang because BDA was a linchpin in the laundering of North Korean funds. It was also thought to house some of the money of senior government officials. More than $25 million in funds were frozen, and every international bank that did business with BDA lost access to the U.S. financial system. The BDA sanctions were "the most effective targeted effort we've had," says former Treasury official Stuart Levey. Two years later, Pyongyang demanded that the BDA sanctions be removed as the price of returning to the nuclear negotiating table in the so-called six party talks—also involving China, Russia, Japan and South Korea. The Bush administration relented. The talks went nowhere.

Fast-forward 10 years, and the North is now closer than ever to lobbing a nuke at the United States. Optimists say that date is at best three years away. Pessimists say 18 months. At that point, the U.S. and its allies will face a critical decision: to either treat Kim as a rational nuclear actor, who can be deterred through mutually assured destruction, or assume the opposite—that he's "unpredictable" a description widely used in the U.S. media, though not universally subscribed to by U.S. policymakers)—and think about pre-emption and the disastrous war that could start. Given that, it's no wonder Team Trump is now willing to risk Beijing's ire and go hard after the Chinese companies that enable the North. Says a White House staffer involved in the North Korea deliberations, "What other real choice do we have?"

The Nuclear Option

The Trump administration has yet to publicly identify the 10 key companies it is now pressuring Beijing to deal with, aside from the recently sanctioned Bank of Dandong. Officials say, however, that there is a precedent for what they intend to do. Washington believes there are a handful of so-called gateway firms in China that facilitate trade and financing for North Korea abroad. Last fall, the U.S. Justice Department brought charges—and the Treasury issued sanctions—against one of those companies, the Dandong Hongxiang Industrial Development Co., and its subsidiary, the Liaoning Hongxiang Group. "It's important to understand," the recent report from C4ADS states, "the unique role the [two companies] played in the broader system of China-North Korea trade." According to documents released by the Department of Justice, DHID described itself as "an enterprise that conducts Sino-North Korea import and export." The firm and its affiliated companies were able to satisfy procurement orders for North Korean government organizations and purchase hundreds of millions of dollars of North Korean commodities that it moved through domestic Chinese distribution channels. Those funds, the U.S. believes, were in turn used to finance the purchase of key dual-use components for Kim's nuclear and missile program.

In addition to being a large-scale trading firm on the border of North Korea, DHID also played a likely much more valuable role for North Korea: It served as a front for the sanctioned North Korean financial institution Korea Kwangson Banking Corp. to access the global financial system. Since 2009, KKBC has been barred from accessing the international financial system because of its alleged role in financing some of North Korea's most notorious weapons proliferators. KKBC is a key bank in North. If it doesn't have access to the international financial system, Pyongyang can't pay various foreign suppliers of parts, machinery and equipment for its weapons program. (Those suppliers want dollars, not North Korean won.) Once KKBC was cut off, DHID stepped in. The Justice Department states that "DHID Entities served as financial intermediaries for U.S. dollar transactions between North Korea–based [companies], who were financed by KKBC and suppliers in other countries in order to evade the restrictions on U.S. dollar transactions." Over two separate time periods, the Justice Department alleges DHID did more than $11 million worth of deals on KKBC's behalf.

In order to pull that off, DHID set up front companies and shells all over the world to try to cover its tracks—altogether 43 companies in six countries on four continents. The Justice Department further states that DHID used at least 22 companies to move nearly $75 million through the U.S. financial system. As C4ADS writes, "Far from being isolated" (as the standard trope about North Korea has it), "the scope of the network allowed sanctioned North Korean entities to conduct financial transactions that

would appear to U.S. and European correspondent banks as coming from companies based in the British Virgin Islands, the Seychelles, England, Wales and Hong Kong."

Trump administration officials believe that targeted international action against entities like DHID strike where the North Korean overseas financing system is most vulnerable—at key "chokepoints" where licit and illicit activities converge. Their pressing question is: Why didn't the Obama administration pursue other important Chinese facilitators beyond DHID? That question can probably be answered with another one: How willing was—and is—the U.S. to anger Beijing?

A one-off case against a big Dandong-based holding company such as DHID is one thing. Beijing apparently didn't protest too much when the Treasury issued its sanctions, apparently believing that it needs to show at least some willingness to pressure Pyongyang, even at the expense of one of China's own firms. But several Trump appointees in the national security community are increasingly scathing about the efforts of both the Obama administration and Beijing to hobble Kim's nukes. "As the North continued to make progress [toward an intercontinental ballistic missile capable of delivering a nuke], the U.S. and the U.N. tightened sanctions, it's true," says one Trump official. "But those were sanctions with a big caveat: They didn't much apply to China, at least when China wanted to ignore them." Another Trump official says the Obama team was focused on climate change as the key issue in bilateral relations with Beijing—not North Korea. "At no point was the sanctions regime against North Korea as effective as the sanctions were against Iran before they came to the [nuclear negotiating table]," says one senior Trump official, "and that's almost entirely because of China."

Now, Trump is vowing that equation will change. His administration has assessed that if Beijing proves itself to be unserious by the end-of-summer deadline Washington has set for action, the U.S. must go after the North's Chinese partners itself, cutting off their access to the U.S. financial system if need be.

Beijing, obviously, won't be happy about this; just how unhappy it will be is the critical (and, for the moment, unknowable) question. An increasingly powerful China has many ways to hurt the U.S., including by punishing the American companies selling into the world's second largest economy, as well as by using economic pressure against the two key U.S. allies in the region, South Korea and Japan. But Washington has decided that pressuring Chinese companies is essentially the only option left, short of war on the Korean Peninsula. No one wants that, including Beijing. It "tried" once, Trump tweeted; now, he's giving China one last shot. Tensions in East Asia are as high as they've been since the end of the Korean War. Prepare for them to get worse.

Nuclear Plants – Target for Hackers

Source: http://i-hls.com/archives/77520

July 13 – Since May, hackers have been penetrating the computer networks of companies that operate nuclear power stations and other energy facilities, as well as manufacturing plants in the United States and other countries. Among the companies targeted was the Wolf Creek Nuclear Operating Corporation, which runs a nuclear power plant, according to security consultants and an urgent joint report issued by the Department of Homeland Security and the FBI recently.

The report did not indicate whether the cyberattacks were an attempt at espionage, such as stealing industrial secrets, or part of a plan to cause destruction. There is no indication that hackers were able to jump from their victims' computers into the control systems of the facilities, nor is it clear how many facilities were breached. Wolf Creek officials explained that while they could not comment on cyberattacks or security issues, no "operation systems" had been affected and their corporate network and the internet were separate from the network that runs the plant.

The hackers appeared determined to map out computer networks for future attacks, the report concluded. But investigators have not been able to analyze the malicious "payload" of the hackers' code, which would offer more detail into what they were after. John Keeley, a spokesman for the Nuclear Energy Institute, which works with all 99 electric utilities that operate nuclear plants in the United States, said nuclear facilities are required to report cyberattacks that relate to their "safety, security and

operations." None have reported that the security of their operations was affected by the latest attacks, Mr. Keeley said.

According to the New York Times, in most cases, the attacks targeted people — industrial control engineers who have direct access to systems that, if damaged, could lead to an explosion, fire or a spill of dangerous material. The origins of the hackers are not known, But the report indicated that an "advanced persistent threat" actor was responsible, which is the language security specialists often use to describe hackers backed by governments.

Hackers wrote email messages containing fake résumés for control engineering jobs and sent them to the senior industrial control engineers who maintain broad access to critical industrial control systems, the government report said. The fake résumés were Microsoft Word documents that were laced with malicious code. Once the recipients clicked on those documents, attackers could steal their credentials and proceed to other machines on the network.

Energy, nuclear and critical manufacturing organizations have frequently been targets for sophisticated cyberattacks. The Department of Homeland Security has called cyberattacks on critical infrastructure "one of the most serious national security challenges we must confront."

On May 11, during the attacks, President Trump signed an executive order to strengthen the cybersecurity defenses of federal networks and critical infrastructure. The order required government agencies to work with public companies to mitigate risks and help defend critical infrastructure organizations "at greatest risk of attacks that could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security."

Jon Wellinghoff, the former chairman of the Federal Energy Regulatory Commission, said in a recent interview that while the security of United States' critical infrastructure systems had improved in recent years, they were still vulnerable to advanced hacking attacks, particularly those that use tools stolen from the National Security Agency.

In 2008, an attack called Stuxnet that was designed by the United States and Israel to hit Iran's main nuclear enrichment facility, demonstrated how computer attacks could disrupt and destroy physical infrastructure. The government hackers infiltrated the systems that controlled Iran's nuclear centrifuges and spun them wildly out of control, or stopped them from spinning entirely, destroying a fifth of Iran's centrifuges.

In retrospect, Mr. Wellinghoff said that attack should have foreshadowed the threats the United States would face on its own infrastructure. Critical infrastructure is increasingly controlled by supervisory control and data acquisition systems. They are used by manufacturers, nuclear plant operators and pipeline operators to monitor variables like pressure and flow rates through pipelines. The software also allows operators to monitor and diagnose unexpected problems.

But like any software, these systems are susceptible to hacking and computer viruses. And for years, security specialists have warned that hackers could use remote access to these systems to cause physical destruction.

There were dirty bomb ingredients in ISIS-controlled Mosul

Source: http://www.homelandsecuritynewswire.com/dr20170724-there-were-dirty-bomb-ingredients-in-isiscontrolled-mosul

July 24 – Two years ago, in the summer of 2015, the Washington, D.C.-based Institute for Science and International Security decided to investigate whether DAESH (Islamic State) controlled dangerous radioactive material in Iraq or Syria. The Institute says that the result of a few months of study by Sarah Burkhard, a young scientist, and other staff surprised the Institute's staff. **Their investigations found that there were apparently two sources of radioactive cobalt in Mosul which posed a risk of being used in a radiological dispersal device.**

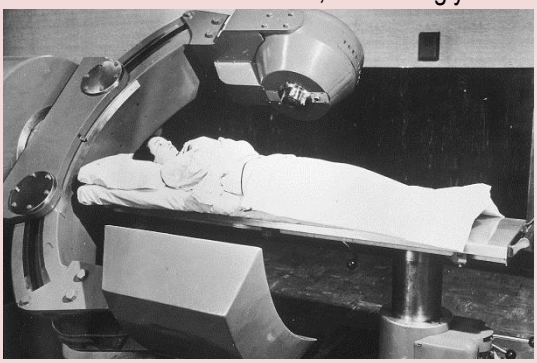
The Institute's researchers could not know whether DAESH was aware of these sources and their potential, or had already taken possession of them. The Institute produced a confidential research study which it used to alert the United States and other friendly governments of the situation as the Institute's researchers knew it. Most of these governments were also monitoring the situation.

At the same time, the Institute decided not to publish any of our results. "As we learned more, we updated our study, which remains a confidential report due to its sensitivity," the researchers say.

The Institute says that it is "very relieved" that these **two, older albeit still dangerous, cobalt 60 sources were not found and used by DAEESH. They were recovered intact recently.** The Institute notes that it is particularly grateful to Joby Warrick at the *Washington Post*, who the researchers had alerted early on for assistance in researching the fate of these sources. "He understood the importance of digging into this story while delaying its publication until the radioactive sources were in safe hands. He and his colleagues at the*Washington Post* recently added greatly to this important story," the Institute says.

Background

DAESH rapidly seized control of the Iraqi city of Mosul in 2014 and inherited with it, unknowingly to the public, **two cobalt 60 teletherapy machines** carrying highly dangerous nuclear material. These machines were procured years ago, in the 1980s or even 1970s, for the treatment of cancer and conducting research.



The Institute's researchers estimated, based on open source information, that the cobalt 60 had decayed considerably but still had a radioactive strength which would place it in the International Atomic Energy Agency's (IAEA's) **category 2** of radioactive sources, described as "very dangerous to the person" (IAEA, "Categorization of Radioactive Sources," Vienna, 2005). In terms of dose strength, the sources could **produce a fatal dose to an individual at a meter from the source within 2-4 hours. For individuals within 0.1 meter distance, it could occur within 2-3 minutes.**

In comparison, a widely publicly discussed radioactive iridium source that went missing in Iraq in late 2015 was also category 2 (the source was later found and secured. See: "Exclusive: Radioactive material stolen in Iraq raises security concerns," Reuters, 17 February 2016). However, the researchers estimated that at least one of the cobalt-60 sources in Mosul had a dose rate roughly twenty times greater than the missing iridium.

Lessons

The Institute says that this case has several lessons for the future, and should serve as a reminder of the risks posed by radioactive sources, many of which are poorly protected or accounted for.

It is not clear why DAESH did not use the cobalt 60 sources to make a radiological dispersal device. The researchers' speculations include that since **the cobalt 60 comes in metal form and not as a powder**, it would be more difficult to use the radioactive cobalt, involving steps that can be very dangerous for unprepared and inexperienced individuals. A more likely possibility is that DAESH did not know about the cobalt 60 sources. **Did courageous hospital and university staff work successfully to keep the existence of the sources secret?**

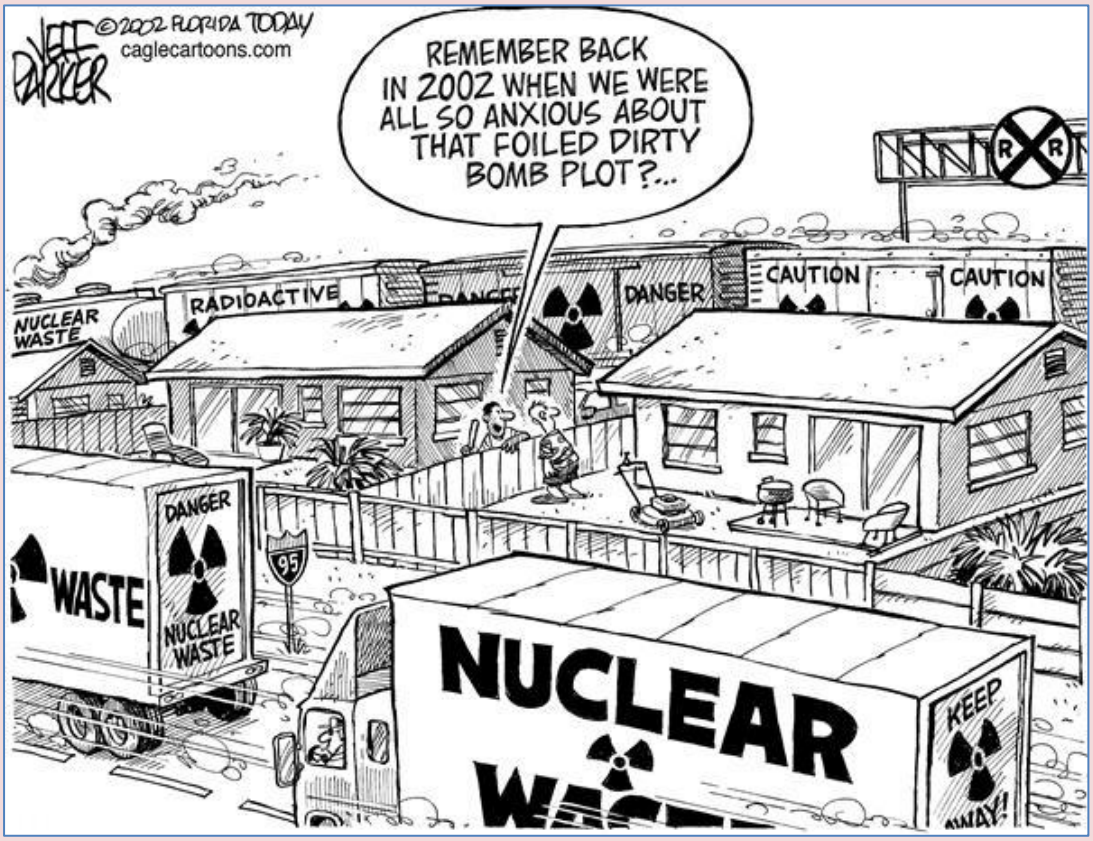
Other potential reasons for the lack of use include

- The sources were judged as not destructive enough for DAESH goals;
- The use of the sources in a radiological dispersal device in the West did not fit the DAESH idea of how they would want to attack the West; Or
- The DAESH leadership was preoccupied elsewhere and did not learn about the sources in Mosul or have a chance to think through the opportunities offered by the cobalt 60 sources.

"Whatever the actual case, we are relieved that these dangerous sources remained intact and were not seized by Daesh. We may not be so fortunate next time. It is important to learn from this near miss and seek improvements to further reduce the chances of a terrorist group misusing radioactive materials," the Institute says.

The Institute says that this case should lead to reinvigorated efforts to inventory and adequately protect radioactive sources throughout the world. However, as this case highlights, improving physical protection may not be enough. It is also important for the United States and its allies to accelerate programs to identify, consolidate, and remove dangerous radioactive sources, particularly in regions of tension or where terrorists are active. "Iraq and other countries in regions of instability and insurgency should receive expedited assistance to remove cobalt 60 sources and receive cobalt-free cancer treatment mechanisms," the Institute concludes.

— Read more in Joby Warrick and Loveday Morris, "How ISIS nearly stumbled on the ingredients for a 'dirty bomb'," Washington Post (22 July 2017).



ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

EXPLOSIVE NEWS

Car bomb kills 30 people outside Afghanistan bank

Source: http://counteriedreport.com/car-bomb-kills-30-people-outside-afghanistan-bank/

June 22 – **At least 30 people were killed** Thursday in a **car bomb** attack outside a bank in Lashkar Gah, the capital of Afghanistan's southern Helmand province, officials said.
In a statement to journalists, Taliban spokesman Qari Yousuf Ahmadi said the group was behind the attack.
A suicide bomber driving an explosive-packed car targeted the New Kabul Bank branch in Lashkar Gah, said Omar Zwak, a spokesman for Helmand province.
"Both civilians and police are among the victims who had gone to the bank to collect their salaries," said Mohammad Karim Atal, the head of the local provincial council.
About 60 others were injured during the blast and were hospitalized, Zwak said.
Helmand province has been the site of intense conflict between the Taliban and Afghan and NATO security forces. Thousands of civilians and soldiers have died in recent years.
The province borders Pakistan and is one of the world's largest producers of opium, which the Taliban harvest to finance their war efforts.
Other car bomb attacks have struck Lashkar Gah.

EDITOR'S COMMENT: 30 dead; 60 injured… Imagine this in a European city! But for Afghanistan is not a big deal – one out of many! I am sure you noticed the wide coverage of this incident (and others alike) by mainstream media and your TV news!

New System to Detect Explosives Traces in Airports

Source: http://i-hls.com/archives/77340

July 01 – US airports security authorities would be able to add another detection system to their arsenal. A new explosives trace detection system has passed certification testing by the US Transportation Security Administration (TSA).

IONSCAN 600, the new model of Smiths Detection, is a next generation, explosives trace detector used to detect and identify the presence of threats invisible to the naked eye. It is used to test surfaces of hands, luggage, packages, clothing, and cargo for explosives. The system also provides operational advantages.
According to businesswire.com, certification testing is the first of three phases in TSA's overall qualification process and is necessary in order to be placed on TSA's Qualified Products List (QPL) for explosives trace detection equipment.
The certification testing represents a milestone for the new model of the Smiths trace detector, which also meets The European Civil Aviation Conference (ECAC) standard for passenger and cargo screening and Civil Aviation Administration of China (CAAC) standard for aviation screening.
Neil Sandhoff, Vice President of Sales and Business Development; Smiths Detection Inc. said: "Regulators need to continuously respond to address emerging threats and work with industry to stay ahead of terrorism. TSA laboratory certification, along with meeting other international regulatory standards for passenger and cargo screening, shows Smiths Detection's continued investment to help protect the traveling public. With this certification IONSCAN 600 is ideally suited for installation at all major airports outside the United States (U.S.) helping them meet the most stringent explosive detection requirements."
Lab certification of detection performance ensures the system meets detection related requirements for systems, which is a prerequisite for deployment at US airports.

Smiths Detection, part of Smiths Group, is a global leader in threat detection and screening technologies for military, air transportation, homeland security and emergency response markets.

Addressing the threat of vehicle-borne IEDs

Source: http://www.homelandsecuritynewswire.com/dr20170703-addressing-the-threat-of-vehicleborne-ieds

July 03 – **In July of 2016, a refrigerator truck packed with explosives detonated next to a crowded apartment block in Baghdad's Karrada neighborhood. The blast killed 323 people and was one of the worst Vehicle–Borne Improvised Explosive Device (VBIED also known as car bombs) attacks ever recorded. On 30 May 2017, a VBIED in a tanker truck ripped through the embassy quarter of Kabul, killing more than 150 people. Several embassies, including those of Germany and France, sustained damage despite the presence of blast protection structures**.

In recent years, several massive VBIEDs (also known as car bombs) have been thwarted by local security forces throughout hotspots in the Middle East and Asia, and by U.S. coalition forces in Afghanistan.

VBIEDs continue to pose a real and evolving threat to even the most secure compounds. S&T says that

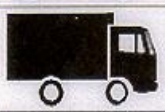
the Explosives Division (EXD) of the Department of Homeland Security's (DHS) Science and Technology Directorate (S&T) has taken measures to address this threat directly.

EXD's Homemade Explosives (HME) program conducts Large–Scale VBIED testing to mitigate the threat posed by massive car bombs and to ensure such attacks do not occur in the United States. This program is part of S&T's Homeland Security Advanced Research Projects Agency.

Recently, S&T EXD conducted a series of explosives tests with varying charge sizes to learn more about mitigating these threats, based on the size and composition of the explosive device. These large-scale explosives tests, conducted at Fort Polk, Louisiana, brought together the HME preparation expertise of the U.S. Naval Surface Warfare Center's (NSWC) Indian Head facility and the live fire testing capability of the U.S. Army Corps of Engineers' Engineering, Research, and Development Center in Vicksburg, Mississippi.

"Due to the wide variety of types of and materials used to make improvised explosives, we often must use simulations to model the behavior of large scale events. When current methods are no longer effective, we have to conduct controlled real-life events to discover new ways of combatting emerging trends in explosives," according to HME Deputy Program Manager Dave Hernandez.

The data from the Fort Polk tests will allow us to understand the damage that different types of HME mixes can inflict. Such information on large-scale detonations could not be accurately calculated before these tests were conducted. This information will facilitate the development of new mitigation techniques for larger-scale explosions. The results of these tests will also be detailed in a report for stakeholders and archived for future reference and distribution by the program office.

ATF	VEHICLE DESCRIPTION	MAXIMUM EXPLOSIVES CAPACITY	LETHAL AIR BLAST RANGE	MINIMUM EVACUATION DISTANCE	FALLING GLASS HAZARD
	COMPACT SEDAN	500 Pounds 227 Kilos *(In Trunk)*	100 Feet 30 Meters	1,500 Feet 457 Meters	1,250 Feet 381 Meters
	FULL SIZE SEDAN	1,000 Pounds 455 Kilos *(In Trunk)*	125 Feet 38 Meters	1,750 Feet 534 Meters	1,750 Feet 534 Meters
	PASSENGER VAN OR CARGO VAN	4,000 Pounds 1,818 Kilos	200 Feet 61 Meters	2,750 Feet 838 Meters	2,750 Feet 838 Meters
	SMALL BOX VAN *(14 FT BOX)*	10,000 Pounds 4,545 Kilos	300 Feet 91 Meters	3,750 Feet 1,143 Meters	3,750 Feet 1,143 Meters
	BOX VAN OR WATER/FUEL TRUCK	30,000 Pounds 13,636 Kilos	450 Feet 137 Meters	6,500 Feet 1,982 Meters	6,500 Feet 1,982 Meters
	SEMI-TRAILER	60,000 Pounds 27,273 Kilos	600 Feet 183 Meters	7,000 Feet 2,134 Meters	7,000 Feet 2,134 Meters

"The S&T HME Characterization program informs the explosives community on current material threats, explosive characteristics, and any potential data enabling mitigation measures such as the development of detection technologies and support those responsible for safety and security in the blast communities in order to prepare for, and prevent, such an attack in the United States", said HME Program Manager Elizabeth Obregon.

"The information generated from this testing will aid the Department of Defense and law enforcement communities by revealing data on the impact of a large–scale VBIED, enabling better protection for vulnerable targets. As the HME threat is constantly changing, a continued effort in this area is required in order to provide timely information to those organizations conducting analysis and acquisitions," Obregon concluded.

S&T notes that, reflecting the DHS "Unity of Effort" goal, these tests included participants from the National Ground Intelligence Center, ERDC, U.S. Navy, Combating Terrorism Technical Support Office, ATF, the Defense Threat Reduction Agency, the Department of State, and other U.S. agencies. The program has also gained visibility within the blast mitigation and effects community as well as the international community.

More rigorous approach to training of explosive-detecting dogs

Source: http://www.homelandsecuritynewswire.com/dr20170703-more-rigorous-approach-to-training-of-explosivedetecting-dogs

July 03 – With a sense of smell much greater than humans, dogs are considered the gold standard for explosive detection in many situations. But that does not mean there is no room for improvement. In a study appearing in the ACS' journal *Analytical Chemistry,*scientists report on a new, more rigorous approach to training dogs and their handlers based on real-time analysis of what canines actually smell when they are exposed to explosive materials.

Explosives are often used in terrorist attacks. Dogs trained to detect odors emanating from TNT, nitroglycerin and other explosives are a crucial part of the first-line defense against these incidents. But delivering low-concentration vapor during training sessions is a challenging task. Cross-contamination of training materials with samples from different explosives can skew results and confuse both dogs and handlers. The ACS says that to address these concerns, Ta-Hsuan Ong and colleagues sought to better understand the components within explosive odors that cue a dog's reaction.

The researchers developed a real-time vapor analysis mass spectrometer to more accurately measure the vapor plumes from explosives that trigger a canine response. In field trials, they used the device and found that some mistakes the dogs made were indeed correct identifications. For example, some "blanks" were used that were ostensibly prepared without explosive material, but the dogs indicated an explosive was present. When the researchers used the mass spectrometer on such blanks, they found evidence of explosive vapors, indicating cross contamination occurred or other interferents were present. Based on these findings, the researchers suggest that use of real-time vapor analysis could help differentiate canine mistakes from cross contamination and other issues during training.

— Read more in Ta-Hsuan Ong et al., "Use of Mass Spectrometric Vapor Analysis to Improve Canine Explosive Detection Efficiency," Analytical Chemistry 89, no. 12 (9 June 2017): 6482-90.

Elton John bomb plotter Haroon Syed jailed for life

Source: http://www.bbc.com/news/uk-40481325

July 03 – A 19-year-old man has been jailed for life for planning a bomb attack that may have targeted an Elton John concert or Oxford Street in central London.

Haroon Syed, of west London, admitted preparing acts of terrorism after trying to source weapons including a suicide bomb and machine gun.

He was caught after approaching MI5 officers, who were posing as a fellow extremist, via social media.

Syed was sentenced to a minimum of 16 years and six months.
Last year, his brother was jailed for life for plotting to behead someone on Remembrance Sunday.
Judge Michael Topolski QC said Syed wanted to carry out "an act of mass murder" and therefore a discretionary life sentence was warranted.

'Do martyrdom'

Prosecutors say Syed's plans ranged from becoming a suicide bomber to staging a gun attack, and while he initially boasted of working with others, those people did not materialise.
Instead, over the summer of last year, he made increasingly urgent efforts to secure weaponry.
After he went online looking for help, a purported jihadist fighting overseas, known only as Abu Isa, introduced him to another extremist going by the name Abu Yusuf.
This second man was, in fact, a group of MI5 officers who were playing the role of a jihadist in what became weeks of social media chat with Syed.
Duncan Penny QC, prosecuting, told the Old Bailey there was initially some "suspicion on both sides" before Abu Yusuf concluded that Syed was a "committed brother" he could deal with.
Syed then began talking about his aspirations and gave his contact a shopping list, saying he wanted "do martyrdom" after first causing "damage" with a machine gun.
"Can you get the gear?" asked Syed. "You will be involved right?
"Two things. Number one, machine gun and we need someone who can make a vest you know the dugma [button] one. So after some damage with machine gun then do itishadi [martyrdom] ... that's what I'm planning to do."
The undercover officer told Syed guns were expensive - but he might be able to get someone to build a bomb. Syed floated the idea of going to fight overseas with his new-found friend - but revealed his passport had been cancelled by the authorities.
He tried and failed twice to get fraudulent loans of thousands of pounds to cover the cost of firearms - and eventually agreed to meet his contact in a coffee shop in Slough, Berkshire, to finalise an alternative plan.
Over two meetings, he talked about his aspirations and then handed over £150, asking for a bomb packed with nails. The conversation was secretly recorded.
"I was thinking of Oxford Street," he told his contact. "If you put those things inside called nails, do you know what that is, nails? Those sharp things - lots of them inside.
"Good man, can't wait akhi [brother]. If I go to prison, I go to prison. If I die, I die, you understand? I have got to get to Jannah [heaven]."
The undercover officer later told Syed a "bomb-making brother" would have the device ready within days - and the suspect went online to narrow his list of targets.
His web searches included "packed places in London" and "Elton John, Hyde Park, 11 September" - a major concert hosted by BBC Radio 2 which also featured Status Quo and Madness.

'ISIS' password

Prosecutors say Syed's character had begun to change outwardly in late 2014, coinciding with the growing support among British extremists for the self-styled Islamic State group.
During the course of the investigation, detectives found his web searches jumped about as he tried to satisfy himself that an attack on civilians was theologically justifiable.
One of his last searches, a week before his arrest, was: "How can I stop being upset about the UK killing innocent Syrians and get on with my day?"
When counter-terrorist detectives arrested him in September and asked him for the password for his phone, he replied: "ISIS - you like that?"
Syed's was one of 18 terror plots to have been foiled since 2013.
Mitigating, Mark Summers QC said it was a "crude, ill-thought-out" plan made at the behest of others.

The court heard Syed had fallen under the influence of members of banned extremist group Al-Muhajiroun, and that he now publicly rejected his past beliefs and condemned the recent bomb attack in Manchester.
But Judge Topolski told Syed: "You were not lured, you were not enticed, you were not entrapped.
"You became, and in my judgement as shown by your online activities away from your contact with Abu Yusuf, deeply committed to the ideology of a brutal and barbaric organisation that sought to hijack and corrupt an ancient and venerable religion for its own purposes and you wanted to be part of it."
Deb Walsh, deputy head of the counter-terrorism division of the Crown Prosecution Service, said: "Haroon Syed is clearly a danger to the public who was prepared to carry out indiscriminate attacks against innocent people.
"The compelling evidence presented by the CPS left him with no choice but to plead guilty."

Taliban targets children with 'toy bomb' killing six boys in Pakistan

Source: http://www.ibtimes.co.uk/taliban-targets-children-toy-bomb-killing-six-boys-pakistan-1627741

July 07 – **Dozens of children in Pakistan have died while playing seemingly harmless toys found on the street.**
A bomb that resembled a toy has killed at least six children and wounded another two in northwestern Pakistan on Sunday (25 June), an official has said.

The children were playing alongside a road in Sararogha area, in the province of South Waziristan, when they found the explosive device, Mohammad Shoaib Khan, a government official, was quoted by AP as saying. He added the two wounded children were in critical condition.
A local government official who spoke to AFP on condition of anonymity said the children were aged "between six to 12 years" and they were "all boys".
The incident occurred one day after two other children were killed after stepping on a land mine in the Spin Toot area.
Dozens of children in Pakistan – particularly in the country's northwest – have died in the past after they picked up seemingly harmless toys that then exploded in their hands and face.
In 2015, a father and two of his children were killed in Swat, an area in the Khyber Pakhtunkhwa Province , after bringing home a bomb concealed as a toy they had found on the street, local media said.

The previous year, two children were killed when a toy bomb exploded in Landi kotalTehsil, in the tribal area of Khyber Agency.

Soviet-era butterfly bombs were designed to intentially look like toys to target children

The origins of the "toy" bomb that exploded on Sunday are not clear.
South Waziristan harboured the Pakistani Taliban, a Sunni Islam militant organisation, until 2009, when the army launched a majour offensive retaking some areas previously controlled by the terrorists.

However, the Taliban still carries out attacks in the country. In one of its deadliest raids in recent years, the group killed at least 141 people – including 132 children, when it stormed a school in Peshawar,capital of the Khyber Pakhtunkhwa province, in 2014.
In response to the attack, Pakistan announced it would lift a six-year-moratorium on the death penalty in order to curb terrorism in the country, in a move condemned by rights groups.

A floating tunnel could withstand an explosion

Source: http://www.homelandsecuritynewswire.com/dr20170710-a-floating-tunnel-could-withstand-an-explosion

July 10 – Concrete can tolerate much more force that previously believed, which could open the door to a new kind of road structure: a floating tunnel. The E39 is a nearly 1100-km long coastal road that crosses seven major fjords by use of ferries. Norwegian authorities are working to improve the road by eliminating ferry crossings, which in addition to being costly, mean that drivers have to wait for ferries if they don't arrive at the crossing at exactly the right time. Norwegian engineers are examining an entirely new type of water crossing: submerged floating tunnels.

Chilling picture shows female Isil fighter holding child moments before detonating suicide vest

Source: http://www.telegraph.co.uk/news/2017/07/08/chilling-picture-shows-female-isil-fighter-holding-child-moments/

July 10 – At first sight the picture appears to show a mother cradling her young child as she flees an Islamic State-held area of Mosul.


But a closer look reveals she is holding a trigger, which she will pull seconds later.
An Iraqi TV station captured the moment before a suspected female Islamic State of Iraq and the Levant (Isil) suicide bomber blew herself - and the baby - up near Iraqi troops.

tried to detonate an explosives vest hidden under her hijab as she passed the soldiers, but it failed to go off until she had walked some distance away, a cameraman for al-Mawsleya TV said.
She was killed along with her child, while two soldiers and several civilians were injured.
The station had been filming the battle between Iraqi troops and Isil fighters and did not realise what they had caught on camera until they reviewed their footage later.
Isil is cornered in a tiny square of the historic Old City, which the army said could be liberated by the end of the day.
"We are seeing now the last metres and then final victory will be announced," a host of Iraqi state TV said on Saturday, citing the channel's correspondents embedded with security forces battling in Isil's redoubt in the Old City, by the Tigris river. "It's a matter of hours," she said.
The jihadists have used everything in their arsenal to fend off the troops in the final throes of the nine month-long offensive.
Isil's use of female suicide bombers in battle, while not new, is exceedingly rare and demonstrates the group's desperation.
More than 20 female suicide bombers hiding among civilians are believed to have detonated explosives in the last two weeks.
"We are seeing now the last metres and then final victory will be announced," a host of Iraqi state TV said on Saturday, citing the channel's correspondents embedded with security forces battling in Isil's redoubt in the Old City, by the Tigris river. "It's a matter of hours," she said.
The jihadists have used everything in their arsenal to fend off the troops in the final throes of the nine month-long offensive.
Isil's use of female suicide bombers in battle, while not new, is exceedingly rare and demonstrates the group's desperation.
More than 20 female suicide bombers hiding among civilians are believed to have detonated explosives in the last two weeks.

Isil's so-called "jihadist brides" typically stay at home and look after the children, but experts say women are becoming more active, wishing to also take part in jihad on a par with men.
During a recent visit to Mosul, civilians told the Telegraph that the women Isil members were as brutal as the men.
"I was more afraid of the women fighters than the men, they were like wild animals," said Umm Omar.
She said women in Isil served as hisba, or morality, officers and would ensure females living in the so-called caliphate adhered to the jihadists' strict dress code. She claimed many were whipped for minor infractions.

EDITOR'S COMMENT: I would like to believe that this woman just grabbed an orphan child – one out of hundrends and conducted the bombing. Even in war zones, the identity of a mother is too valuable and precious to be awarded to an insane fanatic criminal. A suicide woman bomber might be justified if detonated in the middle of a group of enemies (that might have killed her husband or children or brothers and sisters) – something like an eye for an eye or many eyes. But a woman with a child? NEVER – go to hell womanoid!

Announcing the ExploDrone, the First and Only Available Drone IED Simulator and Test Training Aid, Released by Explotrain LLC

Source: http://www.businesswire.com/news/home/20170711006336/en/

July 11 – Explotrain® LLC, a Florida based small business, is taking the defensive response to the emerging drone threat straight to the troops through their development of a realistic drone based IED simulation and training system. With the first and only functional drone and simulated IED integrated device, Explotrain is addressing the vital and emerging threat of drone weapons in theatre.
Asymmetric warfare by its very nature leads combatants on all sides to develop new weapons and defenses. The latest emerging threat in current conflicts is the use of sUAVs or drones as a method, not of reconnaissance, but delivering and deploying weapons in the form of explosives. The drone based IED delivery systems seen most recently in Syria, Iraq, and Afghanistan are just the latest step in the evolution of the improvised explosives threat.

While the US military is exploring multiple counter drone technologies, from electronic signal jamming and interception to laser based disabling systems, Explotrain has created the first and only drone based IED simulation system to be used in live training, testing and evaluation. As the recognized leader in products currently used for training against the conventional IED threat, Explotrain is using their patented technologies to accurately simulate IEDs delivered by drones and other Small Unmanned Aerial Systems (sUAVs).
"A key challenge in developing, testing and validating the current crop of counter-unmanned aerial systems (cUAS) is a lack of true simulators," said

Mr. Michael Hopmeier, a world recognized expert on cUAS system strategy and technology. "Faked YouTube videos and staged tests are entertaining, but they are what lead to so many casualties from IEDs just a decade ago."

Working in conjunction with military, law enforcement and business partners, Explotrain's new ExploDrone™ system is able to accurately simulate the two main types of attacks carried out by enemy drones. Lightweight pneumatic based Explosive Blast Simulators are carried by larger drones and are used to simulate attacks wherein the drone itself is used as an explosive device, akin to the Japanese kamikaze pilots of WWII. However, unlike their real world counterpart, these training drones and simulators can be reused indefinitely to save training costs. Additionally, smaller drones are used that carry simulations of the repurposed military and improvised munitions that are being dropped onto personnel, vehicles, or other military targets. These simulated munitions are interfaced with Explosive Blast Simulators prepositioned in or on the target area to create the realistic effects so necessary to providing psychologically effective training to ground troops.

One of Explotrain's partner companies, Inert Products, specializes in the rapid development and reproduction of ordnance and munitions and is capable of providing the wide array of Inert Dropped Aerial Munitions (IDAM™s) that troops and law enforcement are likely to face. By using these and other advancements in rapid manufacturing technologies, Explotrain and its partners are able to reduce costs while providing the rapid response to emerging threats now needed.

These advancements are used not only in training scenarios but also as a means of testing and evaluating new tactics and technologies without the risks and expenses of using them against a live threat.

Four Female Suicide Bombers Kill 15 in Nigeria

Source: https://english.aawsat.com/asharq-al-awsat-english/world-news/four-female-suicide-bombers-kill-15-nigeria

July 12 – **At least 15 people were killed when four female suicide bombers detonated their explosives in Maiduguri, northeast Nigeria**, police said on Wednesday, in the latest violence to hit the strategic city.

Borno state police commissioner Damian Chukwu told reporters the four struck in the suburb of Molai Kalemari on Tuesday night and that most of the victims were civilian militia manning security posts.

"The bombers detonated IEDs (improvised explosive devices) strapped to their bodies at different locations of the area, killing 19 people, including the bombers," he said.

"A total of 23 people were injured."

Bello Danbatta, a spokesman for the Civilian Joint Task Force (JTF) militia and chief security officer at the Borno State Emergency Management Agency (SEMA), said it appeared his men were the targets.

Two of the bombers blew themselves up at checkpoints manned by militia members, who assist the military with security and sometimes accompany soldiers on operations against Boko Haram extremists.

"In all we lost 12 of our gallant JTF," he said.

He added: "Civilian JTF have sacrificed their lives to protect their people and the life and property of the citizens of Borno state.

SEMA operatives in face-masks and white overalls were on Wednesday seen removing body parts from the scene of the attacks. Victims were covered with rugs awaiting burial, as local people looked on.

Suicide bombings have become a feature of Boko Haram's eight-year insurgency in northeast Nigeria, which has killed at least 20,000 people and made more than 2.6 million others homeless.
Nine people were killed in a string of suicide bomb attacks in the city last month around the Eid al-Fitr holiday marking the end of the Muslim holy month of Ramadan.
The University of Maiduguri, which lies on the edge of the city, has become a frequent target since the start of the year, as it teaches the "western" education despised by an affiliate to terror group, ISIS.
Nigeria's military and government maintain the group is a spent force and on the verge of defeat as a result of sustained counter-insurgency operations since early 2015.
But sporadic fighting still occurs, while mines and blasts remain a constant threat.

Large–Scale Vehicle–Borne Improvised Explosive Device Testing

Source: https://newswise.com/articles/large-scale-vehicle-borne-improvised-explosive-device-testing

June 29 – In July of 2016, a refrigerator truck packed with explosives detonated next to a crowded apartment block in Baghdad's Karrada neighborhood. The blast killed 323 people and was one of the worst Vehicle–Borne Improvised Explosive Device (VBIED also known as car bombs) attacks ever recorded. On May 30, 2017, a VBIED in a tanker truck ripped through the embassy quarter of Kabul, killing more than 150 people. Several embassies, including those of Germany and France, sustained damage despite the presence of blast protection structures.
In recent years, several massive VBIEDs (also known as car bombs) have been thwarted by local security forces throughout hotspots in the Middle East and Asia, and by U.S. coalition forces in Afghanistan.
VBIEDs continue to pose a real and evolving threat to even the most secure compounds. The Explosives Division (EXD) of the Department of Homeland Security's (DHS) Science and Technology Directorate (S&T) has taken measures to address this threat directly.
EXD's Homemade Explosives (HME) program conducts Large–Scale VBIED testing to mitigate the threat posed by massive car bombs and to ensure such attacks do not occur in the U.S. This program is part of S&T's Homeland Security Advanced Research Projects Agency.

Recently, S&T EXD conducted a series of explosives tests with varying charge sizes to learn more about mitigating these threats, based on the size and composition of the explosive device. These large-scale explosives tests, conducted at Fort Polk, Louisiana, brought together the HME preparation expertise of the U.S. Naval Surface Warfare Center's (NSWC) Indian Head facility and the live fire testing capability of the U.S. Army Corps of Engineers' Engineering, Research, and Development Center in Vicksburg, Mississippi.

"Due to the wide variety of types of and materials used to make improvised explosives, we often must use simulations to model the behavior of large scale events. When current methods are no longer effective, we have to conduct controlled real-life events to discover new ways of combatting emerging trends in explosives," according to HME Deputy Program Manager Dave Hernandez.

The data from the Fort Polk tests will allow us to understand the damage that different types of HME mixes can inflict. Such information on large-scale detonations could not be accurately calculated before these tests were conducted. This information will facilitate the development of new mitigation techniques for larger-scale explosions. The results of these tests will also be detailed in a report for stakeholders and archived for future reference and distribution by the program office.

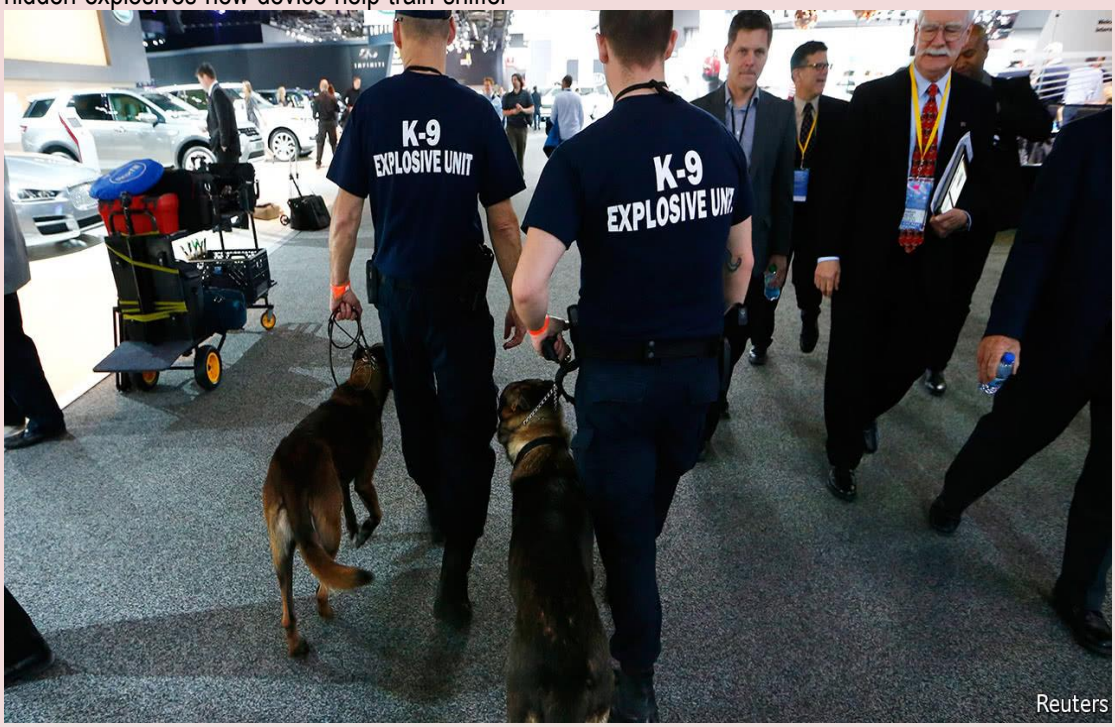
"The S&T HME Characterization program informs the explosives community on current material threats, explosive characteristics, and any potential data enabling mitigation measures such as the development of detection technologies and support those responsible for safety and security in the blast communities in order to prepare for, and prevent, such an attack in the United States", said HME Program Manager Elizabeth Obregon.

"The information generated from this testing will aid the Department of Defense and law enforcement communities by revealing data on the impact of a large–scale VBIED, enabling better protection for vulnerable targets. As the HME threat is constantly changing, a continued effort in this area is required in order to provide timely information to those organizations conducting analysis and acquisitions," Obregon concluded.

Reflecting the DHS "Unity of Effort" goal, these tests included participants from the National Ground Intelligence Center, ERDC, U.S. Navy, Combating Terrorism Technical Support Office, ATF, the Defense Threat Reduction Agency, the Department of State, and other U.S. agencies. The program has also gained visibility within the blast mitigation and effects community as well as the international community.

A new device to help train sniffer dogs

Source: https://www.economist.com/news/science-and-technology/21724798-honing-hounds-find-hidden-explosives-new-device-help-train-sniffer



July 06 – When it comes to finding hidden explosives, the self-propelled detection system known as a sniffer dog has no equal. But sniffer dogs have to be trained, and that is a delicate process. In particular, the trace levels of explosive vapour involved are so low (because dogs' noses are so sensitive) that accidental contamination of supposedly residue-free "control" samples is a serious possibility. That confuses the animal and slows down its training. Things would therefore go more smoothly if a trainer could find out instantly whether a sample had indeed been compromised by traces of explosive, so that he could tell whether a dog's reaction to a supposed blank was justified.

This is no theoretical risk. When Ta-Hsuan Ong of the Massachusetts Institute of Technology monitored one such training session he found that six out of 68 controls were

contaminated—and that one out of 28 supposedly "live" samples had no explosive residue. Dr Ong thinks, however, that he has a solution to the problem. The monitoring device he and his colleagues built for their experiment, the details of which they have just reported in *Analytical Chemistry*, lets handlers check instantly whether an apparent mistake by a dog

is a real one. That will both speed the process of training and, if deployed in the field, permit a suspicious object which a dog has nosed out to be double-checked by technology, and to have its precise explosive characteristics logged instantly.

Dr Ong's invention is a type of mass spectrometer—a device that, by measuring the flight time of ions (electrically charged molecules) in an electric field, is able to work out their mass and therefore their probable composition. A conventional mass spectrometer depends on samples being collected, concentrated and deliberately fed into it, but that would not be a practical way to provide the instant feedback needed for dog training. Dr Ong required something that could pick up chemical compounds directly from the air around a suspicious object.

Sniffers that can detect explosive vapours do, of course, exist. They are used in places like airports. But they are not as sensitive as dogs' noses. Instead, Dr Ong turned to what is known as electrospray ionisation technology (EIT). Commercial EIT works by applying a high voltage to a reservoir of solvent containing compounds of interest. This both sprays the liquid into the air, creating an aerosol, and ionises the molecules within. An adjacent spectrometer then sucks in the aerosol and conducts an analysis. Dr Ong and his team adapted that approach by using pure solvent and aiming the charged aerosol droplets directly at an air stream being pulled into a spectrometer. This ionises the compounds within the air stream, including any derived from explosives, before they enter the device.

The spectrometer the researchers used was set up to sound the alarm if one or more of nine explosive-related materials, such as nitroglycerine, cyclohexanone and triacetone triperoxide, turned up. When tested, it proved able to detect those compounds in concentrations as low as parts per quadrillion—the same sensitivity as a dog's nose. As the trial showed, it was able to confirm dogs' opinions about a sample when those opinions were at variance with the ones held by a human handler.

In principle, once turned into a robust product, Dr Ong's invention might replace the canine variety of

detector altogether. In practice, though, that is unlikely to happen. The mobility and tenacity of a dog give it qualities that a piece of hand-held equipment is never going to replicate. And when it comes to searching people, at least, it is hard to beat a tail-wagging quadruped for user-friendliness.

Bomb alert! How Delhi airport security failed to detect 'explosives' in a bag

Source: http://www.hindustantimes.com/delhi-news/bomb-in-bag-goes-undetected-at-delhi-airport-during-drill-cisf-under-scanner/story-WCtOIwZUkhQVQL1dUQfdhL.html

July 14 – A bag with a 'bomb' has gone undetected through Delhi airport security checks. Luckily, it was only part of a drill to check arrangements at the airport — a test that the CISF personnel flunked.

The Bureau for Civil Aviation Security (BCAS) conducted dummy checks at Delhi, Pune and few other airports over the past three months. In a drill conducted in April, CISF officials failed in the security drill.

Parts of an improvised explosive device were put in a hand bag without a detonator, and civil aviation officials made an easy entry to the Delhi airport with it. Security checks conducted on hand baggage for an Air India flight to Jammu also failed to detect the explosive.

It was only then that the CISF, which is responsible for airport security, was informed that it had failed the test. The CISF checks only hand baggage of passengers with the help of scanners after check-in.

"To ensure that security at airports is at its best and personnel are well aware, we keep conducting dummy checks to know the level of alertness. In April, a drill was conducted where components of improvised explosive device were kept in a bag by a BCAS official. The CISF missed it," said a civil aviation official.

"We have prepared a report listing incidents where CISF failed to notice components of IED in the bag. We keep wires, some explosives and some other parts in bags," the official said.

The CISF said they take action against the staff who fail to perform their duty, and give them security training so that they can identify suspicious objects during scanning.

"Though, we take action against our staff, the BCAS conduct

dummy checks by keeping random items related with making a bomb. Sometimes, it is without a detonator, making it all the more difficult to detect. In some cases, we have even suspended the staff," a CISF official said.

For better concentration, the CISF personnel also rotate baggage screener every hour.

"We have an in-built software through which we throw random images of bomb, knives and other prohibited items and if our staff fail to detect it, we take action against them. This also helps us keep them alert," the official added.

It could take more than a decade to clear Mosul of explosives

Source: https://www.washingtonpost.com/news/checkpoint/wp/2017/07/13/it-could-take-more-than-a-decade-to-clear-mosul-of-unexploded-munitions-and-booby-traps/

July 13 – After nine months of vicious street-to-street fighting to drive the Islamic State out of Mosul, it could take many years more to fully remove explosives and other munitions from one of Iraq's most populous cities, U.S. State Department officials said.

"When I look around the world in some ways there's nothing like Mosul that we've encountered." said Stanley Brown, the director of State's Office of Weapons Removal and Abatement. "The level of contamination though is not one of those where we're talking weeks and months, we're talking years and maybe decades."

Over three years of occupation, the Islamic State mined and booby-trapped large sections of Mosul. Heavy combat has also littered the city with unexploded ordnance such as artillery shells and hand grenades. In the western reaches of the city, where the fighting was especially fierce, massive debris fields will need to be removed to clear the ground beneath.

Pehr Lodhammar, the senior program manager for the United Nations Mine Action Service, or UNMAS, in Iraq said that the State Department's clearance estimate could be accurate, but added that his team is still assessing explosive contamination levels in western Mosul.

"It's hard to grasp the scope," he said.

The Islamic State's grip on the city, which began in the summer of 2014, allowed the militants to experiment with, refine and even industrialize their improvised explosive devices, or IEDs. While the explosives in the weapons are fairly basic, their **triggering devices are some of the most complex de-miners have ever seen, according to U.S. and U.N. officials.** They often involve multiple anti-tampering mechanisms and triggers that are

undetectable to metal detectors, the officials said.

In addition to booby traps, the tens of thousands of rounds of explosive ammunition fired by Iraqi and U.S.-led coalition forces are estimated to have had a roughly 10 percent failure rate, said Lodhammar, adding that the Islamic State, with its home-built munitions, had an even higher failure rate. All of that material will have to be disposed of and destroyed.

"It sounds like a nightmare problem for bomb disposal technicians," said John Ismay, a former Navy Explosive Ordnance Disposal officer who is now a senior crisis adviser at Amnesty International.

"The hazard won't be gone until every last bit of rubble is cleared away," he added.

Solomon Black, a program manager at the Office of Weapons Removal and Abatement, said the amount of explosives remaining in Mosul is "incomparable to anywhere else we've encountered in Iraq." He added that Iraqis on the ground have said that many of the explosive devices have been planted around key infrastructure in the city, 90 percent of which is damaged, adding to the difficulty of clearance.

"They want to keep the water from running, they want to keep the lights out and they want to keep people from coming back to their homes," Black said of the Islamic State. Both U.S. and U.N. efforts are concentrated on demining areas with water treatment, power plants and other critical infrastructure in a bid to restore some semblance of normalcy in the city.

Mosul had a prewar population of nearly 2 million, but tens of thousands of residents have died or fled from the fighting and will have to navigate the risks from unexploded munitions when they return home.

Both the U.N.'s Mine Action Service and the State Department have dedicated significant resources to warning civilians about the dangers of unexploded munitions and booby traps. At entry points into Mosul, the U.N. is handing out leaflets for residents returning to their homes and holding classes at some of the refugee camps on the city's outskirts.

"They turned our house into a weapon against the army," said a young woman in east Mosul who gave her name as Qammar. "I grew up in that home. They turned something so beautiful into something so ugly. It makes me cry when I think about it."

Islamic State booby traps have been found in vacuum cleaners, couches, ovens and other everyday items, officials said.

Residents evacuated from several of Mosul's western districts also said this week that the militants had also mined the road residents had tried to flee along. For 23-year-old Muhammed Nabila that meant watching from the window as his cousin died testing the route.

"The explosion seemed to come out of nowhere," he recounted. "He lost both his legs at the side of the

road. No one was allowed to recover his body for days."

A lack of enough trained personnel and resources remains one of the biggest impediments to clearance operations. Iraqis working with U.S. and European contractors will have to be taught how to handle some of the more sophisticated booby traps; Iraqi forces have already suffered significant casualties from mine clearing.

David Johnson, vice president for strategic development at Janus Global, a State Department contractor that provides mine-clearing services in Iraq and Syria, said that **$100 to $200 million will likely cover the cost of clearance around key infrastructure in Mosul, but more will be needed to clear the entire city.**

"If you look at the fact that we're still cleaning up unexploded ordnance in Southeast Asia and we've been there 20-plus years; in Afghanistan our program started in the 1988-1989 time frame and there's still a lot of work to do," Brown said. "We're talking years, if not over a decade to get everything done."

What is PETN? What you need to know about the explosive found in UP assembly

Source: http://www.dnaindia.com/india/report-what-is-petn-what-you-need-to-know-about-the-explosive-found-in-up-assembly-2502182

July 16 – The PETN explosive found lying under the seat of a Samajwadi Party MLA inside the UP Assembly is one of the most dangerous plastic explosives available in the black market and preferred by

militants as the colourless crystals easily surpass security checks.

The packet, which weighed around 150 g, was found close to the seat of Leader of the Opposition Ram Govind Chaudhary, which is close to the podium where the Speaker sits.

"This is PETN (Pentaerythritol Tetranitrate), this is a dangerous substance," Chief Minister Yogi Adityanath told a stunned House soon after it assembled for the day.

"As informed by experts, 500 gm of this explosive is enough to blow up the House," he said.

PETN is one of the most dangerous plastic explosives which is available in black market, and belongs to the same family as nitroglycerin.

It is preferred by militant groups because it cannot be easily detected owing to its colourless crystals. Majority of explosive detectors use metal detectors, but PETN can be kept hidden in a sealed container or an electrical equipment and thus can easily surpass security checks.

"The dog squad failed to detect the explosive that was found by the cleaning staff on July 12," the chief minister said.

Several countries have severe restrictions on purchase of PETN which can be bought in powder form or thin plastic sheet.
The substance is legally used by the military and in mining industries where it is used in detonators for detonating cords and mines. PETN can be mixed with other chemicals to form Semtex.

PETN before crystallization from acetone (WikiMedia Commons)

Experts say PETN does not go off on its own. The explosive needs a secondary detonating mechanism to produce heat or a shockwave, which can detonate the explosive. The substance is stable and safe to handle, but requires a primary explosive to detonate it.
PETN substance has been used in number of bombing incidents over the years.
Apart from reports of PETN explosives from all around the world, the substance is believed to have been used in the 2011 Delhi High Court blast, in which at least 17 people lost their lives.

How lawmakers reacted to the explosive

Taking note into the issue of a suspicious white powder packet found in the State Assembly, Uttar Pradesh Minister Shrikant Sharma on Friday said the entire state stands together against terrorism and forces planning such activities will never be successful in their plans.
'The entire matter has been handed over to the NIA, so that the probe could be done properly. The entire country stands united against terrorism and such forces will never be successful in carrying out any such activity in Uttar Pradesh,' Sharma told ANI.
He said whatever decision will be taken by the speaker to ensure security in the Assembly, every member is committed to follow it.
Meanwhile, Bahujan Samaj Party (BSP) leader Mukhtar Ansari referred the incident as very crucial and expressed confidence that the accused will be revealed soon.
'I am sure the matter will be solved because the footage of the entire incident is available in the CCTV camera. Attempt like this has taken place earlier also against me and because of that I am suspecting that a psycho person can take any step,' he said.
Earlier, Uttar Pradesh Chief Minister Yogi Adityanath sought for a National Investigative Agency (NIA) probe into the matter.
Adityanath, while confirming that an explosive, by the name of Pentaerythritol tetranitrate (PETN), was indeed found in the Assembly, pressed for more vigilance in Uttar Pradesh, more particularly in the Assembly and rued the absence of a Quick Response Team (QRT) for the state.

"The packet of the explosive was found under the chair of the Opposition's leader. It was 150 gm of PETN. 500 gm of PETN is enough to blow the whole Assembly off. This shows the severity of the situation. I suggest that everybody present in the Assembly should be investigated by the police and that the NIA should investigate into the matter," he said.
"It's unfortunate that the largest Assembly of the country doesn't have a QRT," he added.
Adityanath also said that this incident could be in connivance with a terrorist or militant group and that the security of the state and the country is paramount.
Aditynath also urged the officials to not compromise on the security of the state and the nation, more so considering the current situation of the country.
Supporting the Chief Minister's assertions, Speaker Mata Prasad Pandey said that the whole Assembly is like a family and that the security cannot be compromised.
He also apprised the members about the new security arrangements in the Assembly.
"There will be a Pradeshik Armed Constabulary (PAC) team at every gate of the Assembly. There will also be a full body scanner at every gate. Moreover, a QRT will also be deployed," he said.

A Syrian Father's Mission To Clear ISIS Mines Is Cut Short

Source: https://www.worldcrunch.com/world-affairs/a-syrian-father39s-mission-to-clear-isis-mines-is-cut-short

July 18 – **Abu al Fadl** devoted the final months of his life to clearing al-Bab of improvised explosives left behind by ISIS in everything from washing machines to cooking pots. **The 60-year-old disabled several thousand mines before one took his life.** As a volunteer land mine removal expert in Aleppo's countryside, he felt his life would end every time he discovered an explosive device. **After destroying nearly 3,500 explosives,** al-Na'sani, known as Abu al-Fadl, was killed on May 8 while taking apart a land mine left by the so-called Islamic State, or ISIS.

In April, just days before he was killed, Abu al-Fadl spoke to Syria Deeply about his work dismantling explosives in al-Bab, a former militant stronghold in the eastern Aleppo countryside, where **an estimated 15,000 land mines are believed to have been left by ISIS fighters.**
The 60-year-old father of five, who lost two of his children during the war, used to teach at the military academy in Aleppo and specialized in explosives.
When he set out on his own to defuse land mines, he noted that much of his work focused on understanding the creative methods used by ISIS to make and hide their bombs, which are often disguised as rocks or propane tanks.
"I have found explosive devices hidden inside washing machines, in vacuum cleaners, under couches and in bathrooms," he told Syria Deeply. By placing explosives in residential areas, he said, ISIS is intentionally targeting civilians.
"The majority of victims of these devices are children," he said.
Earlier this year, Abu al-Fadl was injured by an ISIS land mine in Akhtarin in northeastern, rural Aleppo. Nearly 20 pieces of shrapnel penetrated his body and he suffered severe burns to parts of his face. The

explosive also hit Ahmad, a 12-year-old boy who suffered serious injuries to his abdomen, arm and leg. Abu al-Fadl said it was a was a miracle that he survived the explosion.

Hundreds of people are killed by land mines in Syria each year, in a crisis that is only getting worse. The International Campaign to Ban Landmines reported that 864 people were killed in Syria by land mines and other explosives in 2015 alone. Since then, the number has increased significantly, because ISIS made a point of littering the territories it lost with land mines and other explosive devices before withdrawing. Explosives were a "major protection concern" in 88% of subdistricts surveyed in Syria, according to the 2017 Protection Needs Overview published by the UN.

Demining former ISIS strongholds, however, is not an easy task, Abu al-Fadl said. ISIS has used mines as a way to continue terrorizing a population even after it has been pushed out of the area. Engineering teams embedded within Turkey's Euphrates Shield Operation have defused more than 5,000 land mines in territories formerly held by ISIS, according to a statement released in April by the chief of general staff in Turkey, which added that the majority of explosive devices found in al-Bab were anti-tank and anti-personnel mines "placed in the streets or hidden inside residential buildings."

The Syrian Democratic Forces, an alliance of Kurdish and Arab combatants fighting ISIS, also contribute by deploying specialized demining teams to areas they liberate from militants.

Every minute of delay results in a higher number of victims.

In al-Bab, where Turkey-backed rebels pushed ISIS out in February, the militant group used **tactics such as putting two mines on top of each other, to double the impact and ensure that even if one was found and deactivated, the other would still explode.** Other devices, including ones with plastic explosives, are very hard for machines to discover.

Syrians are dependent on volunteers like Abu al-Fadl because organizations working on the ground in northern Syria do not have the resources or the capacity to solve this problem. "Individual efforts and initiatives are much needed. Every minute of delay results in a higher number of victims," Abu al-Fadl said.

The volunteer-based Syrian Mine Action Center (SMAC), for example, has received at least 11,000 reports of areas contaminated with explosive devices in rural Aleppo, northern Hama and in Idlib as well as its countryside, but the organization does not have the resources to deal with such a large number of notices, according to the center's managing director, Ahmad Nasif.

The SMAC is not alone. Most organizations in Syria do not have enough funding to tackle the problem. **Studies indicate that Syria needs $52 million for mine action this year.** After an appeal made in 2016 to raise $347 million, the UN launched a $511 million international appeal in February for humanitarian mine action in conflict and post-conflict settings. The UN anti-mine agency's Syria response received $3.8 million on an appeal for $10.5 million for "coordination, risk education, impact survey, and victim assistance activities."

Small Russian Drones Do Massive Damage With Grenade Weapons

By David Hambling

Source: http://www.scout.com/military/warrior/story/1791949-small-russian-drones-drop-grenade-weapons

July 18 – **Small consumer drones rigged to drop grenades have proved an effective weapon in Iraq and Syria.** The volume of attacks by ISIS drones threatened to stall the assault on Mosul, and the Iraqi Federal Police soon now deploy their own grenade-dropping drones against ISIS. However, such drones are not limited to the tactical battlefield. In spite of their diminutive size, such drones may become weapons of mass destruction in their own right. A precision attack does not need to deliver a massive warhead: it just has to 'bring the detonator' to a vulnerable target.

The Ukrainian SBU – the equivalent of the FBI – now believe that the destruction of a giant arms depot at **Balakliya** (photo – left) in eastern **Ukraine** in March was carried out by a small drone. The spectacular explosion and fire destroyed some seventy thousand tons of munitions with damage estimated at a billion dollars, though only one person was killed. This destruction is a graphic illustration of the threat posed by small drones, as many other high-value targets may be equally vulnerable.

Balakliya was said to be the largest ammunition dump in the world. Photographs of the site show wooden boxes of ammunition left in the open, making it a tempting target for an aerial saboteur. Several similar strikes have been carried out in Ukraine.

"This form of anti-materiel attack—though on a lesser scale—has already taken place at least two times in South-East Ukraine by Russian-linked forces utilizing weaponized UAS

dropping incendiary bomblets," says Robert Bunker, Adjunct Research Professor at the U.S. Army War College.

On 29th October 2015, the ammunition depot at Svatovo was hit. Some three thousand tons of ammunition went up, and 1,700 homes were damaged nearby.

This year, on the night of 17th February, an ammunition warehouse in Zaporozhye region was set on fire causing a series of explosions. The same tactics were used the next night at a storage site near Grodovka village in the Donetsk region, but this time the fires were put out. On 14th March a drone attacked another Ukrainian military facility near Donestsk, making three separate sorties and dropping two grenades each time according to Ukrainian military officials.

There had been a previous drone attack at Balakliya in December 2015, when small drones dropped at least fourteen grenades. The grenades started fires in the open storage areas, but the Ukrainian soldiers, showing considerable bravery, put out the fires. On that occasion one of the devices was recovered intact, and was identified as a Russian ZMG-1 mine grenade. (photo – below)

The **ZMG-1** is a thermite charge, a specialist tool used for demolition by Russian special forces, which resembles the U.S. AN-M14 grenade. Grenades of this type burn rather than exploding, and are placed rather than thrown, as they must be in contact with the target. They are filled with a mixture of metal and metal oxide which react to produce extreme temperatures – something over 4,000 degrees Fahrenheit.

The **AN-M14** (photo – right) can melt through a steel plate half an inch thick and is typically used to disable artillery. The ZMG-1 appears to have similar capability. The Ukrainian SBU have previously captured ZMG-1s in caches associated with Russian separatist groups, so they have such weapons, and ammunition dumps are a prime target.

"A weapons depot is such a good target for drones because incendiary device dropped from the drone only needs to act as fuse, using the materiel on the ground for the actual explosion," says Ulrike Franke, a drone expert at the European Council on Foreign Relations.

This echoes the warning by T X Hammes of the Center for Strategic Research about a type of attack he calls 'bringing the detonator'. Where there is a suitably vulnerable target, even a drone with a small warhead can do tremendous damage. It does not need to carry the explosive, because explosive is already there, it is just a matter of setting it off. This does not just mean ammunition dumps.

"Other infrastructure sites that would be particularly vulnerable to this form of attack would be those storing highly flammable substances such as fuel — especially aviation fuel," says Bunker. "Commercial aircraft parked at an airport laden with fuel in their wing storage cells would also be very susceptible."

Hammes also mentions parked aircraft as a target. Sites storing quantities of liquified natural gas or petrochemicals, fuel depots and similar locations could be similarly susceptible to such attacks. Storage tanks of other dangerous chemicals might not explodes and burn, but if ruptured they could still have catastrophic effects. Th accidental release of methyl isocyanate gas from a plant on Bhopal in 1984 caused over three thousand deaths. Any risk

of a similar incident is likely to result in the evacuation of a wide area as a minimum, even if there are no casualties.

Small drones are readily available over the internet. Unlike earlier generations of radio-controlled aircraft, they are easy to use, and a beginner can fly one out of the box. Grenades of the sort dropped by drones in Iraq and Syria may be hard to acquire outside of a war zone, but thermite is another matter. It is easy to make, and can be legally purchased in the US, UK and elsewhere. Terrorists may have trouble making their own explosives, and often get caught in the process, but they can acquire thermite without attractive attention.

ISIS may be living on borrowed time in Iraq and Syria, but the group is likely to survive as a diffuse, international, online presence. Having had so much success with consumer weaponized drones they are not likely to abandon them. Similarly, anyone opposed to Russia's foreign policy might find themselves on the receiving end of thermite charges delivered by untraceable commercial drones in the hands of 'Little Green Men' who may or may not belong to the Russian military.

While the spectacular destruction at Balakliya made headlines around the world, the billion dollars of damage may only represent an opening bid. One airliner can cost upwards of $400m. While counter-drone defenses have tended to concentrate on military and government installations and public spaces such as sports stadiums, the biggest risk may be to economic targets. Expect to see more 'bring the detonator' strikes by small drones in the near future.

David Hambling *is a special contributor to Scout Warrior. He has authored several books, including Swarm Troopers: How Small Drones Will Conquer the World and Weapons Grade: How Modern Warfare Gave Birth to Our High-Tech World.*

Should conventional terrorist bombings be considered weapons of mass ~~destruction~~ terrorism?

By Bryan R. Early, Erika G. Martin, Brian Nussbaum and Kathleen Deloughery

Dynamics of Asymmetric Conflict. Volume 10, 2017 - Issue 1; pp. 54-73

Source:http://www.tandfonline.com/doi/abs/10.1080/17467586.2017.1349327?af=R&journalCode=rdac20

Since weapons of mass destruction (WMD) are typically thought of as chemical, biological, radiological, or nuclear (CBRN) weapons, the designation of conventional bombings as WMD terrorism under US law has generated controversy and can affect how policymakers plan for future attacks. Using quantitative data on terrorist attacks, federal planning documents, and the academic literature, we argue that placing the conventional terrorist bombings in the same legal category as CBRN terrorism confuses two distinct terrorist threats with different risks of occurrence, casualty profiles, consequences, and emergency response requirements. We explore the logical and practical reasons why such threat conflation could create policy problems. We conclude that the current definition of WMD terrorism under US law that aggregates conventional terrorist bombings with CBRN terrorism should be revised.

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

CYBER NEWS

Almost 16,000 Belgians on the World's biggest black list

Source: http://deredactie.be/cm/vrtnieuws.english/News/1.3009194

June 24 – The Flemish business daily 'De Tijd' is among a number of international media that have published articles this weekend about World-Check. World-Check is a database of so-called "Politically Exposed Persons" and heightened risk individuals.

The organisation is used around the world to help to identify and manage financial, regulatory and reputational risk. As such it is the biggest black list in the world. Around 16,000 Belgians appear on the list, quiet a number of them wrongly or on the basis on inaccurate information. Being branded a risk by World-Check can have negative consequences without you even realising it.

The British whistle-blower Chris Vickery was able to obtain a 2014 version of the World-Check list. Journalists in 6 countries examined the list over a period of 5 months.

'De Tijd', 'The Times' (GB), 'The Intercept'(USA), NPO Radio 1 (NL), La Republicca (I), NRD/Süddeutsche Zeitung (D), have all published/broadcast pieces about World-Check today.

Anyone that is named as a risk on the World-Check database risks being black-listed by 6,000 big banks, companies and public services without them even knowing.

In Belgium big High Street banks such as KBC, BNP-Paribas Fortis, Belfius and ING have confirmed that they screen their customer data based on information gained from World-Check.

De Tijd looked at the data related to 15,833 Belgians on the World-Check black list. The paper comes to the conclusion that a lot of people have been branded a risk unfairly.

The sources used by World-Check are not always accurate. A quarter of the names come from official sanctioning lists. However, the rest are taken from more than 100,000 other "news sources".

De Tijd concludes that the database is anything but accurate, complete and up-to-date.

Not everyone on the terrorism list is a terrorist or a terrorist suspect

At the end of 2014 346 people in Belgium appeared on the World-Check database in the "terrorism" category. However, this included people that had been suspects, but had never been charged or cleared of any charges laid against them.

The League of Belgian Muslims, an organisation that has for many years condemned violence and describes terrorist attacks as "barbaric" also appears on the list in the "terrorism" category.

World-Check provides no evidence to link the organisation to terrorism.

Two of the links cited as the reason for the League of Belgian Muslims appearing on the list have been taken off line and a third article relates to a charter calling for all Muslims to strive for peace and prosperity that the League signed up to.

How do organisations and individuals remain on the list

There are also concerns about how long names remain on the list. 238 people in Belgium appear in the fiscal fraud category. They include the former Belgian international goalkeeper Jean-Marie Pfaff and his wife Carmen.

They were once the subject of a tax-evasion investigation, but settled out of court. The television producer Wouter Vandenhautte also appears despite him having been given discharges in court cases brought against him for fiscal fraud in 2010 and 2012.

The former Belgian Minister and NATO Secretary General Willy Claes also appears on the 2014 list, almost 20 years after the Agusta affair that led to his downfall.

"Politically-sensitive persons"

6.565 Belgian are categorised as being "politically-sensitive" persons. In addition to almost everyone that has political mandate there are many children, (ex) partners, brothers, sisters, parents and other family members that appear on the list.

These include the children of the leader of the Liberal Group in the European Parliament Guy Verhofstadt and the children of the Justice Minister Koen Geens (Flemish Christian democrat).

The illegitimate daughter of King Albert II, Delphine Boël also appears on the list.

Privacy Commission to ask the banks for an explanation

'De Tijd' put its findings to the Belgian Privacy Commission. The Commission's Chairman Willem Debeuckelaere said that he definitely intends to discuss the issue with the banks".

"As the banks should inform their customers that the use World-Check, as they are using data that doesn't come from the customers, but from a third party".

Mr Debeuckelaere adds that people should be able to object to their inclusion on the list and to ask for information to be modified or corrected. World-Check should also be made to delete inaccurate data.

How to navigate fake news: An expert's guide to cutting through the nonsense and staying objective

Source (video): http://www.dailymail.co.uk/news/article-4637638/How-navigate-fake-news-experts-guide.html

June 25 – Journalist **David Patrikarakos** provides an step-by-step guide to staying objective.

Hackers can exploit electronic cigarettes and any other electronic device to deliver a malware in a poorly protected network.

Source: http://securityaffairs.co/wordpress/60296/hacking/electronic-cigarettes-hacking-took.html

June 25 – **In November 2014, in a discussion started on the Reddit news media website it has been debated the case of a malware implanted by using electronic cigarettes connected over USB.**
Hackers are able to exploit any electronic device to deliver a malware in a poorly protected network. Electronic cigarettes could be an attack vector, the idea may appear hilarious, many electronic cigarettes can be charged over USB, using a special cable or by inserting one end of the cigarette directly into a USB port.
The report posted on the social news Reddit website reported a strange case happened to an executive that discovered a malware in his system without immediately identify its source.
"One particular executive had a malware infection on his computer from which the source could not be determined," reported a Reddit user "After all traditional means of infection were covered, IT started looking into other possibilities.
Investigating on the case, the man discovered that the electronic cigarettes were infected by a malware hardcoded into the charger, once the victim will connect it to the computer the malicious code will contact the C&C server to drop other malicious code and infect the system

Electronic cigarettes or vape pens properly modified could be an effective hacking tool to infect a targeted computer.
The security researcher Ross Bevington presented at BSides London how to use electronic cigarettes to compromise a computer by tricking it to believe that it was a keyboard.The researchers also explained that it is BSides London how to use electronic cigarettes to compromise a computer by tricking it to believe that it was a keyboard.
It is important to note that Bevington's attack required the victim's machine to be unlocked.
"PoisonTap is a very similar style of attack that will even work on locked machines," Mr *Bevington told Sky News.*
The researchers also explained that it is possible to use the electronic cigarettes to interfere with its network traffic.
E-cigarettes are powered by a rechargeable lithium-ion battery that can be plugged into a cable or directly connects to the USB port of a computer.
"Security researchers have demonstrated how e-cigarettes can easily be modified into tools to hack computers." reported SkyNews.

"With only minor modifications, the vape pen can be used by attackers to compromise the computers they are connected to – even if it seems just like they are charging."
The researcher @FourOctets published a proof-of-concept video (click at source's URL), which showed arbitrary commands being sent to an unlocked laptop just by charging a vape pen.

Cyberattack Hits Ukraine Then Spreads Internationally

Source: https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html

Several companies have been affected by the Petya cyberattack, including, from left, Rosneft, the Russian energy giant; Merck, a pharmaceutical company; and Maersk, a shipping company. Credit Left, Sergei Karpukhin/Reuters; center, Matt Rourke/Associated Press; right, Enrique Castro Sanchez/Agence France-Presse — Getty Images

June 27 – Computer systems from Ukraine to the United States were struck on Tuesday in an international cyberattack that was similar to a recent assault that crippled tens of thousands of machines worldwide.
In Kiev, the capital of Ukraine, A.T.M.s stopped working. About 80 miles away, workers were forced to manually monitor radiation at the old Chernobyl nuclear plant when their computers failed. And tech managers at companies around the world — from Maersk, the Danish shipping conglomerate, to Merck, the drug giant in the United States — were scrambling to respond. Even an Australian factory for the chocolate giant Cadbury was affected.
It was unclear who was behind this cyberattack, and the extent of its impact was still hard to gauge Tuesday. It started as an attack on Ukrainian government and business computer systems — an assault that appeared to have been intended to hit the day before a holiday marking the adoption in 1996 of Ukraine's first Constitution after its break from the Soviet Union. The attack spread from there, causing collateral damage around the world.
The outbreak was the latest and perhaps the most sophisticated in a series of attacks making use of dozens of hacking tools that were stolen from the National Security Agency and leaked online in April by a group called the Shadow Brokers.
"The N.S.A. needs to take a leadership role in working closely with security and operating system platform vendors such as Apple and...
As well documented in Andy Greenberg's well researched recent article in Wired magazine's July issue, Russian based cyber-terrorists seem...

Like the WannaCry attacks in May, the latest global hacking took control of computers and demanded digital ransom from their owners to regain access. The new attack used the same National Security Agency hacking tool, Eternal Blue, that was used in the WannaCry episode, as well as two other methods to promote its spread, according to researchers at the computer security company Symantec.
The National Security Agency has not acknowledged its tools were used in WannaCry or other attacks. But computer security specialists are demanding that the agency help the rest of the world defend against the weapons it created.
"The N.S.A. needs to take a leadership role in working closely with security and operating system platform vendors such as Apple and Microsoft to address the plague that they've unleashed," said Golan Ben-Oni, the global chief information officer at IDT, a Newark-based conglomerate hit by a separate attack in April that used the agency's hacking tools. Mr. Ben-Oni warned federal officials that more serious attacks were probably on the horizon.
The vulnerability in Windows software used by Eternal Blue was patched by Microsoft in March, but as the WannaCry attacks demonstrated, hundreds of thousands of groups around the world failed to properly install the fix.
"Just because you roll out a patch doesn't mean it'll be put in place quickly," said Carl Herberger, vice president for security at Radware. "The more bureaucratic an organization is, the higher chance it won't have updated its software."
Because the ransomware used at least two other ways to spread on Tuesday — including stealing victims' credentials — even those who used the Microsoft patch could be vulnerable and potential targets for later attacks, according to researchers at F-Secure, a Finnish cybersecurity firm, and others.
A Microsoft spokesman said the company's latest antivirus software should protect against the attack.

Who Has Been Affected
Governments and companies in Europe and the United States have been impacted. Here are several:

- **Ukrainian institutions**
  Including the Infrastructure Ministry, central bank, state postal service and largest telephone company.
- **Rosneft**
  A Russian oil company.
- **A.P. MOLLER-MAERSK**
  The world's largest container-shipping company.
- **Merck**
  A U.S. pharmaceutical company.
- **Saint-Gobain**
  A French construction materials company.
- **WPP**
  A British marketing company.
- **DLA Piper**
  Law firm.
- **Deutsche Bahn**
  German railway company.

The Ukrainian government said several of its ministries, local banks and metro systems had been affected. A number of other European companies, including Rosneft, the Russian energy giant; Saint-Gobain, the French construction materials company; and WPP, the British advertising agency, also said they had been targeted.
Ukrainian officials pointed a finger at Russia on Tuesday, although Russian companies were also affected. Home Credit bank, one of Russia's top 50 lenders, was paralyzed, with all of its offices closed, according to the RBC news website. The attack also affected Evraz, a steel manufacturing and mining company that employs about 80,000 people, the RBC website reported.
In the United States, the multinational law firm DLA Piper also reported being hit. **Hospitals** in Pennsylvania were being forced to cancel operations after the attack hit computers at Heritage Valley Health Systems, a Pennsylvania health care provider, and its hospitals in Beaver and Sewickley, Penn., and satellite locations across the state.
The ransomware also hurt Australian branches of international companies. DLA Piper's Australian offices warned clients that they were dealing with a "serious global cyber incident" and had disabled email as a precautionary measure. Local news reports said that in Hobart, Tasmania, on Tuesday evening, computers in a Cadbury chocolate factory, owned by Mondelez International, had displayed ransomware messages that demanded $300 in bitcoins.
Qantas Airways' booking system failed for a time on Tuesday, but the company said the breakdown was due to an unrelated hardware issue.

The Australian government has urged companies to install security updates and isolate any infected computers from their networks.

"This ransomware attack is a wake-up call to all Australian businesses to regularly back up their data and install the latest security patches," said Dan Tehan, the cybersecurity minister. "We are aware of the situation and monitoring it closely."

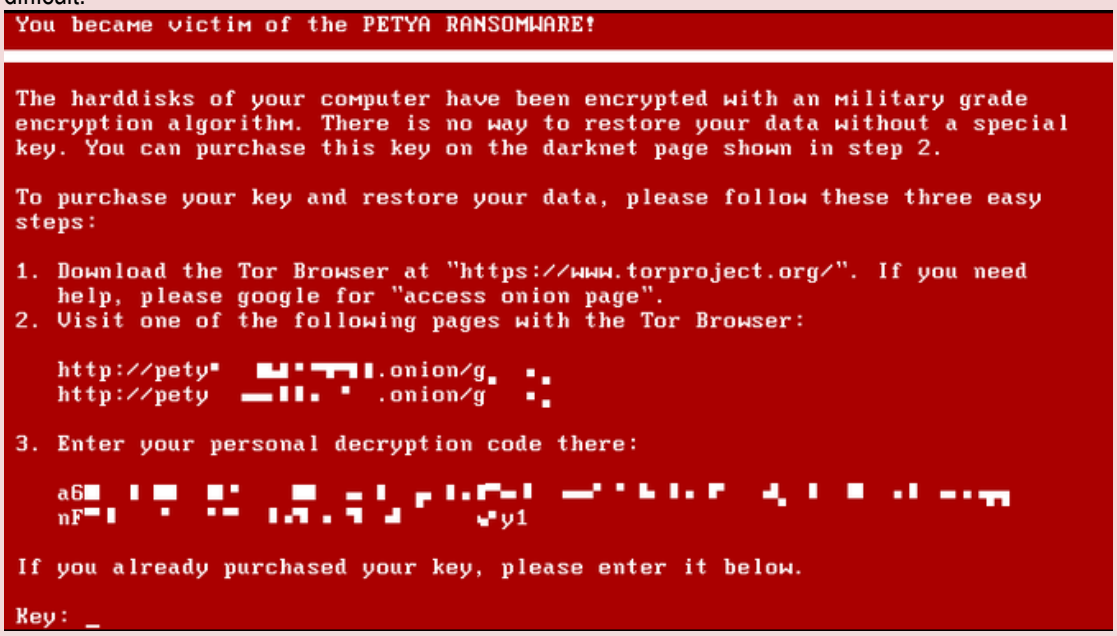
A National Security Agency spokesman referred questions about the attack to the Department of Homeland Security. "The Department of Homeland Security is monitoring reports of cyberattacks affecting multiple global entities and is coordinating with our international and domestic cyber partners," Scott McConnell, a department spokesman, said in a statement.

Computer specialists said the ransomware was very similar to a virus that emerged last year called Petya. Petya means "Little Peter," in Russian, leading some to speculate the name referred to Sergei Prokofiev's 1936 symphony "Peter and the Wolf," about a boy who captures a wolf.

Reports that the computer virus was a variant of Petya suggest the attackers will be hard to trace. Petya was for sale on the so-called dark web, where its creators made the ransomware available as "ransomware as a service" — a play on Silicon Valley terminology for delivering software over the internet, according to the security firm Avast Threat Labs.

That means anyone could launch the ransomware with the click of a button, encrypt someone's systems and demand a ransom to unlock it. If the victim pays, the authors of the Petya ransomware, who call themselves Janus Cybercrime Solutions, get a cut of the payment.

That distribution method means that pinning down the people responsible for Tuesday's attack could be difficult.



A screenshot of what appeared to be the ransomware affecting systems worldwide on Tuesday. The Ukrainian government posted the shot to its official Facebook page.

The attack is "an improved and more lethal version of WannaCry," said Matthieu Suiche, a security researcher who helped contain the spread of the WannaCry ransomware when he created a kill switch that stopped the attacks.

In just the last seven days, Mr. Suiche noted, WannaCry had tried to hit an additional 80,000 organizations but was prevented from executing attack code because of the kill switch. Petya does not have a kill switch. Petya also encrypts and locks entire hard drives, whereas the earlier ransomware attacks locked only individual files, said Chris Hinkley, a researcher at the security firm Armor.

The hackers behind Petya demanded $300 worth of the cybercurrency Bitcoin to unlock victims' machines. By Tuesday afternoon, online records showed that 30 victims had paid the ransom, although it was not clear whether they had regained access to their files. Other victims may be out of luck, after Posteo, the German email service provider, shut down the hackers' email account.

In Ukraine, people turned up at post offices, A.T.M.s and airports to find blank computer screens, or signs about closures. At Kiev's central post office, a few bewildered customers milled about, holding parcels and letters, looking at a sign that said, "Closed for technical reasons."
The hackers compromised Ukrainian accounting software mandated to be used in various industries in the country, including government agencies and banks, according to researchers at Cisco Talos, the security division of the computer networking company. That allowed them to unleash their ransomware when the software, which is also used in other countries, was updated.
The ransomware spread for five days across Ukraine, and around the world, before activating Tuesday evening.
"If I had to guess, I would think this was done to send a political message," said Craig Williams, the senior technical researcher at Talos.
One Kiev resident, Tetiana Vasylieva, was forced to borrow money from a relative after failing to withdraw money at four automated teller machines. At one A.T.M. in Kiev belonging to the Ukrainian branch of the Austrian bank Raiffeisen, a message on the screen said the machine was not functioning.
Ukraine's Infrastructure Ministry, the postal service, the national railway company, and one of the country's largest communications companies, Ukrtelecom, had been affected, Volodymyr Omelyan, the country's infrastructure minister, said in a Facebook post.
Officials for the metro system in Kiev said card payments could not be accepted. The national power grid company Kievenergo had to switch off all of its computers, but the situation was under control, according to the Interfax-Ukraine news agency. Metro Group, a German company that runs wholesale food stores, said its operations in Ukraine had been affected.

At the Chernobyl plant, the computers affected by the attack collected data on radiation levels and were not connected to industrial systems at the site, where, although all reactors have been decommissioned, huge volumes of radioactive waste remain. Operators said radiation monitoring was being done manually.

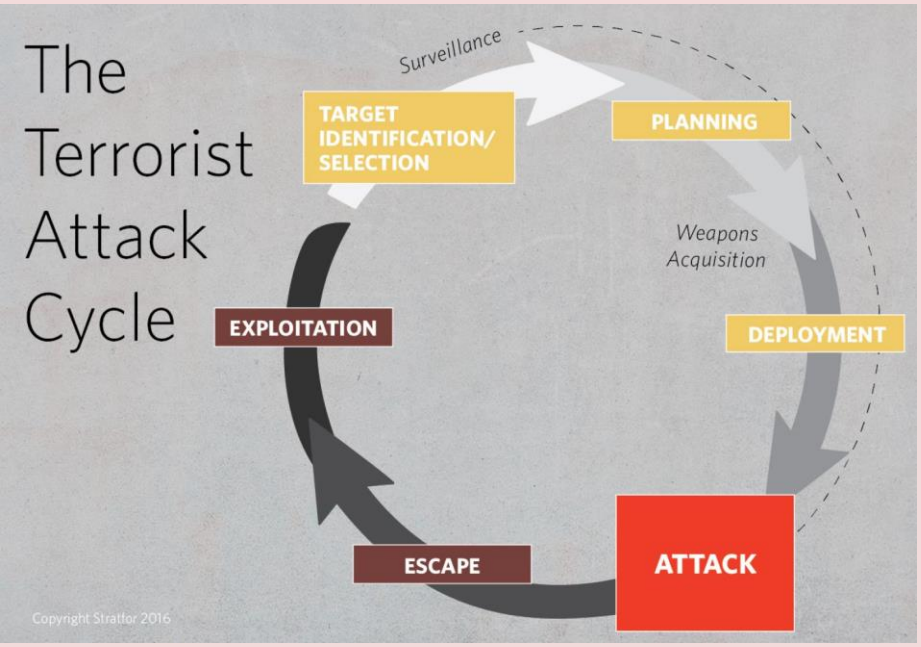
Cybersecurity researchers questioned whether collecting ransom was the true objective of the attack.
"It's entirely possible that this attack could have been a smoke screen," said Justin Harvey, the managing director of global incident response at Accenture Security. "If you are an evildoer and you wanted to cause mayhem, why wouldn't you try to first mask it as something else?"

Finding Low-Tech Solutions for High-Tech Terrorism

By Scott Stewart
Source: https://worldview.stratfor.com/article/finding-low-tech-solutions-high-tech-terrorism

Jume 29 – Last week, I noted that there is nothing that can be done to stop the advancement of digital encryption. In the years to come, not only will the practice become more widely used, it will also be even harder to crack, resulting in more and larger digital "black holes," or safe spaces where terrorists and other criminals can communicate and store data. When authorities are limited in their ability to monitor the communications of terrorist suspects, they are deprived of important information streams typically used to conduct threat assessments and counterterrorism investigations. However, the age of encryption does not deliver a fatal blow to counterterrorism efforts, and as long as authorities continue to use valuable low-tech intelligence methods, they will be able to adjust to this new reality.
Even Black Holes Have Limits
First, it is important to recognize that although it does allow terrorists to accomplish many things, the protection provided by digital encryption is actually fairly limited. Encryption is certainly quite useful for communications: It can help terrorists recruit and radicalize new militants or provide instructions. It also allows terrorist operatives to send lists of prospective targets to their leadership for approval and gives clandestine surveillance cells the ability to remotely and anonymously share digital files with attack planners and operational cells. And I've written before about how I believe digital safe havens will at some point provide space for the formation of a sort of "online university of terrorism" that can be used to train grassroots operatives in terrorist tradecraft skills.
But eventually, to conduct a physical attack, terrorist operatives will need to leave their digital hideouts, and when they do, they will continue to be limited by the constraints inherent in the terrorist attack cycle. While some tasks in the cycle can be accomplished electronically, like

discussing potential targets, assigning tasks and doing certain types of presurveillance research, there are simply many others that require interaction with the real world. And during these interactions, terrorist operatives are vulnerable to detection.



One of the times when terrorist planners are most susceptible is the preoperational surveillance phase, because terrorists must repeatedly expose themselves to their potential target, and they risk being noticed. There is a myth that terrorist surveillance is sophisticated. But in most cases, the surveillance tradecraft of terrorist operatives is quite rudimentary, and the only reason they are able to get away with this sloppy tradecraft is that the average person is not looking for them. In the age of digital encryption, surveillance remains perhaps the most significant weakness in the terrorist attack cycle.

The weapons acquisition phase is also a rather unguarded part of the cycle, requiring terrorist planners to abandon their digital safe havens to gather weapons, which can give authorities the opportunity to identify and arrest them. In several instances, attempts to obtain weapons have led attack planners into government sting operations. It is also during this phase that operatives must obtain precursor chemicals for making homemade explosives and other components needed to fabricate bombs. Telltale signs of bombmaking activity can give plotters away. The diary kept by Oslo attacker Anders Breivik as he was progressing through his attack cycle provides a great glimpse into how vulnerable an attacker feels during the weapons acquisition and bombmaking stages. So no matter how effective a terrorist's encryption tools may be, there are still always going to be physical actions that counterterrorism forces can watch for and respond to.

A Long History of Communications Monitoring

Counterterrorism forces have sought out terrorist communications since Victorian-era detectives first began intercepting the letters of suspected anarchists. In the modern era, those efforts expanded to include planting listening devices and wiretapping telephone lines, and later, monitoring cell phones, email and other internet messaging applications. Indeed, this government monitoring helped prompt the widespread adoption of sophisticated digital encryption in the first place. But even before that, people being monitored have adopted many methods to try to evade that surveillance.

In the past, when terrorists suspected that agents were monitoring their written communications, they would employ a number of codes and hidden writing techniques to try to foil them. Suspects have used pay phones and satellite phones to avoid wiretapping. And in many cases, such as that of Osama bin Laden, they would communicate only through trusted couriers to avoid having their locations compromised. In a way, digital encryption is quite similar to using a physical courier — just far more rapid and efficient.

And encryption is only useful to terrorist groups if they really trust that governments can't break it; some groups simply do not. The fear of intelligence agencies' capabilities, and the difficulty that fear added to attack planning, is in part what led jihadist ideologues to start advocating for the concept of leaderless resistance. After all, in its purest construct, a leaderless resistance offers no communications that could be monitored. Of course, in practice, strict communications security protocols are frequently ignored, exemplified by Fort Hood shooter Nidal Hasan's communications with Anwar al-Awlaki. And there have also been examples of terrorists intentionally sending false messages along monitored channels in order to cause panic by triggering warnings.

The bottom line is that several factors have long made it difficult for counterterrorism forces to access terrorist communications; encryption is merely the latest, and it does not represent

an impossible roadblock in the fight against terrorism. As encryption improves, governments will, in turn, improve their own tools and methods for compromising terrorists' electronic systems.

Returning the Focus to HUMINT

Furthermore, the rise of encryption has highlighted the intelligence community's unhealthy reliance upon signals intelligence (SIGINT), or information gathered from signals, often electronic. The initial successes of SIGINT programs, such as the breaking of the Japanese Imperial Navy's codes and the solving of Nazi Enigma machines during World War II, were incredibly intoxicating. But those successes have proved hard to replicate, and intelligence and law enforcement agencies have spent billions of dollars in their efforts to re-create the euphoria of those achievements. SIGINT can be a useful part of an overall national intelligence program, but as targets have adjusted their behavior, it has become increasingly irresponsible to rely too heavily on that method. The encryption of digital communications poses new problems to data collection, but not the first or only ones.

The failings of SIGINT in the face of encryption serve as a reminder that one of the method's counterparts, human intelligence (HUMINT), remains a crucial component of a successful counterterrorism program. Even in the digital age, developing and managing human sources remains a vital discipline, and its value comes in many forms.

HUMINT can entail traditional operations, such as sending undercover agents to penetrate cells and groups or recruiting members of those groups to serve as agents — though it is more difficult to use HUMINT to target movements that employ the leaderless resistance model instead of a traditional hierarchy. Counterterrorism efforts can also include law enforcement HUMINT practices, such as "flipping" a suspect and sending them back into an organization to serve as an informant. The FBI has been quite successful in using this approach to identify and catch grassroots terrorist operatives. And of course, interrogations can be a crucial source of HUMINT as well. However, they must be conducted properly in order to provide useful intelligence. Despite the promises of proponents of "enhanced interrogation" methods, torture does not provide a reliable shortcut to obtaining important information.

But HUMINT writ large can also include information provided through programs such as the U.S. Department of State's Rewards for Justice program, which has led to the arrests of several significant terrorist figures. Public outreach programs by law enforcement agencies have also resulted in tips that have thwarted terrorist attacks. Some of these came as would-be terrorists were attempting to acquire bombmaking components. Others came from concerned family or community members. The Unabomber's yearslong terrorist campaign finally ended when his brother identified him to the FBI after reading his manifesto. In several unfortunate recent terrorist cases, such as the May 22 bombing in Manchester, England, tips provided to the authorities were seemingly disregarded.

Ultimately, it is important for those in the intelligence community to embrace the necessity of HUMINT. Ignoring its results on the basis that it is somehow less reliable than SIGINT will only limit the community's overall effectiveness. Low-tech solutions such as surveillance detection and HUMINT will continue to provide actionable intelligence for counterterrorism investigators and analysts and will improve their ability to fight terrorism, even as technologies and methods used by terrorist groups evolve.

***Scott Stewart** supervises Stratfor's analysis of terrorism and security issues. Before joining Stratfor, he was a special agent with the U.S. State Department for 10 years and was involved in hundreds of terrorism investigations.*

NotPetya is a wiper, not ransomware: Here's what that means

Source: http://www.digit.in/internet/notpetya-is-a-wiper-not-ransomware-heres-what-that-means-35819.html

June 29 – The NotPetya malware breaking computers worldwide since Tuesday is not a ransomware at all. It's a wiper.

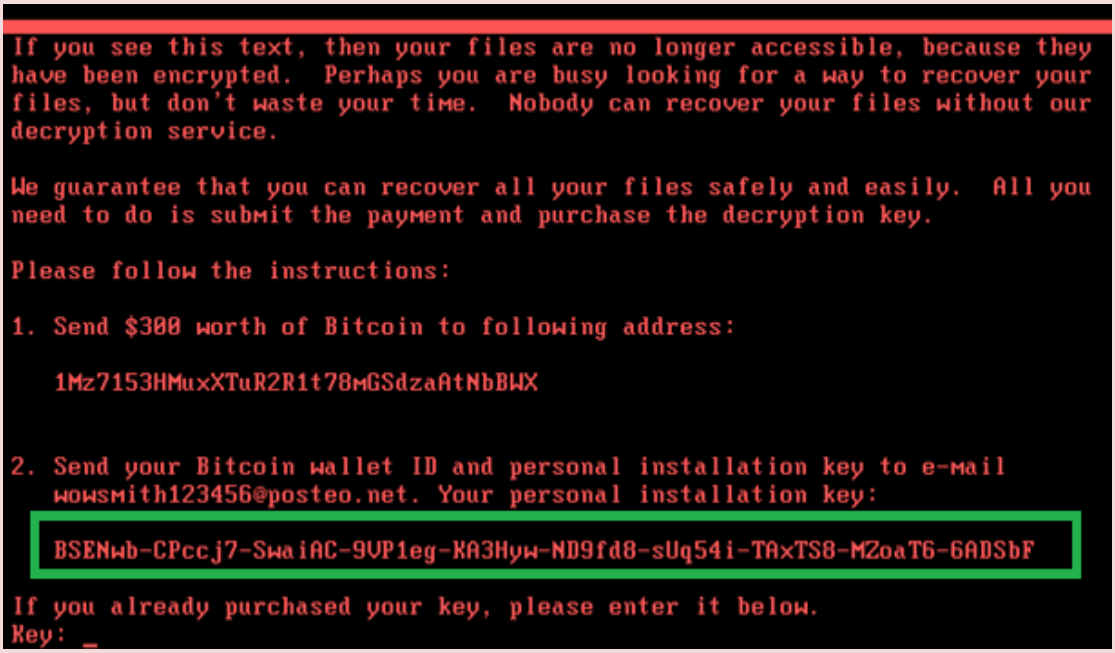
I've been the TV series Dexter recently, so let me explain this by drawing a parallel from that. Imagine two serial killers — one that has a code and only kills bad guys, while the other just goes about killing. The first killer has a purpose of sorts, he's committing a crime, but in his mind he has a reason for it. That's WannaCry, the ransomware that would take away access to your files, but it would do so to extort money from you.

On the other hand, Petwrap/NotPetya is simply destroying files on your PC, with no real intent to earn money. "The goal of this malware is pure evil. It's not to make money, it's to destroy data," says Saket Modi, CEO of Lucideus, a cybersecurity services company. NotPetya is that second killer, who is simply a bad guy doing bad things.

Why did you call it a ransomware then?

That's because the malware is cleverly made to look like one, possibly to get public interest going. WannaCry worked up quite a storm, and this new one wants to ride that into the history books. In reality, NotPetya could be a much more dangerous malware than WannaCry ever was.

You see, by definition, a ransomware encrypts your files, holding them hostage for a ransom. A decryption key is generated, that the attacker promises to give you when the ransom has been paid, usually in bitcoins. In the case of NotPetya, the files have not been encrypted in the first place, explains Modi. The malware is sort of deleting the data on your hard drive, and there was no decryption key to begin with.



"After an analysis of the encryption routine of the malware used in the Petya/ExPetr attacks, we have thought that the threat actor cannot decrypt victims' disk, even if a payment was made," wrote researchers from Kaspersky Labs, in a blog post. If there was ever a reason to not pay the ransom, this is it. Modi says there were very few payments made after the first few days, and researchers have seen no instances of decryption anywhere in the world.

So what is NotPetya then?

They're calling it a wiper. "The goal of a wiper is to destroy and damage. The goal of a ransomware is to make money. Different intent. Different motive. Different narrative. A ransomware has the ability to restore its modification such as (restoring the MBR like in the 2016 Petya, or decrypting files if the victim pays)—a wiper would simply destroy and exclude possibilities of restoration," writes Matt Suiche, hacker and founder of Comae Technologies, a UAE-based cybersecurity firm.

The image below is from Kaspersky Labs' analysis of the malware. The highlighted portion represents an "installation ID", which Kaspersky says is seen on most ransomware. This installation ID is unique for each victim, and attackers need it to produce the decryption key. On NotPetya, "the ID shown in the ransom screen is just plain random data", Kaspersky writes.

This means that even if you pay the ransom, your data is likely lost forever. Secondly, it's in line with suspicions that NotPetya was never financially motivated in the first place. Lucideus' Modi also explained that while some data may be recoverable on SSDs and HDDs, flash storage-based systems will be completely wiped.

This is because flash storage doesn't use layering of data and the classic RAM/ROM architecture (in SSDs and HDDs) isn't used. So, when the malware writes to a disk on flash storage, it is essentially deleting all of its earlier data.

Am I safe?

As we explained in yesterday's report, the means of infection for NotPetya remains the same. Updated Windows software will protect against the EternalBlue vulnerability, while there's also a "vaccine" for this malware. You could simply create a perfc.dat file within the Windows folder, in read only mode, which stops the malware from deleting your files. It will still spread to other PCs on the network, but it will at least save your own data.

Israeli general: Cyber terror - why are global leaders waiting for their cyber 9/11?

By Brig. Gen. Eli Ben Meir

Source: http://www.foxnews.com/opinion/2017/06/30/israeli-general-cyber-terror-why-are-global-leaders-waiting-for-their-cyber-911.html

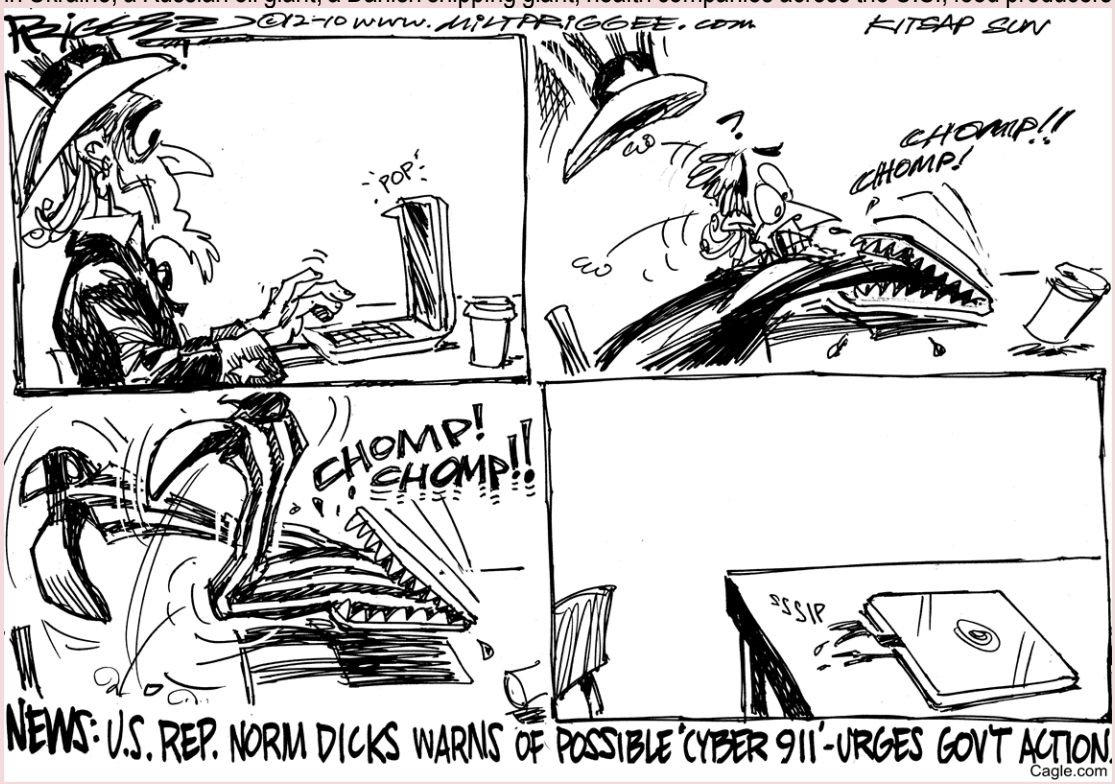
June 30 – Petya ransomware virus infects computers worldwide

Brig. Gen. Eli Ben-Meir, left, shakes hands with Brig. Gen. (res.) Itai Brun, right, as Ben-Meir takes over as head of the IDF's Research Brigade, during a ceremony, with head of army intelligence Maj. Gen. Herzi Halevi, on January 4, 2015. (IDF Spokesperson's Unit)

As a former Brigadier General in Israel's Military Intelligence, I am today reminded of a German word one of my commanders, a former Prime Minister and Chief of Staff, used to throw around: Gestalt. Gestalt, literally meaning shape, has a deeper meaning in the world of philosophy and psychology, referring to a complex holistic world. It stands for an idea where all systems should be viewed as a whole; where everything is interconnected.

It took two planes and thousands of murdered Americans for world governments to realize that the fight against terror involves cooperation and intelligence sharing - 9/11 was the wake-up call for governments to centralize their efforts, and take a holistic and eventually strategic view of the inter-agency and multi-disciplinary fight against terrorism.

Yet, once again the world's governments are snoozing. This week's Petya multi-sector cyber attack has already caused huge disruption. Victims so far include banks, aircraft manufacturers and postal services in Ukraine, a Russian oil giant, a Danish shipping giant, health companies across the U.S., food producers



in Spain, even chocolate factories in Australia. Petya is yet more evidence that, like the war on conventional terror, the cyber war must be fought with close cooperation, centralization, and a holistic approach to the problem.

Just a few weeks ago, another widespread hack, WannaCry, also targeted multiple countries and institutions, including the UK's National Health Service. For a moment, it appeared that we had reached a turning point, and that governments would begin to take cyber warfare as seriously as conventional warfare. But lessons were clearly not properly learned. Petya was detectable. The tool it deployed has been known about for over a year and is part of the Ransom wear as a service market in the dark web. Meanwhile, a technological patch developed after WannaCry was available to companies and institutions, but was clearly not adopted widely enough.

In other words, it appears that the proverbial snooze button was activated once more. Perhaps in the wake of Petya, governments will realize that cyber warfare is here to stay and it is only going to become more intense and dangerous. Perhaps governments will realize that now is the time to develop an effective, comprehensive and long-lasting response.

That does not mean that the fight will be easy. Far from it. Digital criminals are anonymous, making it difficult to locate and apprehend those who deployed Petya. Their weapons of choice are constantly advancing in a cat and mouse game where the hackers are always looking to locate a new vulnerability in their victims' defenses. And of course, national borders or boundaries between different sectors mean nothing to the digital criminals.

Cyber terrorists don't respect borders, they don't play by the rules of the game, so why should we? You don't arrest a bank robber with your eyes blindfolded and your hands tied behind your back. You call for backup, you conduct deep intelligence, you work with other agencies. And if the criminals do get away, you use all the tools at your disposal (and at the disposal of your local and international colleagues) to catch them and bring them to justice.

In Israel, we have unfortunately been at the forefront of countering cyber attacks. We have plenty of enemies who wish us harm, and we do not enjoy the margin of error that other larger nations (think they) have. For the last decade we have taken a holistic approach towards our cyber security. An attack on one entity, is an attack on all. An attack on one company, is a potential attack on an entire nation.

The government and military in Israel have therefore fused a centralized, strategic problem-solving mentality with the most advanced technologies, to identify, prevent and protect against cyber enemies. This expertise is no secret, it is at the disposal of world leaders. It could prove invaluable if we are to win what is unquestionably an international conflict. Regional and international cooperation between centralized agencies holds the keys to unlock the crucial cyber solutions we so evidently need.

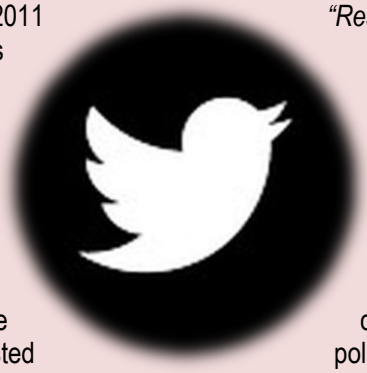
Progress is being made. This week's remarks by the Homeland Security Advisor, calling for greater international cyber security partnership, is a positive development. But global leaders need to do more. The world of cyber defense needs leadership, and we need it now. Let's not wait for our own cyber 9/11.

Brig. Gen. (ret.) Eli Ben Meir *is the Chief Strategy Officer and co-founder of CyGov, a leading cyber security advisory. He is formerly the second in command of Israel's military intelligence.*

Twitter can detect riots long before police are called – study

Source: https://www.rt.com/news/394450-twitter-riot-detection-police/

June 29 – Twitter can be used for more than simply keeping up with trending hashtags. In fact, it can be used as an "invaluable" police tool for detecting riots, according to a new study. The study from Cardiff University examined 1.6 million tweets relating to the 2011 London riots, which brought levels of violence, looting, and property destruction which England had not seen in more than three decades.



Researchers used machine-learning algorithms to analyze each tweet, taking into account details including when they were posted, where they were posted from, and the contents of the tweets.

Researchers found that computer systems could automatically scan through Twitter and detect serious incidents before they were reported to police. Such events included cars being set on fire and stores being broken into.

Computers could also gather information about where riots were rumored to take place, and where groups of youths were gathering.

"On average the computer systems could pick up on disruptive events several minutes before officials and over an hour in some cases," Cardiff University wrote in a press release earlier this week.

When the very first reports of disorder occurring in the London borough of Enfield were received by police, researchers found that their systems could have picked up the information from Twitter one hour and 23 minutes earlier.

"Results showed that the machine-learning algorithms were quicker than police sources in all but two of the disruptive events reported," the release states.

Study co-author Pete Burnap, from Cardiff University's School of Computer Science and Informatics, said the information can be used alongside existing policing methods.

"We will never replace traditional policing resource on the ground but we have demonstrated that this research could augment existing intelligence gathering and draw on new technologies to support more established policing methods," he said.

That thought was echoed by co-author Nasser Alsaedi, who recently completed his PhD at Cardiff under Burnap's supervision.

"Coming from a policing background myself I see the need for this type of cutting edge research every day," he said.

"I would like to see this

implemented alongside the established decision-making processes."

Cardiff University's Social Date Science Lab, directed by Burnap, has a partnership with London's Metropolitan Police which is aimed at using social media for the benefit of security and policing.

The study has been published in the journal ACM Transactions on Internet Technology.

Greek-Turkish Cyber War

This time it was the Police website (emniyetsen.org.tr)

UK Universities and the PC Police

Source: https://clarionproject.org/uk-universities-pc-police/

EU-Funded project uses artificial intelligence to tackle terrorist cyber-propaganda

Source: https://www.city.ac.uk/news/2017/july/eu-funded-project-uses-artificial-intelligence-to-tackle-terrorist-cyber-propaganda

July 11 – Professor of Security Engineering, Professor Muttukrishnan Rajarajan, and his City-based team are playing a leading role in the RED-Alert research and innovation project funded by the European Union's Horizon 2020 programme which is aimed at developing new online content for monitoring and analysis tools to fight terrorism.

The full title of the project is 'Real-time Early Detection and Alert System for Online Terrorist Content based on Natural Language Processing, Social Network Analysis, Artificial Intelligence and Complex Event Processing.'

Privacy-preservation methods

Professor Muttukrishnan says that he and his team of researchers "will be analysing social media data in a privacy-preserving manner, classifying it in an encrypted domain using homomorphic methods".

He also said that the social media data collection methodology used by his team will be General Data Protection Regulation (GDPR)-compliant.

Extremist and terrorist groups use the Internet for psychological warfare, propaganda, recruitment and misinformation, with dramatic consequences for European citizens.

Social media and online communication channels have increasingly become the primary tools for terrorist groups to reach out to vulnerable individuals and prompt them to action, resulting in over 40 terrorist attacks on European soil since 2015, all of them perpetrated by radicalized individuals.

RED-Alert attempts to bring together the best in European research and innovation to fight terrorism with a consortium of 16 organizations from 8 countries, including 6 European law enforcement agencies, supported by Europol's counter-terrorism unit. The project starts in June 2017 and will last 3 years.

Commander Dean Haydon, head of the Met Police Counter Terrorism Command, said: "We welcome efforts to advance technology that would make it easier for the UK's Counter Terrorism Network to identify and remove online terrorist material."

Definition

Homomorphic encryptions

Homomorphic encryption is the conversion of data into ciphertext that can be analyzed and worked with as if it were still in its original form. Homomorphic encryptions allow complex mathematical operations to be performed on encrypted data without compromising the encryption. In mathematics, homomorphic describes the transformation of one data set into another while preserving relationships between elements in both sets. The term is derived from the Greek words for "same structure." Because the data in a homomorphic encryption scheme retains the same structure, identical mathematical operations - whether they are performed on encrypted or decrypted data - will yield equivalent results.

Cyberattack could cost $120 billion: Lloyd's

Source: http://www.homelandsecuritynewswire.com/dr20170717-cyberattack-could-cost-120-billion-lloyd-s

July 17 – **Insurance giant Lloyd's of London has warned that the cost of a serious cyberattack to the global economy could reach $120 billion or more – which was the cost of damage inflicted by Hurricanes Katrina or Sandy.**

The 56-page report from the world's oldest insurance firm says the threat posed by global cyberattacks has spiraled, and that it poses a huge risk over the next decade to business and governments everywhere.

The report says that the most likely cyberattack scenario is a hack which manages to shut down a cloud service provider. The insurer estimates the losses resulting from such an attack to be $53 billion. This is the average estimate. There are uncertainties involved in calculating cyber losses, so Lloyd's provides a range of possible losses — as high as $121 billion or as low as $15 billion.

The *Guardian* notes that if the losses are around the upper end, they would exceed the damage cvasued by Hurricane Katrina in 2005, estimated at $108 billion (including $80 billion of insured losses). Hurricane Sandy in 2012 is estimated to have caused economic losses of $50 billion to $70 billion.

Inga Beale, chief executive of Lloyd's, said: "This report gives a real sense of the scale of damage a cyber-attack could cause the global economy. Just like some of the worst natural catastrophes, cyber events can cause a severe impact on businesses and economies, trigger multiple claims and dramatically increase insurers' claims costs.

"Underwriters need to consider cyber cover in this way and ensure that premium calculations keep pace with the cyber-threat reality," she said.

The second-most likely threat scenario involves attacks on computer operating systems, which are operated by a large number of businesses around the world. Such an attack could result in losses of up to $28.7 billion (the report calls this the "mass software vulnerability scenario").
Lloyd's notes that the majority of these losses are not insured, leaving governments and businesses vulnerable. The uninsured gap could be as high as $45 billion for the cloud services scenario, and $26bn for the mass vulnerability scenario, Lloyd's says.
Trevor Maynard, Lloyd's head of innovation and co-author of the report with the cybersecurity firm Cyence, said the global cyberattack in May "showed us that these sorts of attacks are absolutely possible."
Financial services are most at risk, followed by software and technology, hospitality, retail, and healthcare.
Cyber cover is a relatively new type of insurance. The field has grown over the last few years, and Lloyds's accounts for about a quarter of global cyber insurance premiums.
The firm's analysts say that it is much more difficult to model and understand the cover and costs of cyberattacks than the cover and costs of natural catastrophe.
Where people are involved, risk changes quite rapidly, Maynard said, from cyberattacks to terrorism and political risk. Climate change, however, remains the biggest challenge in the long run.
"From year to year, risk varies relatively little but climate change in the end will be far larger as a risk," he said. "It affects the global economic structure, food, water. [It's like] trying to turn a supertanker around – we can't start in thirty years when things are going bad, we have to start now."

— Read more in Counting the cost: Cyber exposure decoded (Lloyd's of London, 10 July 2017).

Why has healthcare become such a target for cyber-attackers?

By Myrsini Athinaiou
Source: http://www.homelandsecuritynewswire.com/dr20170720-why-has-healthcare-become-such-a-target-for-cyberattackers

July 20 – More than 16m patient records were stolen from healthcare organizations in the United States and related parties in 2016. That year, healthcare was the fifth most targeted industry when it came to cyber-attacks. And earlier this year, Britain's National Health Service was crippled by a ransomware attack that locked up the computers holding many of its records and booking systems.

But it's not just health data and services that are at risk from cyber-attacks – it's also human lives. In 2007, the then US vice-president, Dick Cheney, had his implanted heart defibrillator modified in order to avoid "death by hacking", a technology weakness that US officials warned of again just recently. Any medical device connected to a network is potentially at risk from being taken over and exploited by hackers, from MRI machines to electric wheelchairs.

As connected technology becomes even more embedded in healthcare, this cyber-threat is only likely to grow. But if we want to protect our health from cyber-attacks, we shouldn't fear technology. Instead, we need to understand it better and realize that the threat becomes much worse when people make simple mistakes.

What is the risk to healthcare?

The most common cyber-threats to healthcare are data theft attacks. They typically start from something like a phishing attack. For example, if you are a doctor with access to patients' records, an attacker may send you an e-mail and convince you to click a link or attachment that downloads a piece of software known as malware to your computer.

The attacker can then use this software to gain access to the organization's financial, administrative and clinical information systems. In the case of the recent "Wannacry" attack that affected the NHS, the malware (in this instance "ransomware") locked users out of their computers and demanded money to release them.

These attacks can also develop into "advanced persistent threats" against healthcare networks. These occur when malware enters a health network and remains there unnoticed while keeping in contact with the attacker. From there it can spread throughout the network, even if the original download is detected and removed. Then it can steal data and direct network traffic to the attacker so they can see exactly what is happening in the system in real time.

Attackers can also use the health network to spread into connected medical devices and equipment such as ventilators, X-ray machines and medical lasers. From here they can create a "back door" that will allow them to maintain access even if software is updated to improve security.

It's also possible that attackers could one day use artificial intelligence to mount more complex attacks. For example, hackers could use an intelligent system to block algorithms in the healthcare network that manage prescriptions or drug libraries and replace them with fakes.

Why is healthcare such a target?

Yet any organization with a computer is at risk from cyber-attacks and there are arguably far more obvious targets for those wanting to extort money. The recent attack on the NHS, for example, yielded very little ransom.

Part of the reason for the threat against the healthcare sector is that it is classed as national critical infrastructure, alongside water, electricity and transport networks. This makes it an attractive target for those hackers wanting to cause chaos, especially from a hostile foreign country. Attacking a healthcare organisation that is part of a wider network of infrastructure could also provide a way in to other critical facilities.

There are also a huge number of opportunities for attacks on healthcare systems simply due to the extent to which they rely on technology. **Healthcare today makes massive use of expensive technology, not just in computer systems and hospital equipment but also devices attached to and even embedded in the human body, such as fitness monitors or digital pacemakers.** There are also many ways in for a healthcare hacker, from data networks to mobile applications and even non-medical systems such as CCTV.

In particular, the spread of the Internet of Things, the connection of increasing numbers of devices and objects to the internet, is increasing the number of potential access points for hackers. Unlike many of the more trivial uses for the Internet of Things, connected medical devices have obvious benefits because they can instantly exchange useful data or instructions with medical staff. This is where some of the greatest dangers lie because the devices are often involved in critical procedures or treatments. Interference with the signals to a robotic surgical tool, for example, would be devastating.

How can we protect healthcare from attacks?

Most of the attacks against health systems fall under the category of missile attacks. They cannot spontaneously harm the attacker and leave limited traces, but can cause significant damage. This makes it very difficult to track down the attackers or predict future attacks.

But healthcare organizations have already become more aware of the danger they are in and started to take measures to protect themselves, for example by building cyber-security into their information technology strategies. At a delivery level, hospitals can establish new security standards and better ways to effectively integrate the new interconnected systems as they emerge.

But healthcare systems suffer from the same inherent problems as any technology. Even when a security team thinks is has a grip on a problem, another often appears. When one is solved, many more are often generated. What's more, they are designed by humans for humans, and so it's fair to assume they are vulnerable by default thanks to human error.

Although you can train staff as best you can, it only takes one person clicking on a rogue attachment to let in malware that can disrupt the whole system. What's more, the fear of legal costs and responsibilities might lead some organizations to under-report incidents and take action that could increase the threat, for example by paying ransoms to hackers. In reality, the reputation and trust of healthcare organizations depends on them understanding the true extent of the threat and taking sufficient measures to guard against it.

Myrsini Athinaiou is Ph.D. Student in Computing, Engineering and Mathematics, University of Brighton.

YouTube now redirects terrorism-related searches to anti-extremist content

Source: https://news.fastcompany.com/youtube-now-redirects-terrorism-related-searches-to-anti-extremist-content-4044090

July 21 – Google's video-sharing platform has begun redirecting users who enter specific terror- and hate-related keywords to a playlist of videos "debunking violent extremist recruiting narratives," reports *Variety*. **YouTube is using technology developed by Jigsaw, a think tank incubator in Google's parent company, Alphabet.** Right now YouTube has confirmed that a small number of specific hate- and terror-related queries will trigger the redirects, but over the next several weeks the breadth of those queries will expand to include more and in additional languages. YouTube is also using machine learning to dynamically update related search query terms.


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

Another impact of disaster

HUMAN TRAFFICKING

What Disaster Responders Need To Know

As a disaster responder and/or a healthcare provider, the likelihood that you will come in contact with a human trafficking victim is very high! Remember that anyone can be trafficked—men and boys, women and girls.

Disasters Increase the Risks of Human Trafficking

BEGINNING OF DISASTERS
- Disruption and chaos make it easy to exploit disaster survivors
- Perpetrators of trafficking may pose as responders offering survivors help with housing, food, or water

DURING DISASTERS
- Disaster survivors may engage in survival strategies that make them vulnerable to being taken advantage of
- Children may be separated, sometimes permanently, from their parents

AFTER DISASTERS
- Rebuilding and cleanup create new markets for cheap or free labor
- Disaster survivors may lose their main source of income and look for new types of work, including commercial sex

Recognize the Signs of Human Trafficking

LABOR TRAFFICKING
- Reports performing work duties in exchange for basic necessities (food, water, housing), rather than money
- Unable to freely choose where they live
- Identification documents are held by employer

SEX TRAFFICKING
- Reports providing sex in exchange for basic necessities (food, water, housing)
- Unexplainable injuries
- Reports being forced to engage in commercial sex
- Aged <18 and involved in commercial sex
- Reports unusually high number of sex partners

If you think someone may be a victim of human trafficking, call and/or encourage them to call the National Human Trafficking Hotline: (888) 373-7888 to receive help, resources, and information.

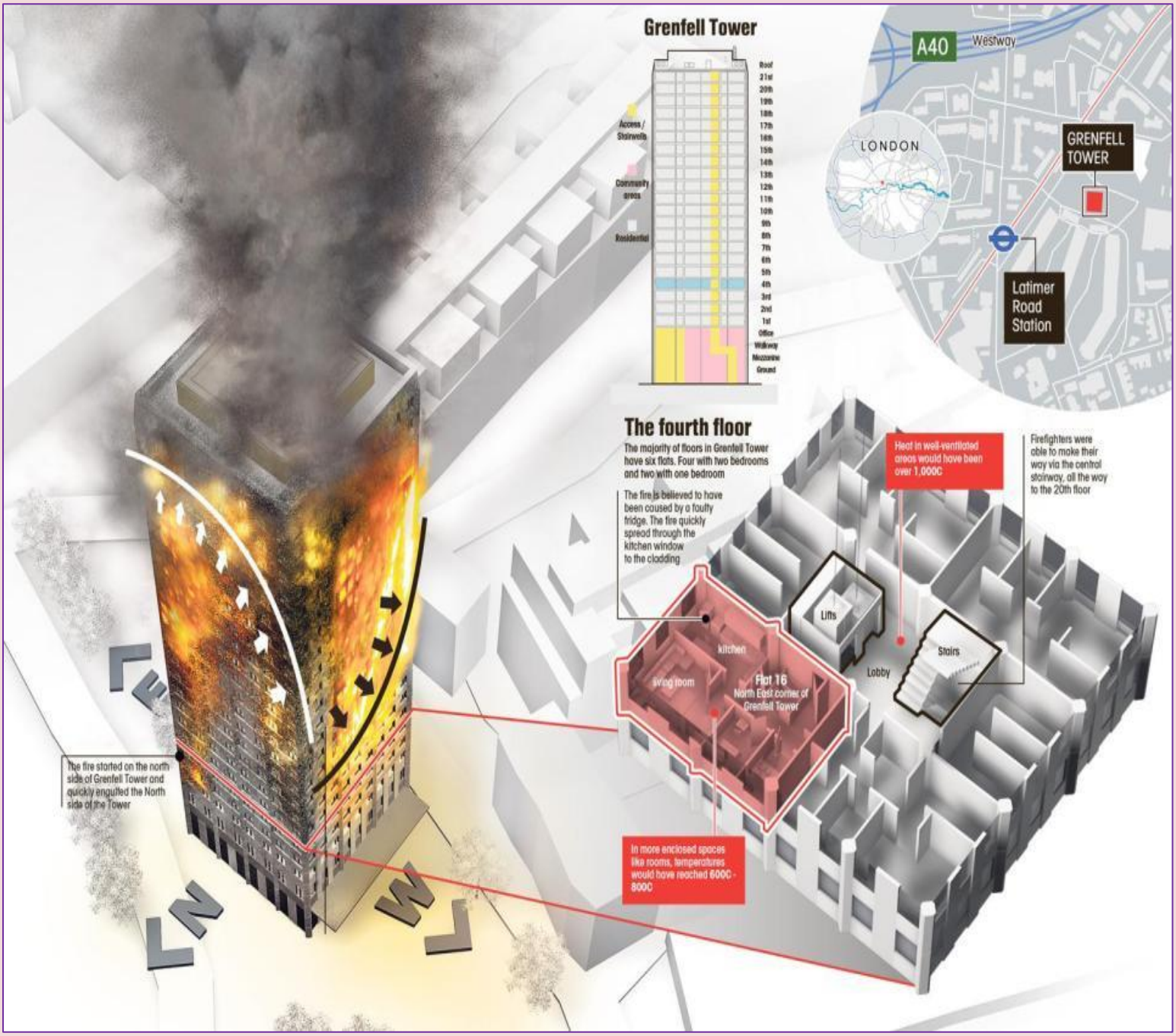
ASPR
ASSISTANT SECRETARY FOR PREPAREDNESS AND RESPONSE

Could a tragedy like the Grenfell Tower fire happen in the U.S.?

By Brian Meacham

Source: http://www.homelandsecuritynewswire.com/dr20170705-could-a-tragedy-like-the-grenfell-tower-fire-happen-in-the-u-s

July 05 – The Grenfell Tower fire in London has triggered questions about how the tragedy could have happened, whether it could happen elsewhere, and what might be learned from it to prevent future disasters. As a professor of fire protection engineering, I know that the answers are not simple, and the fixes not quick.



Investigations into what actually happened at Grenfell Tower are still ongoing. While some factors have been identified, completing the picture could take years. As details emerge, though, it may not be easy to translate them to other situations. Buildings differ widely, based on when each was constructed and any renovations or other modifications since. And then

there are the different rules, design concepts and construction practices that vary from country to country, and, in the U.S., sometimes from state to state.
The basic problem, however, is clear: The Grenfell Tower fire spread much faster and more intensely than anyone expected. From what we know so far, there are physical, cultural and legal reasons dozens of people died. Addressing each of them will help British authorities, and fire protection and fire prevention professionals around the world, improve their efforts to reduce the chance of future tragedies like the one at Grenfell Tower.

Structure
It appears that the main problem was the dangerously flammable cladding, the material covering the outside of the building – aluminum panels with foam insulation installed in a recent effort to improve the building's energy efficiency. Once the fire escaped the apartment where it began, reportedly in the refrigerator, and ignited the cladding, the rest of the building was primed to burn quickly.
Additional insulation underneath that cladding may have released poisonous fumes as it burned, overcoming residents who might otherwise have escaped the flames.
In addition, the building lacked an automatic fire-sprinkler system, and had only a single stairway to get out.

Culture
That lone stairway – and the fact that building occupants were reportedly told to remain in their apartments in case of fire – are the result of fire safety culture influencing emergency planning. In England and around the world, including the U.S., the historical approach has been to rely significantly on the fire resistance of the structure itself to contain the fire. We call this "passive" fire protection, and it largely involves using non-combustible materials to separate areas, limiting how far a fire can spread.
This concept has been used at least since the 1666 Great Fire of London, as a way to prevent city-wide conflagrations from developing when a blaze burning in one building catches the structure next door. The same principle is used within buildings, for example by requiring fire-resistant construction among apartments or offices on each floor, as well as between floors.
However, the concept only works when the initial fire is contained. That didn't happen at Grenfell Tower. Once the fire reached the external cladding, it spread rapidly. If the building's residents had their windows open for ventilation, the fire could have spread even faster: The heat just outside could have ignited drapes or other items near the windows.
With multiple fires burning simultaneously in different apartments on several floors, the situation would have been grim. There were no sprinklers to quench the flames. And the only stairway down for the building's occupants was also the only stairway up for firefighters coming to the rescue.
This situation was very similar to the confluence of problems in the 2001 World Trade Center disaster, when multiple fires burned across several floors simultaneously, the automatic sprinkler system was damaged, and some exit stairways were blocked. Occupants of the Twin Towers buildings and Grenfell Tower who were above the fires had few options – because they were not expected to need them. The regular fire safety plans didn't call for immediate evacuation, because the building's construction was supposed to keep a large fire from happening.

Rules
Those expectations about how structures will function in a fire inform the rules people make about how to protect occupants of a burning building. In most countries, including the U.S., the rules governing how buildings are constructed are enforced when a new structure is going up.
As we learn more over time about how to keep people safer, building codes change – but they usually apply just to new structures, not existing ones. The new codes can kick in if there's a major renovation or expansion project or the building's main use changes from, say, offices to apartments. That means many buildings aren't up to modern standards.
In addition, it takes time from when a model building code is published, to when it becomes adopted into legislation. As such, even a building constructed in 1997, if it hadn't been significantly renovated, may not have to comply with new provisions introduced in the 20 years since.

There are some exceptions. Many parts of the U.S. required building owners to install automatic sprinkler systems in existing high-rise buildings in the wake of the 1980 MGM Grand Hotel fire in Las Vegas. A similar requirement in the U.K. didn't take effect until 2007; existing buildings are not covered unless a specific risk assessment recommends otherwise.

Could it happen here?

There have been many exterior-cladding fires in high-rise buildings around the world, including in Australia, the Middle East and here in the U.S. In September 2007, the Water Club tower at the Borgata Casino hotel in Atlantic City, New Jersey, caught fire. The building was under construction at the time, so it was largely unoccupied. And there was a concrete wall separating the burning cladding from the rest of the building.

In the U.S., most fire codes limit the use of combustible exterior cladding material, particularly on high-rise buildings. The requirements for automatic sprinklers (one element of what we call "active" fire protection systems) and at least two escape routes from every floor add depth to these defenses. Together, these rules increase the chance that a small fire will be put out quickly, reduce its ability to spread up the side of the building, and help people get out if they need to.

Several other Grenfell Tower-like buildings have already been identified in the U.K. These high-rises have combustible cladding or insulation, either permitted at the time of construction or perhaps added during a retrofit. Some of those buildings may not have sprinklers, either. The thousands of residents of those buildings have already been evacuated to prevent a repeat disaster.

But at least in the U.S., most will have both sprinklers and multiple escape routes. So while another tragic event like the Grenfell Tower fire is possible, we can hope that building owners and fire protection experts alike will learn from this disaster and work even harder to prevent it from happening again.

Brian Meacham *is Associate Professor of Fire Protection Engineering, Worcester Polytechnic Institute.*

The How and the Why of Crowd Management

By Stephen Maloney

Source: https://www.domesticpreparedness.com/preparedness/the-how-and-the-why-of-crowd-management/

Mar 13 – On a Saturday night in 2013, a fire broke out in a nightclub in Sao Paulo, Brazil. More than 240 people, mostly college students, were killed. Two years later, two people were killed and more than 70 injured in a stampede to exit a club in Malta, due to a possible

gas leak. Although the immediate causes of the two incidents were different, a common factor that led to so many dead and injured was poor management of large groups.
Fire and crowd-crush incidents resulting in mass casualties, with a contributing factor of poor crowd management, continue to be relatively common worldwide. The United States began to seriously address the issue after a pair of tragedies in 2003.

Triggers for Stronger Regulation
On 17 February 2003, the E2 nightclub in Chicago, Illinois, should not have been open. Despite being forbidden to operate until 11 structural and fire code violations were remediated, more than 1,000 people were inside the club that night. Sometime around 2 a.m., security officers sprayed a chemical irritant to break up a fight, and 21 people were killed in the ensuing efforts to flee from the contaminated air and exit the club.
Three days later, more than 200 people gathered at the Station nightclub in Rhode Island to listen to several bands. Shortly after 11 p.m., and seconds after the headlining act began to play, pyrotechnic special effects devices ignited wall materials around the stage. The entire building was involved in fire within about five minutes, and 100 people died, having been unable to exit the club in time.
These back-to-back disasters led the National Fire Protection Association (NFPA) to call an emergency meeting of its Technical Committee on Assembly Occupancies in July 2003. Later that month, the NFPA Standards Council issued new interim requirements, known as the Tentative Interim Amendments (TIAs). Included in the TIAs was a dramatic decrease in the threshold requiring trained crowd managers in assembly occupancies from the original occupant load threshold of greater than 1,000 occupants down to the revised load of greater than 49. In 2006, the TIAs became permanent provisions of NFPA 101®: Life Safety Code®, NFPA 5000®: Building Construction and Safety Code®, and NFPA 1®: Uniform Fire Code®. Several states adopted the TIAs within months of being issued.

Crowd Management
In most cases, a trained crowd manager is now required to be present during any assembly of 50 or more people. Additional crowd managers are required for every 250 people. Crowd management is not just about knowing and managing the facility's occupant load. The crowd managers must complete certain tasks both before and during an event. Some examples are listed below:

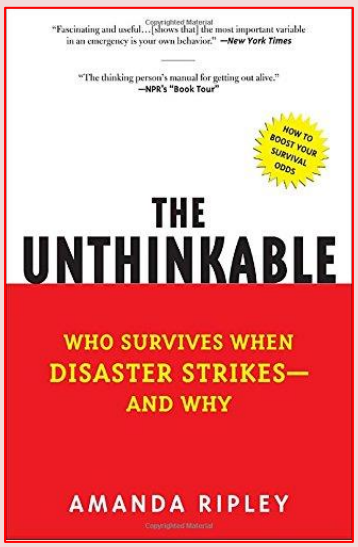
- Ensure exits are marked, exit doors are operational, and all egress paths are unobstructed.
- Ensure fire alarms, sprinkler systems, and emergency lighting are operational.
- Ensure fire lanes are unobstructed.
- Put in place an emergency notification plan, including how people will be notified and who will deliver the message.
- Ensure aisles and other exit routes remain clear throughout the event.

Implementation at a College
Montgomery College is a community college located in Maryland, just outside of Washington, D.C. With three campuses and more than 30,000 students and 3,000 employees,

Montgomery College hosts countless assemblies where crowd management is necessary. In 2011, the college implemented a formal Crowd Management Program. This involved identifying spaces where the crowd manager standard potentially would apply, identifying staff requiring training, developing a training plan, and developing a checklist for trained crowd managers to follow both before and during an event. Montgomery College chose to require its crowd managers complete the Maryland State Fire Marshal's Online Crowd Manager Training. This program was chosen because it was the only class mentioned by NFPA as meeting the training requirement, it was comprehensive, it was free of charge (until 2014), it was short (about 30 minutes, until 2014), and it included the powerful Station nightclub fire footage. That video served to demonstrate the tremendous value of including context in training, rather than simply stating a requirement.

The Power of Why

In "The Unthinkable," investigative journalist Amanda Ripley's groundbreaking study of how people respond to disaster, the author pointed out the value of explaining why it is important to follow particular safety instructions, not just stating they should be followed. She argued that, rather than simply telling airline passengers they should put their own oxygen masks on before helping others or that they should inflate their life vests only after exiting the plane, they should be told why they should do those things. If told that they would lose consciousness in seconds during a rapid decompression and be unable to help their children or that inflating a life vest inside the plane could prevent them from swimming out of the plane and surviving, the warnings become motivators to remember and comply.



At Montgomery College, the new training requirement for people not normally involved in emergency response was enthusiastically received by staff. The simple, but dramatic and moving Station video made believers and vocal program advocates of the events management staff. It clearly demonstrated the long-term value of explaining the "why" in addition to the "what."

Recommendations

Many organizations are still unaware that they are required to use trained crowd managers for events involving 50 or more people. Even competent occupational safety and fire protection professionals may not be aware of this requirement. **Any emergency manager or safety professional in an organization that could potentially host an event with 50 or more people should consider taking the following actions:**

- Become versed in the NFPA Crowd Manager requirements (NFPA 101®: Life Safety Code®, Sections 12.7.6.1/13.7.6.1) and the requirement of the local agency having jurisdiction. Some jurisdictions have different thresholds, and they may allow for changes in the requirements based on the nature of the event or whether or not a building is fully sprinklered.
- Identify potential spaces and events where crowd management requirements would apply.
- Identify or develop a simple training program and a checklist to be used by crowd managers.
- Present the problem and its solution to leadership only after having completed the simple steps above. It is possible to obtain rapid buy-in after already having done the homework. Show that the requirement is not optional, that it only applies to particular spaces and events, that related training is short, that training applies to only select staff (renewed every three years), and that compliance is as easy as following a basic checklist.
- Ensure the Station nightclub fire video is part of the training product, whether that product is developed in-house or not. This simple step creates allies and helps ensure a self-sustaining program.

Conclusion

Incidents with great loss of life due to overcrowding or inadequately informing a crowd of their egress options are numerous. Efforts of the NFPA and state and local jurisdictions have resulted in an effective and easily implemented standard for managing the problem. By following Montgomery College's example of gaining leadership buy-in (by demonstrating the very limited increases in cost and on staff training and workload) and ensuring program

sustainability (by gaining a cadre of supporters simply by teaching the "why" along with the "what"), an organization can prevent fire and crowd crush tragedies relatively painlessly.
Additionally, good crowd management does not just address fire hazards. An effective program also increases an organization's readiness for the armed intruder or other no-warning threats. Having trained people and processes in place for rapid dissemination of specific instructions is a critical element in preventing and mitigating against a variety of potential tragedies.

Stephen Maloney, *CEM, is an emergency manager with the U.S. Federal Reserve Board. He has a B.S. in geology from the University of Maryland, an M.S. in environmental science and policy from Johns Hopkins University, and is a graduate of the National Emergency Management Executive Academy and Harvard University's National Preparedness Leadership Initiative.*

Protecting Water as a Lifeline in Disaster

By Mary Lasky and William Harris
Source: http://www.domesticpreparedness.com/preparedness/protecting-water-as-a-lifeline-in-disaster/

May 17 – Water is vital to life. Water and wastewater are taken for granted, with people believing that the faucet will turn on and the toilet will flush – that is, until a disaster. To ensure access to critical resources such as water when needed the most requires understanding the scale and scope of the problem, identifying ways to preserve such lifeline services, and strategizing to best allocate these resources during both disaster and non-disaster times.
As the lack of electrical power continued for days, Hurricane Sandy in 2012 provided many lessons learned. Generators started to break down because most emergency generators are not designed for continuous use for days or weeks. Competition for generators increased as the outage continued. Many generators ran out of fuel and too many, even for hospitals, were located in basements subject to flooding. Some emergency managers did not understand the need for the water sector to have generators. And, according to the Electric Infrastructure Security Council's E-Pro® Handbook II, fuel transport companies needed emergency credits when their customers could not pay for fuel deliveries.
Understanding the Scale & Scope of the Problem
In the eight hardest-hit states, about 11 billion gallons of untreated and partially treated sewage (including 3.45 billion gallons of raw sewage) flowed into rivers, bays, canals, and, in some cases, city streets. Downstream water treatment plants were designed for normal raw water sources, but not these heavily contaminated sources. Additionally, citizens attempting to use such contaminated surface water sources as potable water or to create potable water faced health risks akin to those in third world nations. The American Water Works Association (AWWA), in its 2013 after action report on Hurricane Sandy, stated that giving the water/wastewater sector priority for generators and fuel during power outages is important. Many of the water utilities have found it too risky and too costly to obtain generators "just-in-time" after a disaster, in lieu of owning them. Unfortunately, obtaining "just-in-time" generators may not be possible in disasters such as hurricanes and less feasible if there were long-term, widespread electric power outages caused by threats to the power grid such as a cyberattack, physical attack, solar storm, or electromagnetic pulse. Another issue is that

there are a limited number of emergency generators. For example, the Federal Emergency Management Agency (FEMA) has 400 generators for its 10 regions. The U.S. Army Corps of Engineers has 25 locations with 30 generators each, primarily reserved for Defense Department requirements. To put these numbers in perspective, there are 160,000 water/wastewater systems. In addition, there is a challenge to allocate skilled people capable of installing the generators and handling the logistics of getting the equipment and fuel stocks to the right locations (see the "Limited Supplies of Emergency Power Generators" section in the E-Pro Handbook II).

Critical infrastructure is greatly dependent upon water, and water is dependent on electric power. *Powering Through: From Fragile Infrastructure to Community Resilience* examined the July 2016 National Infrastructure Advisory Council (NIAC) Report on Water Sector Resilience (see Figure 1). The NIAC report:

provides an excellent illustration of how tightly coupled modern civilization is to modern water delivery systems. It clearly illustrates that every category of water user surveyed will experience significantly degraded capabilities after 8 hours without water. Thus, even if they have emergency generators that can provide on-site power for an extended period, they are degraded nonetheless by a lack of water. Additionally, should the water utilities have electric power, they maintain a limited quantity of treatment chemicals on site, and chemical supply chains depend upon electricity. Catastrophic loss of potable water has many consequences to include degrading or eliminating much of healthcare capacity both in hospitals, and via first responders. The NIAC Report on the Water Sector indicates that hospital capabilities may be degraded by 67% to 99% within just two hours of loss of water services. Emergency replacement of healthcare facilities relies on nearby facilities being operable. This is not a feasible planning consideration in the event of an extended regional or larger-scale loss of electrical power and corresponding loss of water and wastewater utilities. (See p. 27 of Powering Through)

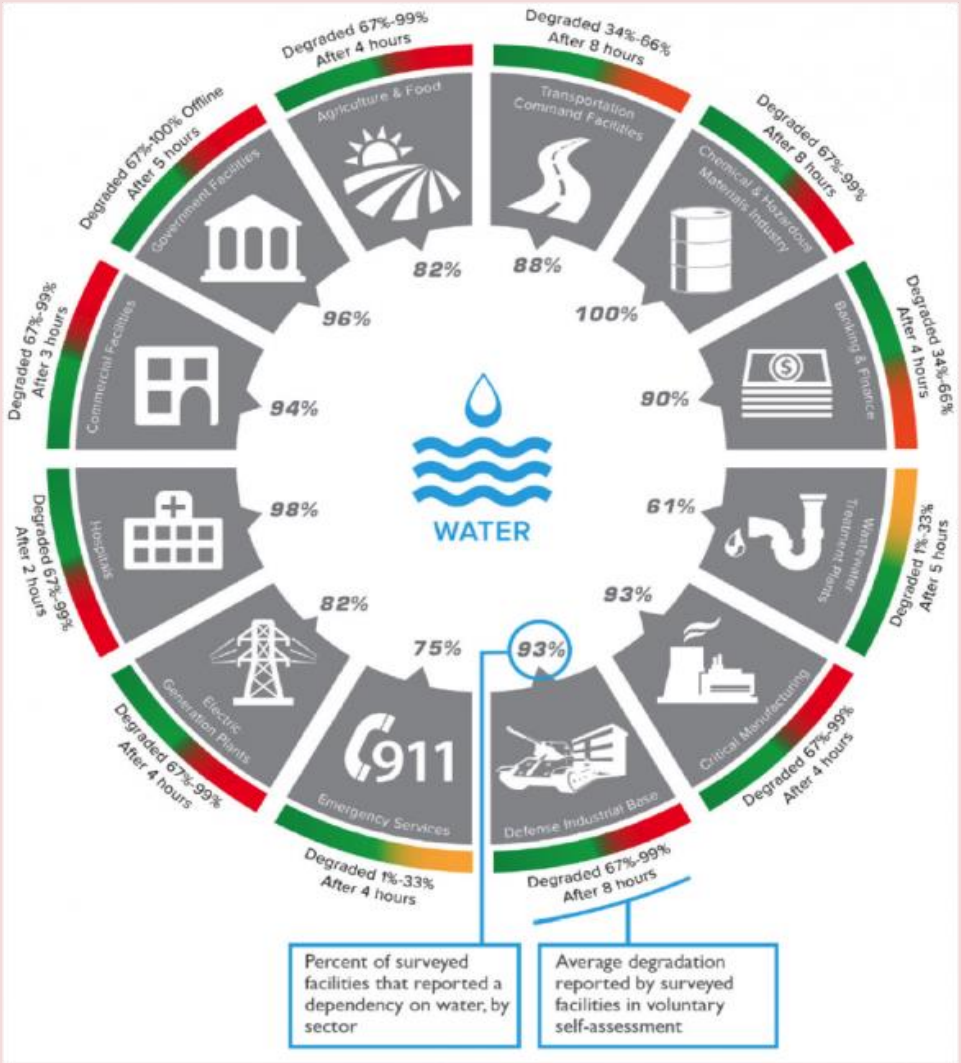


Fig. 1. National Infrastructure Advisory Council (NIAC) critical infrastructure dependence on water and potential function degradation following loss of water services (*Source:* NIAC, July 2016).

Identifying Ways to Preserve Lifeline Services

One of the goals during a long-term power regional or national outage would be to keep people in their homes where they are safer than becoming stranded attempting travel elsewhere. In a severe power outage that is wide spread, there would be no place for the population to flee because no reachable destination would have power. If water and wastewater are available, people

are more likely to remain in their homes. Without water, there could be a "tipping point" beyond which lives will be lost. Then FEMA Administrator Craig Fugate has remarked that loss of water service threatens lives and urges, "Keep the water on" (see 2015 Koppel article). Ideally, the highest priority for generators, fuel, chemical distribution, and maintenance materials would be the water/wastewater systems.

As mentioned in *Powering Through*, uncoordinated and unplanned self-evacuations are contraindicated. The Three Mile Island (TMI) Nuclear Incident of March 1979 showed that self-evacuation was not beneficial and caused prolonged congestion of transportation systems and fuel shortages. Between March 28 and April 4 of that year, an estimated 144,000 regional residents self-evacuated from the area surrounding the power plant. Within the 20-mile radius of TMI, the residential population was about 600,000; so roughly one-quarter of the population evacuated, mainly before official instructions were broadcast. *Powering Through* stated, "Since that incident, the Nuclear Regulatory Commission has mandated installation and monitoring of radiological sensors within designated evacuation zones of licensed nuclear power plants, in part to avert rumor-based evacuations that congest and undermine recovery capabilities."

Ted Koppel explored the real or potential contradictions among federal policies to prepare for and to recover from a long-term grid blackout in his book, *Lights Out* (2015). He wrote, "In the case of a power grid going down urging people to stay in their homes may be exactly the right thing to do . . . leaving routes open for resupply convoys."

For a long-term electric grid outage, relying on "shelter in place" as the preferred policy to the maximum extent feasible has multiple advantages, including conservation of scarce fuel, prioritizing uses of transportation routes, preserving law and order, and benefitting from community networking by those in their own neighborhoods. Others, such as the EPRO® Black Sky Systems Engineering Process, share this preference for "shelter in place" outcomes. A preferential policy to shelter in place depends on the resilience of "lifeline services" such as pre-positioned food, restoration of water and wastewater services, essential transportation, and communications. The former FEMA administrator, Craig Fugate, in 2015 expressed concern about the advisability of mass evacuations for long-duration disasters. The government, he noted in Koppel's *Lights Out*, "Can't move 'em fast enough." And Koppel replied, "anyway where are you going to move them?"

Strategizing for Re-Allocation of Resources

In managing the water supply, a water mitigation strategy could aim at providing just enough water to sustain most of the population without fully energizing the water system. Typically, when communities are without power, the demand on water is reduced because people and businesses are not running water-intensive appliances, such as washing machines and dishwashers. Utilities could also define the level of service goals for long-term emergencies – for example, water quantity and quality.

One possible level of service goal might be average winter daily demand since this is typically significantly lower than water demand during other times of the year. Emergency response plans/playbooks ideally would reflect these reduced levels of service goals. For example, if water and wastewater systems were re-engineered to provide just 20% of capacity, recoverable within 24 hours, one could sustain wastewater system pressure and support emergency water rationing. The huge waste of water under normal conditions could serve as a cushion for emergencies. It would also be best to maintain water pressure even if the water cannot be properly treated for human consumption. This would allow for delivery of water to each residence where it could be boiled or otherwise decontaminated, and also provide water for firefighting (see p. 150 of E-Pro Handbook II).

Additional information about emergency water supply preparation, sanitation, and hygiene can be found at the Centers for Disease Control and Prevention's website. In conclusion, keeping water and wastewater facilities operational during disasters is critical and needs to be a high priority. Citizens could be prepared using CDC guidelines and having supplies and water filters in households and businesses.

***Mary Lasky**, a Certified Business Continuity Professional (CBCP), serves as the program manager for business continuity planning for the Johns Hopkins University Applied Physics Laboratory (JHU/APL), where she coordinated the APL Incident Command System Team. She also as a member of: InfraGard, where she is the vice chair for the InfraGard EMP-SIG. In Howard County, Maryland, she served as: president of the Community Emergency Response Network Inc. (CERN); president of the board of directors of Grassroots Crisis Intervention*

Center; and for Leadership Howard County is co-chair of the Steering Committee for the Leadership Premier Program. For many years, she has been on the adjunct faculty of the Johns Hopkins University Whiting School of Engineering. She is the immediate past president of the Central Maryland Chapter of the Association of Contingency Planners (ACP) and has held a variety of supervisory positions in information technology and in business services. Her consulting work has included helping nonprofit organizations create and implement their business continuity plans.
***William R. Harris** is a senior advisor to the congressionally mandated EMP Commission since January 2017. He serves on the board of directors, and is the secretary of the Foundation for Resilient Societies, a New Hampshire-based nonprofit engaged in research and education on critical infrastructure protection. He is an international lawyer (Harvard, J.D., 1966) and former energy, nuclear non-proliferation, environmental, and national security project manager at the RAND Corporation. Working with physicists and engineers, he supports electric and other critical infrastructure "reliability standard" development for international, federal, and state institutions.*

Significant contribution to this article was provided by:
***Stephen Volandt,** who is vice president of Auroros Inc., a contracting and management-consulting firm based in Raleigh, North Carolina. He specializes in successfully connecting strategic purpose, risk management, decision-making, enterprise project portfolio management, operational user requirements, and the technology that supports them. He co-authored the DoD CIO Executive board governance charter. Mr. Volandt served as the lead architect for transforming the multi-billion-dollar United States Marine Corps business enterprise to better support combat operations and readiness cycles. He provided policy, operations modeling, IT and communications modeling, planning, and budget justification for a global U.S. Army weapon of mass destruction response capability; and was a principal operations planner and architect for joint U.S. Army and National Guard response to smuggled nuclear weapon ground burst terrorism in the homeland. He is a former U.S. Marine Corps. He graduated from The Citadel. He is the 2nd vice president for the Eastern North Carolina InfraGard Chapter, as the deputy director, InfraGard SE Region EMP-SIG, and as the National InfraGard EMP-SIG administrative officer. He authored the exercise scenario, exercise process, provided the maturity model for the 2015 EMP SIG annual workshop and conference. His current passion is the design, funding, and creation of resilient communities.*

Lessons for first responders on the front lines of terrorism

By Mahshid Abir and Christopher Nelson
Source: http://www.homelandsecuritynewswire.com/dr20170710-lessons-for-first-responders-on-the-front-lines-of-terrorism

July 10 – Acts of terrorism are on the rise globally. Over the past several weeks alone, the world has seen stabbings, shootings and bombings in Flint, Tehran, London, Kabul and Bogota.
We've spent the past several years researching how communities can prepare to provide urgent medical care to the large numbers of victims these events produce.
Given the persistent risk of terrorist attacks and large-scale accidents, it's more critical than ever to learn from past incidents. That will ensure that first responders can work together effectively during the chaotic but critical minutes and hours after an incident.

Better coordination
Televised images of attack or disaster scenes often show patients being treated and transported by paramedics. Hours later, hospital press conferences often recount the heroic efforts of emergency physicians, trauma surgeons and nurses to minimize loss of life and limb.
But equally important are the actions of nonmedical first responders. Police, firefighters and even bystanders compress wounds, apply tourniquets or drive casualties to hospitals.
In the Boston marathon bombing, for instance, 264 victims transported to local hospitals survived, despite many serious injuries. This was credited not only to excellent triage, transport and care by medically trained paramedics, EMS and hospital staff, but also to immediate lifesaving actions by police and bystanders.
However, things do not always go so well. In the often chaotic post-incident scene, it can be difficult to coordinate the efforts of multiple response agencies and bystanders. Even as EMS personnel triage and transfer victims, law enforcement needs to maintain security, preserve

evidence and locate potential perpetrators. That makes it challenging to manage access to and traffic around the scene.
For instance, an Orlando Police Department report on the Pulse nightclub attack cited the need for improved communication and coordination between the police and fire departments responding to the incident. While such problems do not always affect how many lives are saved, they can slow down the overall response.
Even when well-coordinated, those not trained in post-disaster casualty triage can unintentionally cause problems. They might transfer patients to hospitals that lack the resources needed to treat them, or transfer them in vehicles that lack critical life-support equipment, such as IVs or oxygen.
What's more, unforeseen events such as poor weather or volume-related cell tower outages can create additional challenges.

Preparing for the next attack

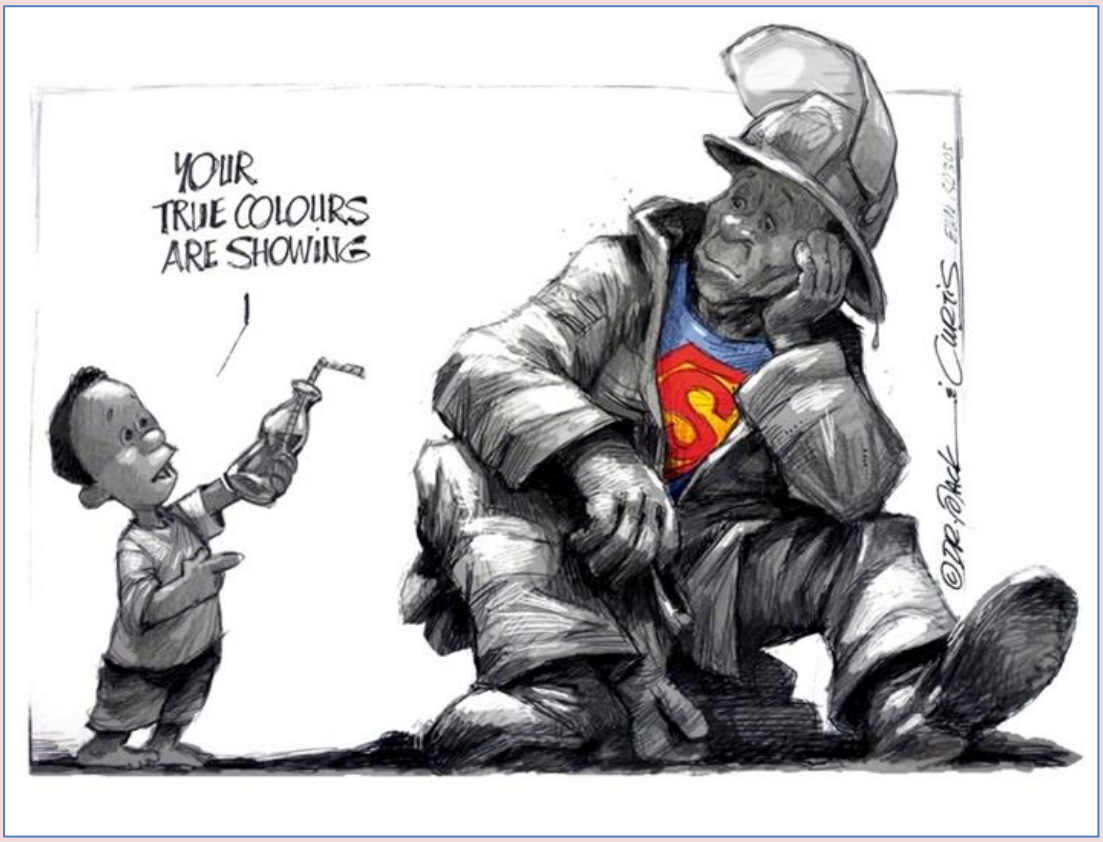
Our recent research looked at three mass casualty incidents in the U.S. between 2013 and 2015, examining both the health care system and community responses.
We identified several best practices that can help medical and nonmedical first responders handle these incidents more effectively.
First, we must provide co-training for medical and nonmedical first responders. Police and firefighters are already starting to be trained in basic lifesaving skills in non-mass casualty incident contexts. In some communities, such as Atlanta and Irvine, California, police patrols carry automated electronic defibrillator devices as well as Narcan to reverse opioid overdose. Other police departments, such as in Denver, provide staff training in tourniquet application. These efforts should be continued.
Moreover, both medical and nonmedical responders should be trained in scene safety, bystander management, field triage and medical techniques such as effective application of tourniquets. Even many medical professionals lack sufficient training in these skills.
Second, we need to ensure open communication lines. A dedicated radio frequency can facilitate communication among the various responder disciplines, as well as guard against problems caused by cell tower outages. Also, responders can be trained to rely, when necessary, on text messaging, which worked when voice communication did not during the events we studied.
Third, interdisciplinary disaster drills are critical. Communities should conduct regular citywide disaster drills that include EMS, fire and police departments, as well as area hospitals and health care systems. Responders need to test their training and protocols under conditions that simulate some of the complexity and stress of real events. This could include adding components without notice, to simulate the sudden onset of terrorist events.
Such drills will help each group understand how its actions contribute to an integrated multidisciplinary response. They can also promote more effective collaboration during response to an incident.
Finally, we need to build relationships in advance that can be leveraged during emergencies. Our research indicates that one of the most important ingredients of an effective multidisciplinary medical response is strong relationships and trust among key players. Regular exercises and drills can help, but they need to be supported by leaders and organizational cultures.
For example, in recent years, with support from the federal government, many communities across the U.S. have created health care coalitions that provide formal mechanisms – including regular multi-stakeholder meetings and agreements to share critical resources – for coordinating the preparedness and response efforts of first responders, health care providers and private sector partners.
Moreover, given the frequent role of bystanders, professional responders should reach out to community emergency response teams and other organizations. That can help raise citizen awareness of basic lifesaving techniques.

Public support

Effective medical response to terrorism and disasters requires sustained investment. That can be difficult to muster in an era marked by increasing skepticism about public investment and distrust in public institutions.
However, experience suggests that we need collaboration among medical and nonmedical response organizations – and civilians. Through supporting public investments in mass casualty incident preparedness and response, both policymakers and civilians should have

the confidence that, even when attacks cannot be prevented, their communities are resilient enough to respond to and recover from them.

Mahshid Abir *is Assistant Professor, Department of Emergency Medicine, Director of the Acute Care Research Unit, Affiliated Adjunct and Natural Scientist, RAND Corporation, University of Michigan.*
Christopher Nelson *is Professor of Policy Analysis, Pardee RAND Graduate School.*




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

Rising seas could create 2 billion refugees by 2100

Source: http://www.homelandsecuritynewswire.com/dr20170627-rising-seas-could-create-2-billion-refugees-by-2100

June 27 – **In the year 2100, 2 billion people – about one-fifth of the world's population – could become climate change refugees due to rising ocean levels.** Those who once lived on coastlines will face displacement and resettlement bottlenecks as they seek habitable places inland, according to Cornell University research.

"We're going to have more people on less land and sooner that we think," said lead author Charles Geisler, professor emeritus of development sociology at Cornell. "The future rise in global mean sea level probably won't be gradual. Yet few policy makers are taking stock of the significant barriers to entry that coastal climate refugees, like other refugees, will encounter when they migrate to higher ground."

Cornell says that Earth's escalating population is expected to top 9 billion people by 2050 and climb to 11 billion people by 2100, according to a United Nations report. Feeding that population will require more arable land even as swelling oceans consume fertile coastal zones and river deltas, driving people to seek new places to dwell.

By 2060, about 1.4 billion people could be climate change refugees, according to the paper. Geisler extrapolated that number to 2 billion by 2100.

"The colliding forces of human fertility, submerging coastal zones, residential retreat, and impediments to inland resettlement is a huge problem. We offer preliminary estimates of the lands unlikely to support new waves of climate refugees due to the residues of war, exhausted natural resources, declining net primary productivity, desertification, urban sprawl, land concentration, 'paving the planet' with roads and greenhouse gas storage zones offsetting permafrost melt," Geisler said.

The paper describes tangible solutions and proactive adaptations in places like Florida and China, which coordinate coastal and interior land-use policies in anticipation of weather-induced population shifts.

Florida has the second-longest coastline in the United States, and its state and local officials have planned for a coastal exodus, Geisler said, in the state's Comprehensive Planning Act.

Beyond sea level rise, low-elevation coastal zones in many countries face intensifying storm surges that will push sea water further inland. **Historically, humans have spent considerable effort reclaiming land from oceans, but now live with the opposite – the oceans reclaiming terrestrial spaces on the planet,"** said Geisler. In their research, Geisler and Currens explore a worst-case scenario for the present century.

The authors note that the competition of reduced space that they foresee will induce land-use trade-offs and conflicts. In the United States and elsewhere, this could mean selling off public lands for human settlement.

"The pressure is on us to contain greenhouse gas emissions at present levels. It's the best 'future proofing' against climate change, sea level rise and the catastrophic consequences likely to play out on coasts, as well as inland in the future," said Geisler.

— Read more in Charles Geisler and Ben Currens, "Impediments to inland resettlement under conditions of accelerated sea level rise," Land Use Policy 66 (July 2017): 322-30.

Drones Needed in Asymmetric War

Source: http://i-hls.com/archives/77420?

July 06 – Turkey's military and procurement officials are increasingly relying on various drone systems, most notably to boost the country's asymmetrical fight against Kurdish insurgents and hostile Islamic groups fighting in the Syrian civil war.

Defensenews.com cites a military official who said that the local unmanned aerial vehicle capabilities have since 2015 yielded "wonderful results" in fighting the PKK, an insurgency group outlawed by Turkey, the United States and European Union.

A procurement official confirmed: "There is increasing appetite from the end user (the military) for drone systems and subsystems. The next years will see even larger demand for drones and related capabilities."

At the end of June, Turkey's procurement office, the Undersecretariat for Defense Industries, or SSM, released a request for information for a new program for the purchase of a drone system with aerial photography capabilities. SSM said the competition would be open to local producers only. Another request for info released by SSM referred to the acquisition of a ship-based vertical take-off and landing drone system.

"The latter program confirms that Turkey's drone requirements are not limited to asymmetrical land warfare only," said one industry source.

The local industry is thriving to cope with the demand. Six armed drones were delivered to the Turkish military. Turkey tested the Bayraktar last year. The drone successfully hit a target at the Konya fire test field in central Anatolia from a distance of eight kilometers. The Bayraktar uses two mini smart munitions developed and produced by Roketsan, the state-controlled missile maker. Roketsan's mini systems weigh 22.5 kilograms, including a 10-kilogram warhead.

Turkey's local industry also is developing BSI-101, a SIGINT system, for the Bayraktar to end Turkey's dependence on U.S.-made SIGINT systems for drones.

The Bayraktar can fly at a maximum altitude of 24,000 feet. Its communications range is 150 kilometers. The aircraft can carry up to 55 kilograms of payload.

In June, Meteksan Savunma, a privately owned Turkish defense company, said it successfully developed the country's first indigenous automatic takeoff and landing, or ATOL, system for drones.

The company said the system, OKIS in its Turkish acronym, aims to replace imported ATOL systems currently used in Turkish-made drones. The radar-based, portable OKIS system features two main components: a transponder and antenna on the platform and a ground radar system designed to ensure safe takeoff and landing.

Identifying global hotspots for water conflict

Source: https://www.sciencedaily.com/releases/2017/07/170717160048.htm

July 19 – **More than 1,400 new dams or water diversion projects are planned or already under construction and many of them are on rivers flowing through multiple nations, fueling the potential for increased water conflict between some countries.**

A new analysis commissioned by the United Nations uses a comprehensive combination of social, economic, political and environmental factors to identify areas around the world most at-risk for "hydro-political" strife. This river basins study was part of the UN's Transboundary Waters Assessment Program. Researchers from the United States, Spain and Chile took part in the analysis, which has been recommended by the U.N. Economic Commission for Europe as an indicator for the U.N.'s sustainable development goals for water cooperation.

Results of the study have just been published in the journal *Global Environmental Change*. OSU says that the analysis suggests that risks for conflict are projected to increase over the next 15 to 30 years in four hotspot regions – the Middle East, central Asia, the Ganges-Brahmaputra-Meghna basin, and the Orange and Limpopo basins in southern Africa.

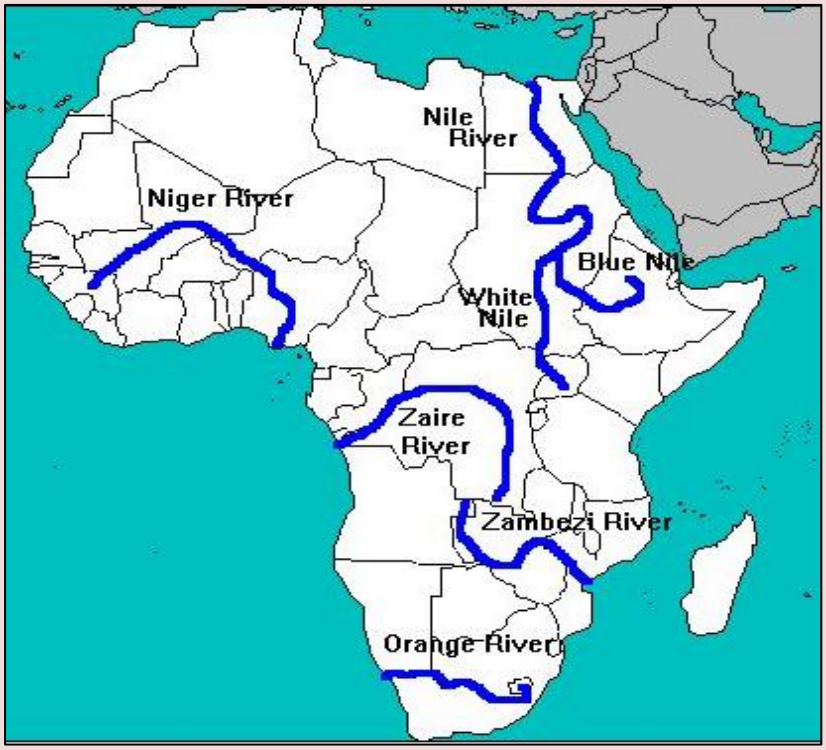
Additionally, the Nile River in Africa, much of southern Asia, the Balkans in southeastern Europe, and upper South America are all areas where new dams are under construction and neighboring countries face increasing water demand, may lack workable treaties, or worse, haven't even discussed the issue.

"If two countries have agreed on water flow and distribution when there's a dam upstream, there usually is no conflict," said Eric Sproles, an Oregon State University hydrologist and a co-author on the study. "Such is the case with the Columbia River basin between the United States and Canada, whose treaty is recognized as one of the most resilient and advanced agreements in the world.

"Unfortunately, that isn't the case with many other river systems, where a variety of factors come into play, including strong nationalism, political contentiousness, and drought or shifting climate conditions."

The conflict over water isn't restricted to human consumption, the researchers say. There is a global threat to biodiversity in many of the world's river systems, and the risk of species extinction is moderate to very high in 70 percent of the area of transboundary river basins.

Asia has the highest number of dams proposed or under construction on transboundary basins of any continent with 807, followed by South America, 354; Europe, 148; Africa, 99; and North America, 8. But Africa has a higher level of hydro-political tension, the researchers say, with more exacerbating factors.



The Nile River, for example, is one of the more contentious areas of the globe. Ethiopia is constructing several dams on tributaries of the Nile in its uplands, which will divert water from countries downstream, including Egypt. Contributing to the tension is drought and a growing population more dependent on a water source that may be diminishing.

"When you look at a region, the first thing you try to identify is whether there is a treaty and, if so, is it one that works for all parties and is flexible enough to withstand change," Sproles said. "It's easy to plan for water if it is the same every year – sometimes even when it's low. When conditions vary – and drought is a key factor – the tension tends to increase and conflict is more likely to occur."

In addition to environmental variability and lack of treaties, other factors leading to conflict include political and economic instability, and armed conflict, the analysis shows.

Sproles said one reason the Columbia River Basin treaty between the U.S. and Canada has worked well is the relative stability of the water supply. In contrast, climate models suggest that the Orinoco River Basin in northern Brazil and the Amazon Basin in upper South America may face drier conditions, which could lead to more strife.

Sproles is a courtesy faculty member in Oregon State's College of Earth, Ocean, and Atmospheric Sciences, where he received his doctorate.

More information on the United Nations Transboundary Waters Assessment Program is available at: http://www.geftwap.org/.

— Read more in L. De Stefano et al., "Assessment of transboundary river basins for potential hydro-political tensions," Global Environmental Change 45 (13 July 2017): 35-46 (DOI: 10.1016/j.gloenvcha.2017.04.008); and Jacob D. Petersen-Perlman et al., "Hydropolitics:


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

Severe terror threat: businesses must be aware

Source: http://www.insurancebusinessmag.com/uk/news/kidnap-ransom-terrorism/severe-terror-threat-businesses-must-be-aware-71447.aspx

June 26 – The international terrorism threat in the UK is currently rated severe, meaning another terrorist attack is highly likely. But how can businesses react to terrorism threat levels?
What has become painstakingly clear is that terrorists have the intent of causing mass casualties by any means possible. While security has tightened in many potentially threatening areas, little can be done to prevent vehicle attacks and the use of homemade, improvised weaponry.
Paul Bassett, managing director, and Justin Priestly, director of crisis management at Arthur J. Gallagher, spoke to Insurance Business about how businesses can better prepare to keep their prevention and security measures in line with the terrorism threat level.
"Businesses can't do anything about the threat – but they must be aware of it," said Bassett. "At Arthur J. Gallagher we advise businesses to organise their activities into four pillars: anticipate, prevent, respond and recover.
"The changing nature of threats presents different challenges to businesses and demands an equally dynamic response from those specialising in risk management and insurance."
He added: "Specialised insurance products are available but they are still relatively new in the stand-alone terrorism insurance market. Business people haven't been that focused in looking at how their insurance works. We would recommend they review their insurance coverages with their brokers to make sure they have fit-for-purpose and cost-effective cover in place."
Brokers at Arthur J. Gallagher have been working with companies to **establish a culture of crisis resilience and awareness.** An underlying factor of that culture is education. Businesses need to assist the government by educating clients about the terror threat level and how to respond to it. The company has also introduced a number of schemes and tools to show businesses how to mitigate and prevent potential terrorist threats.
"Once you understand the threat to your business, it's then a case of how you can mitigate and prevent those sorts of things from happening. The easiest thing to do is to educate your workforce and educate the people who are coming into your building. We call that situational awareness," said Priestly.
There are various ways to mitigate threat, according to Priestly. **Education is key** and so is the collection of information and intelligence. Businesses can contribute to this intelligence by keeping accurate logs and using CCTV effectively.
"Businesses could use CCTV cameras to look out of the building or premises and collect data when things are happening," Priestly told Insurance Business. "There's a whole lot of low-level information that is now being filtered up and turned into intelligence. The security services are doing a lot for UK business by using this low-level information to create an intelligence picture to prevent things from happening."
Arthur J. Gallagher has compiled a global terrorism database, made by (in simplified terms) plotting client risk portfolios onto a map. The database categorises where terrorists are likely to target and provides valuable risk data for clients.
Priestly explained: "We are able to sit with clients and look at where they are potentially vulnerable. What we are then able to do is run realistic disaster scenarios against our client's assets to look at any potential impact to their people or buildings. This enables clients to quantify what their losses might be."

As Cyber Threats Mount, Businesses Must Mount a Defense

Source: http://www.hstoday.us/single-article/as-cyber-threats-mount-businesses-must-mount-a-defense/9ca488010dac2982c1e74aa0e3bbffcc.html

June 06 – US Chamber of Commerce President and CEO Tom Donohue said this week that, "Five years ago, people thought of cybersecurity mostly as an IT issue. More recently, it's become a hot topic in boardrooms and a priority in the C-Suite. Today, cybersecurity must be a core management issue for all businesses—from the Fortune 500 to the mom-and-pop shop to the micro-entrepreneur."

"Every business," he urged in a statement, "must take steps to protect data, assets and consumers. Doing so will promote a strong, secure and resilient economy."

His plea to businesses to strengthen their cybersecurity efforts comes on the heels of WannaCry ransomware attack.

To help businesses, the US Chamber is continuing its Cybersecurity Awareness Campaign which is geared toward educating small and midsize businesses about cyber threats and best practices to defend their systems against intrusion.

Donohue said, "Businesses around the world and across a wide range of industries continue to reel from the biggest ransomware attack in history. The WannaCry ransomware attack hit more than 230,000 computers in over 150 countries, holding data hostage from hospitals, global shipping businesses, entertainment companies and more."

He said, "It's a stark reminder of the digital risks facing all levels of government and all businesses and institutions in the digital age—and yet another reason for American businesses to step up their cybersecurity efforts."

Donohue pointed out that, "While large businesses invest heavily in defense systems, many smaller firms often lack the tools or resources to protect themselves."

He said, "To help close this gap, the US Chamber of Commerce is continuing our Cybersecurity Awareness Campaign with regional events around the country. The campaign is geared toward educating small and midsize businesses about cyber threats and best practices to defend their systems against intrusion. Originally launched in 2014, the campaign is in its fourth year. We kicked off our 2017 efforts in March hosting a conference with the Salt Lake Chamber and followed up with an event in South Carolina last month. The Chamber will hold three more regional roundtables leading up to our Sixth Annual Cybersecurity Summit in October."

The Chamber also urges all businesses to use the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity. This framework, which was updated earlier this year, provides practical guidance for companies to reduce network weaknesses.

But, "While businesses take steps to protect themselves, the government must play a role too," Donohue stressed, noting, "The Chamber was encouraged that President Trump signed an executive order last month bolstering our nation's cyber defenses. The measure emphasized the importance of strengthening public-private partnerships, which has long been a priority of the American business community. The Chamber will continue working with the administration to address cyber challenges, including streamlining the bureaucratic hurdles that impede private sector security efforts and promoting real-time information sharing between business and government."

Donohue said, "It's clear that this challenge will only grow in scope and sophistication—and businesses must prepare accordingly. Five years ago, people thought of cybersecurity mostly as an IT issue. More recently, it's become a hot topic in boardrooms and a priority in the C-Suite. Today, cybersecurity must be a core management issue for all businesses—from the Fortune 500 to the mom-and-pop shop to the micro-entrepreneur. Every business must take steps to protect data, assets, and consumers. Doing so will promote a strong, secure and resilient economy."