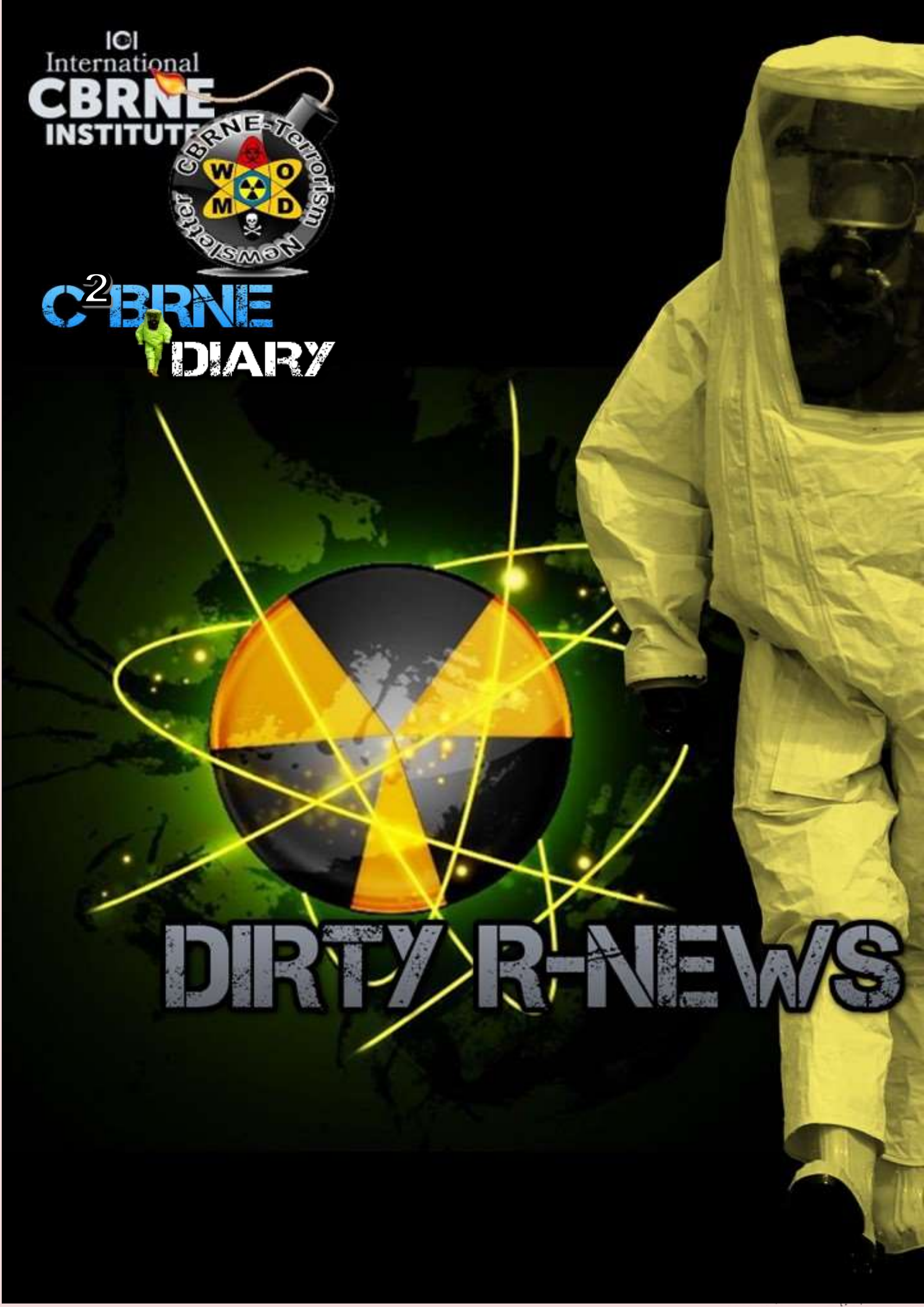
2 CBRNE DIARY

Dedicated to Global First Responders

CBRNE-Terrorism Newsletter

August 2018

www.cbrne-terrorism-newsletter.com


ICI
International
CBRNE
INSTITUTE
CBRNE-Terrorism Newsletter
W
O
M
D
C2BRNE
DIARY
DIRTY R-NEWS

Next-gen Nukes

By Nathanael Johnson

Source: https://grist.org/article/next-gen-nuclear-is-coming-if-we-want-it/

July 18 – Back in 2009, Simon Irish, an investment manager in New York, found the kind of opportunity that he thought could transform the world while — in the process — transforming dollars into riches.

Irish saw that countries around the globe needed to build a boggling amount of clean-power projects to replace their fossil fuel infrastructure, while also providing enough energy for rising demand from China, India, and other rapidly growing countries. He realized that it would be very hard for renewables, which depend on the wind blowing and the sun shining, to do everything. And he knew that nuclear power, the only existing form of clean energy that could fill the gaps, was too expensive to compete with oil and gas.

But then, at a conference in 2011, he met an engineer with an innovative design for a nuclear reactor cooled by molten salt. If it worked, Irish figured, it could not only solve the problems with aging nuclear power, but also provide a realistic path to dropping fossil fuels.

"The question was, 'Can we do better than the conventional reactors that were commercialized 60 years ago?" Irish recalled. "And the answer was, 'Absolutely.'"

Irish was so convinced that this new reactor was a great investment that he bet his career on it. Nearly a decade later, Irish is the CEO of New York City-based Terrestrial Energy, a company that expects to have a molten-salt reactor online before 2030.

Terrestrial is far from alone. Dozens of nuclear startups are popping up around the country, aiming to solve the well-known problems with nuclear power — radioactive waste, meltdowns, weapons proliferation, and high costs.

There are reactors that burn nuclear waste. There are reactors designed to destroy isotopes that could be made into weapons. There are small reactors that could be built inexpensively in factories. So many ideas!

To former Secretary of Energy Ernest Moniz, an advisor to Terrestrial, it feels as if something new is underway. "I have never seen this kind of innovation in the sector," he said. "It's really exciting."

Other reactors, like Terrestrial's molten-salt-cooled design, automatically cool down if they get too hot. Water flows through conventional reactors to keep them from overheating, but if something halts this flow — like the earthquake and tsunami in Fukushima — the water boils off, leaving nothing to stop a meltdown.

Unlike water, salt wouldn't boil off, so even if operators switched off safety systems and walked away, the salts would keep cooling the system, Irish said. Salts heat up and expand, pushing uranium atoms apart and slowing down the reaction (the farther apart the uranium atoms, the less likely a flying neutron will split them apart, triggering the next link in the chain reaction).

"It's like your pot on the stove when you are boiling pasta," Irish said. No matter how hot your stove, your pasta will never get hotter than 212 degrees Fahrenheit unless the water boils off. Until it's gone, the water is just circulating and dissipating heat. When you replace water with liquid salt, however, you have to get to 2,500 degrees Fahrenheit before your coolant starts to evaporate.

This stuff can sound like science fiction — but it's real. Russia has been producing electricity from an advanced reactor that burns up radioactive waste since 2016. China has built a "pebble bed" reactor that keeps radioactive elements locked inside cue ball-sized graphite spheres.

In 2015, to keep track of the startups and public-sector projects working on trying to provide low-carbon energy with safer, cheaper, and cleaner nuclear power, the centrist think tank, Third Way, started mapping all of the advanced nuke projects across the country. There were 48 dots on the first map, and now there are 75, spreading like a candy-colored case of measles.

"In terms of the number of projects, the number of people working on it, and the amount of private financing, there isn't anything to compare it to unless you go back to the 1960s," said Ryan Fitzpatrick who works on clean energy for Third Way.

Back then, just after Walt Disney released the film "Our Friend the Atom" promoting nuclear energy, when the futuristic notion of electricity "too cheap to meter" seemed plausible, electric utilities had plans to build hundreds of reactors across the United States.

Why is this all happening now? After all, scientists have been working on these alternative types of reactors since the beginning of the Cold War, yet they've never caught on. The history of advanced reactors is littered with the carcasses of failed attempts. A salt-cooled reactor first ran successfully back in 1954, but the United States opted to specialize in water-cooled reactors and defunded other designs.

But something fundamental has changed: Previously, there was no reason for a nuclear company to pony up the billion dollars needed to get a new design through the federal regulatory process because conventional reactors were profitable. That's not true anymore.

"For the first time in half a century, the incumbent nuclear players are in financial distress," Irish said.

Recently, the United States' bet on conventional water-cooled reactors has been going bad in very expensive ways. In 2012, South Carolina Electric & Gas got permission to build two huge conventional reactors to generate 2,200 megawatts, enough to power 1.8 million homes, promising to have them up and running sometime in 2018. Electricity users saw their bills jump 18 percent to pay for the construction, which soon ran into delays. Last year, after sinking $9 billion into the project, the utility gave up.

"The most recent builds in the United States have been a disaster, largely due to poor on-sight construction practices," said John Parsons, codirector of MIT's Low-Carbon Energy Center for Advanced Nuclear Energy Systems.

Similar stories have played out abroad. In Finland, construction of a new reactor at the Olkiluoto power plant is eight years behind schedule and $6.5 billion over budget.

In response, these nuclear startups are designing their businesses to avoid horrible cost overruns. Many have plans to build standardized reactor parts in a factory, then put them together like Legos at the construction site. "If you can move construction to the factory you can drive costs down significantly," Parsons said.

New reactors could also reduce costs by being safer. Conventional reactors have a fundamental risk of meltdown, largely because they were designed to power submarines. It's easy to cool a reactor with water when it's in a submarine, underwater, but when we lifted these reactors onto land, we had to start pumping water up to cool them, Irish explained. "That pumping system can never, ever break, or you get a Fukushima. You need safety system on top of safety system, redundancy on top of redundancy."

Oklo, a Silicon Valley startup, based its reactor design on a prototype that isn't susceptible to meltdowns. "When engineers shut off all the cooling systems, it cooled itself and then started back up and was running normally later that day," said Caroline Cochran, Oklo's cofounder. If these safer reactors don't require all those backup cooling systems and concrete containment domes, companies can build plants for much less money.

Technologies often fail for a long time before succeeding: 45 years of tinkering passed between the first electric light and Thomas Edison's patent for an incandescent bulb. It can take decades for the engineering to catch up to the idea. Others have tried seemingly every idea for advanced nuclear in the past, Parsons said. "But science has moved forward," he

said. "You have much better materials than you did a few decades ago. That makes it believable these things could work."

A recent study from the nonprofit Energy Innovation Reform Project estimated that the latest batch of nuclear startups could deliver electricity somewhere between $36 and $90 a megawatt hour. That's competitive with any power plant that runs on natural gas (which runs between $42 to $78), and would provide a viable alternative to fossil fuels.

In a best-case scenario, nuclear power could be even cheaper. There are projections a study like this can make based on, say, an improved design that cuts construction costs, but it can't anticipate revolutionary advances.

"Hopefully these designers will come up with much more radical reductions in cost — you would like energy to be more accessible to a billion more people — so that nuclear becomes a cheap alternative that can beat natural gas even if there's no carbon price," Parsons said. "That's just a hope, but that's what entrepreneurs are supposed to do."

Matthew Bunn, a nuclear expert at Harvard, said that if nuclear power is going to play a role in fighting climate change, these advanced nuclear companies will have to scale up insanely fast. "To supply a tenth of the clean energy we need by 2050, we have to add 30 gigawatts to the grid every year," he said.

That means the world would have to build 10 times as much nuclear power as it was before the Fukushima disaster in 2011. Is that even realistic?

"I think we ought to be trying — I'm not optimistic," Bunn said, noting that the pace at which we'd need to build solar and wind to quit fossil fuels is just as daunting.

Big barriers remain in the way of a nuclear renaissance. It takes years to test prototypes and get approval from federal regulators before a company can even start construction. "In order for advanced nuclear technologies to play a role in deep decarbonization over the next several decades," the United States would need to overhaul the way it's rolling out the technology, according to a study published earlier this month in the Proceedings of the National Academy of Sciences.

Experts point to many of the same steps to give advanced nuclear a fighting chance: Making regulations more friendly to innovation, instead of favoring conventional reactors. Creating incentives to reward utilities for buying low-carbon power. And a lot more funding.

A rendering of an advanced nuclear-gas hybrid reactor. Hybrid Power Technologies LLC

The people behind the new crop of nuclear companies think they can get to market much faster with the right help. Oklo is shooting to have a commercial reactor online before 2025. "Can we decarbonize quickly with nuclear? France did it, it can be done," Cochran from Oklo said. "Our reactors are 500 times smaller than the [latest conventional reactors], they have

all these inherent safety characteristics, and they can consume nuclear waste. Will our application process be any shorter?"

Lowering these barriers would be cheaper than letting the government pick one promising idea and coddle it like a privileged child, which is the way we've treated conventional nuclear in the past, said Jessica Lovering, who studies nuclear power at the Breakthrough Institute, a pro-technology environmental think tank.

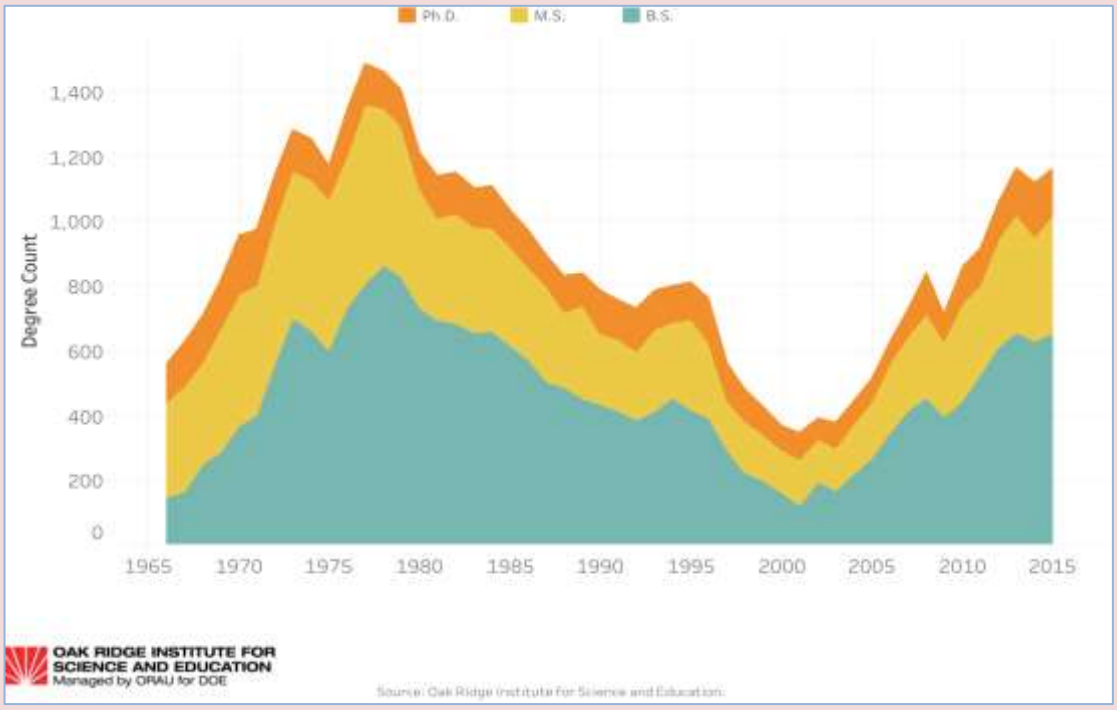
"We could pick one idea, spend a lot of money helping it become commercial, and then subsidize every project for even more money," Lovering said. "Or, we could invest a much smaller amount of money across the entire innovation system."

Still, it could easily take the advanced nuclear projects 30 years to get through regulatory review, fix the unexpected problems that crop up along the way, and prove that they can compete, said Dan Kammen, who studies clean energy at the University of California Berkeley. And by then Kammen thinks there will be other options in competition: Electric storage is getting better, and fusion could have a breakthrough.

"Ultimately on a planet with 10 billion people, some amount of large, convenient, affordable, safe baseload power — like we get from nuclear fission, or fusion — would be just hugely beneficial," Kammen said. "There are other competitors in view on the straight solar side that 10 years ago sounded like science fiction — space-based solar, transparent solar films on every window. That world works, too."

At this point in history, everything is a longshot. We've got to completely replace our energy system on the fly. To do that, people are planting a lot of different seeds. It's still a long time until harvest, but we're seeing a flush of new sprouts from the advanced nuclear section of the garden.

This new flush of nuclear possibility has excited young people who see nuclear as a way to shift away from fossil fuels. College students are gravitating toward nuclear engineering. The number of students studying the subject cratered when the nuclear industry collapsed in the late 1970s (the Three Mile Island accident in 1979 didn't help), but it has been creeping steadily higher since the early 2000s.



The number of degrees earned in nuclear engineering since 1966. Oak Ridge Institute and Science and Education

Some of those students are going on to start their own advanced nuclear companies. David Schumacher, a documentary filmmaker, met some of these young people and became so infected with their enthusiasm that he made a documentary about them, *The New Fire*, which came out last year.

"They are truly idealistic young people trying to save the planet by doing something really important but really unpopular," Schumacher said. "They could be making a lot of money elsewhere, but instead they are starting these nuclear companies, knowing they are going to be maligned."
It's a feeling Simon Irish, at Terrestrial Energy, is familiar with. "The views on nuclear are so negative," he said. "The great win is simply to persuade busy people to listen."
While Terrestrial battles public opinion, Irish said his company has been hitting every milestone on time. Canadian regulators announced last year that Terrestrial had completed the initial stage of its design review — the first step toward approval in that country. Irish has already selected sites in Ontario where Terrestrial could build the first reactors.
Although Irish was mum on Terrestrial's other milestones, he did describe an experience that he said gives him more confidence in the company's prospects than any of its other accomplishments so far.
Last August, he found himself in the office of a prominent New York investor, a major contributor to environmental organizations. Getting the meeting had been a challenge — again because of the controversy around nuclear. But by the end, Irish had convinced the businessman that renewables and nuclear could not just coexist but compliment each other.
In Irish's telling, he was in the middle of explaining Terrestrial's reactor design when the man stopped him and said, "'Hold on, this can deliver heat! The industrial sector needs heat, and wind and solar aren't making any dent in that at all.'
"As far as he was concerned," Irish said, "this was the great missing piece."

***Nathanael Johnson** is Grist's senior writer and the author of two books.*

Hiroshima & Nagasaki

A collection of related articles

Source: https://thebulletin.org/collections/hiroshima-nagasaki/

It's been 73 years since the Bomb was dropped on Hiroshima and, a few days later, on Nagasaki, Japan. That week in August changed the world forever; ever since, the global nuclear arsenal has risen and dropped. But the nuclear threat has never dissipated. Here's a collection of *Bulletin* articles that

provide what you need to remember and think about as the world navigates a particularly dangerous portion of the Nuclear Age.

Latest tests at Barakah successful as reactor systems exposed to 300-degree heat

Source: https://www.thenational.ae/uae/latest-tests-at-barakah-successful-as-reactor-systems-exposed-to-300-degree-heat-1.757411

Testing is complete on Unit 2 at Barakah Nuclear Energy Plant. Courtesy: ENEC

Aug 06 – Tests that expose the reactors at Barakah nuclear power plant to extreme heat have been successfully completed.

The Emirates Nuclear Energy Corporation said the results of hot functional testing on Unit 2 showed it had achieved the highest standards of quality, safety and efficiency.

Enec said it worked closely with the Korea Electric Power Corporation, the joint venture partner and prime contractor, to achieve the milestone in the testing and commissioning of Unit 2.

"We are proud to have maintained our track record of safety and efficiency with the successful completion of Hot Functional Testing on Unit 2. By incorporating the lessons learnt from the same tests on Unit 1, we continue to establish Barakah as the benchmark for new nuclear construction projects worldwide," said Mohamed Al Hammadi, chief executive of Enec.

"Keeping construction progress approximately one year apart for each of the units at Barakah makes it possible for us to implement all lessons learnt from one unit to the subsequent ones, in line with international best practices in the management of megaprojects."

Testing takes place over a number of weeks and consists of almost 200 individual and integrated tests on major systems to check their performance under normal operational conditions, without the presence of nuclear fuel in the reactor.

The test was the first time that most of the reactor's systems experienced the operational temperature of nearly 300 degrees Celsius and operational pressure of more than 150 kilograms per square centimetre, which is the equivalent of the pressure at 1,500 metres underwater.

During the testing, components were checked for thermal expansion, vibration and wear.

In May, the plant's operators said it would not begin generating electricity until the end of next year, or possibly 2020.

Construction of the $25 billion plant began in 2011, with electricity generation originally set for last year.

Al Hammadi said: "This most recent round of testing ensures that Unit 2's systems and components are on track to reliably and safely perform their intended functions when the plant becomes operational."

Enec announced in April that the plant was a step closer to being switched on after completion of tests on Unit 1.

The UAE plans to bring a total of four nuclear reactors into operation by 2021 producing a combined 5,600 megawatts of power.
The project has been described as a vital component in the country's programme to diversify its energy supply and reduce its reliance on fossil fuels.

Uranium in Qeens?

By Andy Karam
Source: http://nct-magazine.com/august18/case-study-uranium-in-queens/

In the Spring of 2014, the NYC Department of Sanitation (DSNY) was cleaning out a vacant lot in the Borough of Queens when they found a metal cylinder that was about 25 cm in diameter and about 40 cm long that weighed about 30 kg. It had a cavity in one end, and the word "Uranium" was stamped in the metal on one side. There were also some projections at the top that could be used to carry the cylinder.

A Mo-99/Tc-99m generator column. The actual radioactivity fits into the small cylindrical section at the bottom.

As DSNY inspected the site further, they found other items that appeared to be plastic buckets, medical tubing and needles of some sort – three or four sets in all – but these seemed to have nothing to do with the metal cylinder.

What instruments told us
Since the Department of Sanitation finds radioactive materials in the trash fairly frequently (usually radium watch dials, radioactive rocks, or medical radioactivity) they are proficient in the use of radio-isotope identifiers (RIIDs) so they brought their instrument to the site and were surprised that the cylinder was identified as being highly enriched uranium (HEU). Radiation measurements obtained on contact with the cylinder indicated a dose rate of about 10 µSv/hr – about 20 times as high as normal background radiation dose rates in that part of New York. At this point, DSNY contacted the NYPD and asked for assistance with identifying and resolving the matter.

Investigating and resolving the matter
When I arrived at the scene with the NYPD Counterterrorism Division, I confirmed the DSNY radiation dose rate and nuclide identification. At the same time, it seemed unlikely that a nuclear weapon had appeared in a vacant lot in Queens. In particular, the shape of the object was wrong, and to the best of my knowledge, we do not stamp "Uranium" into the actual fuel for such devices. However, the cylinder was the shape of a depleted uranium (DU) shield frequently used for medical radioactivity, and the tubing and bucket that were found were consistent with a device used to produce Tc-99m for medical use. On the other hand, the nuclide identifications that I was obtaining with the RIID simply did not make any sense – it insisted that the metal was weapons-grade

uranium and that the tubing contained an isotope of cesium (specifically Cs-134, which is produced in nuclear reactors in relatively small quantities).

When I took a closer look at the cylinder itself, I noticed the name of an American radiopharmaceutical company and a serial number stamped into the metal. One of the detectives demonstrated his investigative talents by locating the company's radiation safety officer and placing a call, then turned the phone over to me. When I read the serial number the RSO replied "Yep – that's one of ours. We lost 8 of those from a customer on Long Island about 6 months ago and we were wondering what had happened to them."

I decided not to reply with what first occurred to me to say and, instead, simply thanked him for this information and informed him that his company would, of course, be responsible for shipping the cylinder and other materials back to his facility, which he agreed to do. With that out of the way, we realized that we still had another 2-3 sets of tubing, plastic buckets, and other internal materials – but we had no corresponding DU shields. So we spent the next hour or so searching the vacant lot and surrounding areas to see if those would turn up. Unfortunately, we were never able to find any additional shields.

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

Andrew Karam *has over 35 years of experience in radiation safety and nuclear power, beginning with his time in the US Navy. For the last 10 years he has been working on issues related to radiological and nuclear emergency response and counterterrorism, including several years as a scientist with the New York City Police Department. He currently works for Mirion Technologies as a Homeland Security Scientific Advisor.*

What are coastal nuclear power plants doing to address climate threats?

By John Vidal

Source: http://www.homelandsecuritynewswire.com/dr20180810-what-are-coastal-nuclear-power-plants-doing-to-address-climate-threats

Aug 10 – The outer defensive wall of what is expected to be the world's most expensive nuclear power station is taking shape on the shorelineof the choppy gray waters of the Bristol Channel in western England.

By the time the $25 billion Hinkley Point C nuclear station is finished, possibly in 2028, the concrete seawall will be 12.5 meters (41 feet) high, 900 meters (3,000 feet) long and durable enough, the UK regulator and French engineers say, to withstand the strongest storm surge, the greatest tsunami and the highest sea-level rise.

But will it? Independent nuclear consultant Pete Roche, a former adviser to the UK government and Greenpeace, points out that the tidal range along this stretch of coast is one of the highest in the world, and that erosion is heavy. Indeed, observers reported serious flooding on the site in 1981 when an earlier nuclear power station had to be shut down for a week. following a spring tide and a storm surge. However well built, says Roche, the new seawall does not adequately take into account sea-level rise due to climate change.

"The wall is strong, but the plans were drawn up in 2012, before the increasing volume of melting of the Greenland ice cap was properly understood and when most experts thought there was no net melting in the Antarctic," he says. "Now estimates of sea level rise in the next 50 years have gone up from less than 30 centimeters to more than a meter, well within the operating lifespan of Hinkley Point C — let alone in 100 years time when the reactors are finally decommissioned or the even longer period when spent nuclear fuel is likely to be stored on site."

In fact, research by *Ensia* suggests that at least 100 U.S., European and Asian nuclear power stations built just a few meters above sea level could be threatened by serious flooding caused by accelerating sea-level rise and more frequent storm surges.

Some efforts are underway to prepare for increased flooding risk in the future. But a number of scientific papers published in 2018 suggest that climate change will impact coastal nuclear plants earlier and

harder than the industry, governments or regulatory bodies have expected, and that the safety standards set by national nuclear regulators and the United Nations' nuclear watchdog, the International Atomic Energy Agency (IAEA), are out of date and take insufficient account of the effects of climate change on nuclear power.

Darlington Nuclear Generating Station (Photo Courtesy of Ontario Power Generation)

The problem with flooding

Flooding can be catastrophic to a nuclear power plant because it can knock out its electrical systems, disabling its cooling mechanisms and leading to overheating and possible meltdown and a dangerous release of radioactivity. Flooding at the Fukushima Daiichi plant in Japan as a result of the March 2011 tsunami caused severe damage to several of the plant's reactors and only narrowly avoided a catastrophic release of radioactivity that could have forced the evacuation of 50 million people. The interactive map from Carbon Brief shows the location of nuclear power plants around the world. According to maps prepared by the World Association of Nuclear Operators (WANO), around one in four of the world's 460 working commercial nuclear reactors are situated on coastlines. Many were built only 10–20 meters (30–70 feet) above sea level at a time when climate change was barely considered a threat.

In the U.S., where nine nuclear plants are within 2 miles (3 kilometers) of the ocean and four reactors have been identified by Stanford academics as vulnerable to storm surges and sea-level rise, flooding is common, says David Lochbaum, a former nuclear engineer and director of the nuclear safety project at the Union of Concerned Scientists (UCS).

Lochbaum says over 20 flooding incidents have been recorded at U.S. nuclear plants since the early 1980s. "The most likely [cause of flooding] is the increasing frequency of extreme events," he says.

"There was no consideration of climate change when most U.S. plants were built," says Natalie Kopytko, a Leeds University researcher who has studied nuclear power plant adaptations to climate change. "They used conservative models of historical reference. Also, they were largely built at a calm period, when there were not many major storms."

"While an accident has never yet happened due solely to sea-level rise and storms, the flooding experienced at Fukushima resembles what could occur in the future from sea-level rise," says Kopytko.

Considering climate change

IAEA's current global safety standards were published in 2011. These state that operators should only "take into account" the 18- to 59-centimeter (7- to 23-inch) sea-level rise projected by 2100 in the Intergovernmental Panel on Climate Change (IPCC)'s fourth assessment report, published in 2007.

But those safety standards don't factor in the most recent assessment of the IPCC, published in 2013–14. This scientific consensus report has seas rising 26 centimeters (10 inches) to 1 meter (39 inches) by 2100, depending on how far temperature continue to rise and the speed at which the polar ice caps melt.

A 1-meter (39-inch) increase, combined with high tides and a storm surge, significantly increases the risk of coasts and nuclear stations being swamped, says Michael Mann, director of the Earth System Science Center at Pennsylvania State University.

"Nuclear stations are on the front line of climate change impacts both figuratively and quite literally," Mann says. "We are likely profoundly underestimating climate change risk and damages in coastal areas."

A recent study from NASA's Goddard Space Flight Center expects the mean average rise to be a minimum of 65 centimeters (26 inches) by 2100.

"This 65-centimeter [rise] is almost certainly a conservative estimate," says NASA lead author Steve Nerem, a professor of aerospace engineering sciences at the University of Colorado Boulder. "Our [study] assumes that sea level continues to change in the future as it has over the last 25 years. Given the large changes we are seeing in the ice sheets today, that's not likely."

A matter of timing

Sea-level rise, averaging 3 millimeters (0.1 inches) a year worldwide — but more or less in some places depending on topography and geography — is regarded by the two global nuclear trade bodies as a future, rather than a present risk.

"The IPCC says sea-level rise is not expected to kick in for some time. It's a very long timeline," says WANO spokesperson Tim Jeffery.

Most reactors, says Jonathan Cobb of the World Nuclear Association, will have been long decommissioned by the time any significant sea-level rise takes place. "The industry has been taking climate change impacts into account and taking action," Cobb says. "This has happened both before and after the Fukushima accident."

However, flooding already is becoming much more frequent along the U.S. coastline. According to the U.S. Environmental Protection Agency (EPA), nearly all of 27 regularly measured coastal sites have experienced a significant increase in flooding since the 1950s, with the rate accelerating in many locations along the East and Gulf Coasts where many reactors are situated.

The most comprehensive research yet conducted also shows sea-level rises are accelerating as ice caps melt. Such is the speed of ice melt observed since 2007 that even the 2013 IPCC estimates of sea-level rise are thought to be outdated.

"There has been a steep increase in ice losses from Antarctica during the past decade, and the continent is causing sea levels to rise faster today than at any time in the past 25 years. This has to be a concern for the governments we trust to protect our coastal cities and communities," says joint lead author Andrew Shepherd, professor of earth observation at the University of Leeds and

principal scientific advisor to the European Space Agency.

Sea-level risewas not considered when the first British and U.S. nuclear stations were built in the 1960s. In the UK, analysis by the government's floods and coastal erosion team found in 2012 that 12 of the country's 19 nuclear plants would be at risk of erosion or coastal flooding by the 2080s without more protection. Those at Bradwell, Hinkley Point, Hartlepool, Sizewell, Dungeness and Oldbury were considered "high risk."

Threats from storms

On top of sea-level rise, the added impact of flooding from storm surges must be considered as well, scientists say. Since 1970, the magnitude and frequency of extreme sea levels (ESLs, a factor of mean sea level, tide and storm-induced increases), which can cause catastrophic flooding, have increased throughout the world, according to the Global Extreme Sea Level Analysis project. New satellite studies by the U.S. government's National Oceanic and Atmospheric Administration (NOAA), NASA, and other leading scientific institutions all show mean sea level rising and magnifying the frequency and severity of ESLs.

The destructive power of the typhoons that regularly wreak havoc across China, Japan, Korea and the Philippines has intensified by 12 to 15 percent in the past 40 years with the proportion of category 4 and 5 storms doubling or tripling. Similarly, many of the most severe recorded Atlantic hurricane seasons have taken place since 2003. And new research suggests that every 1.8 °F (1 °C) increase in global average temperatures could lead, via increased sea level and more severe storms, to a two- to sevenfold increase in the risk of surges that are the magnitude of those caused by Hurricane Katrina, which struck New Orleans and other U.S. southern coastal cities in 2005.

Some individual U.S. plants are highly vulnerable, says Kopytko. Using the global average of an annual 3-millimeter (0.1-inch) sea-level rise and taking into account natural subsidence and the latest storm data and surge levels, she calculated in 2015 that several U.S. coastal plants could be inundated by storm surges. These included the St. Lucie and Turkey Point stations in Florida.

Her research, published in the Bulletin of Atomic Scientists, supports a 2012 Stanford University study that showed that many coastal nuclear plants are more vulnerable to inundation than was Fukushima Daiichi, including the Salem and Hope Creek nuclear plants in New Jersey, the Millstone station in Connecticut, and the Seabrook reactors in New Hampshire.

While no nuclear power plant has been in imminent danger of a meltdown because of a storm surge, there have been many close calls. Three U.S. nuclear power reactors were temporarily shut down because of Hurricane Sandy in 2012 and a fourth, Oyster Creek in New Jersey, was put on alert when water levels rose dramatically, according to the U.S. Nuclear Regulatory Commission (NRC).

The closest any U.S. station may have come to a storm-related disaster was in 1992 when Hurricane Andrew hit Florida's Turkey Point plant. Wind gusts of 175 miles per hour (282 kilometers per hour) and a 16-foot (4.9-meter) surge did only limited damage, but if the sea levels had been as high as are now projected, it could have led to a major disaster, according to Lochbaum.

"Hurricane Andrew is historic because this is the first time that a hurricane significantly affected a commercial nuclear power plant," wrote the NRC in a 1993 review of how Turkey Point fared during the emergency. None of the essential safety features was compromised during the storm, and the nuclear units, which had been shut down hours before the hurricane arrived, remained in a stable condition.

In 2006, if Typhoon Saomai — one of the strongest storms to hit China in 50 years, with 3.76-meter (12-foot) storm surges and 7-meter (23-foot) waves that caused 240 deaths and sank 952 ships — had landed two hours later on the coast it would have coincided with a spring tide and would almost certainly have inundated the reactors at Qinshan nuclear plant, says researcher Liu Defu of the Ocean University of China at Quinbgdao.

Reassess and improve

The IAEA advised the 31 countries that generate commercial nuclear power to reassess their safety after the Fukushima disaster in 2011. Within days of the 2011 earthquake, China suspended approvals for new plant construction and temporarily stopped work pending tests at plants under construction.

Stress tests on reactors demanded by the IAEA and nuclear regulators

after Fukushima forced the world's nuclear operators to reassess and improve their emergency control measures, including those related to flooding. One aging British station at Dungeness, for instance, was shut down for two months in 2013 while extra flood protection measures were set in to place in the wake of the Fukushima disaster.

Since the Fukushima incident, all coastal nuclear plants have installed more powerful pumps, upgraded power supplies, and installed waterproof doors and moveable flood barriers, says the World Nuclear Association's Cobb.

"In response to the accident [at Fukushima], reviews took place at reactors around the world, including checks of flood defenses and robustness of back-up power supplies — the so-called stress tests," he says.

In the U.S., the NRC ordered operators to tighten their safety plans after Fukushima and Hurricane Sandy. New back-up equipment to handle flooding was installed, substations and generating stations were shored up, new batteries installed and access roads strengthened, says NRC spokesperson Scott Burnell.

"All U.S. coastal nuclear facilities are built to withstand the worst-case storm scenario," Burnell says. "Every U.S. reactor site has completed its flooding hazard re-analysis. Forty of 49 sites have completed required focused evaluations of local intense precipitation and the plants' available margin to safely deal with the updated hazard. These include for sea-level rise and related effects such as storm surge."

However, few regulatory authorities around the world appear to have specifically asked operators to increase their defenses against climate-change-related dangers.

"Steps have been taken to lessen vulnerability to flooding at nuclear plants, but problems remain," says UCS's Lochbaum. "More portable power supplies, to give people more chance to respond to flooding have been installed. But pumps have been found to be inadequate. People spent a lot of money on new equipment after Fukushima, but it's not always working."

"The plant operators understand the problems of sea-level rise and extreme events," he adds. "They look at Fukushima and take note. They have billions of dollars in assets and they don't want to lose them. But if the regulator doesn't require a more robust structure then it's up to the operator, and they have shallow pockets."

A look to the future

According to the World Nuclear Association, some 50 nuclear power plants are now under construction, with roughly another 150 planned. Many of the world's new nuclear plants are being built on the coasts of Asian countries, which face floods, sea-level rise and typhoons. At least 15 of China's 39 reactors in operation, and many of the plants it has under construction, are on the coast.

According to an IAEA spokesman, Jeffrey Donovan, the agency's Department of Nuclear Energy hopes to publish later this year a study on how nuclear power and other energy facilities can adapt to climate change, including rising sea levels.

"Changes are happening faster than expected," says Myles Allen, head of the Climate Dynamics Group at Oxford University's department of physics and lead author of the upcoming IPCC 1.5 °C special report. "Standards must take climate change into account."

__John Vidal__ was environment editor of the Guardian for 27 years. He has reported on climate change and international environmental issues.

Lessons from Hiroshima: From Weapons of Mass Destruction to a Weapon of Mass Connection

By Dr. Michael Laitman

Source: https://www.breakingisraelnews.com/112206/lessons-from-hiroshima-from-weapons-of-mass-destruction-to-a-weapon-of-mass-connection-opinion/

Aug 13 – The 73rd anniversary of the atomic bombings of Hiroshima and Nagasaki, where two nuclear weapons killed at least 129,000 people—most of them civilians, with thousands more dying years later due to indirect injuries and radioactive exposure—is a worthy time for introspection, where we should ask ourselves, "What have we learned from such a tragic event?"

Simply put, very little.

We still live in an extremely volatile world. Decades of nuclear standoff may end in a blink of an eye with nuclear powers ready to push the red button at any given provocation, regardless of the global devastation it would inflict. The US is making efforts to limit Iran's nuclear program, but it's an uncertain road to peace. According to White House national security adviser, John Bolton, another global threat, North Korea, has not taken the necessary steps to de-nuclearize despite an agreement signed in June.

Back in the 1950s, the great Kabbalist of the twentieth century, Rabbi Yehuda Ashlag (Baal HaSulam) wrote about the consequences of nuclear proliferation in his essay *The Writings of the Last Generation*: "If the total ruin that they are destined to bring upon the world is still not evident to the world, they can wait for a third world war, or a fourth one. The bombs will do their thing and the relics that remain after the ruin will have no other choice but to take upon themselves this work, where both individuals and nations will not work for themselves more than is necessary for their sustenance, while everything else they do will be for the good of others."

The teachings of Baal HaSulam are more relevant now than ever. Mutual hatred overflows within societies, between people and countries, at all levels. Humanity is acting in the opposite direction of nature, which is balanced and harmonious. Instead, we are moving away from each other, immersed in global confrontation and frictions, developing sophisticated weaponry to destroy each other.

The human being is the most harmful force in nature, even more so than a nuclear bomb. The path to destruction is paved by incitement and separation among people. The ever-increasing human ego, the evil inclination that resides in people, manifests itself in self-centered actions at the expense of others. The exponential effect of this division within humanity is what causes wars and global crises. If we fail to implement a change in our self-centered focus, then we will continue heading down a path of prolonged suffering.

There is, however, another path. It is one where we realize the corrupt way we relate to each other, and construct new, positive relations among society—a path of unity.

The more we tread the path of suffering, the more unbearable pressure would eventually make it evident that there must be another way to lessen the pain. Human society would then seek advice on how to survive and escape war and crisis. It will then be up to the generation's leaders to do whatever possible to guide human society toward peaceful coexistence in an interconnected world.

The current global scenario is urging us to conduct this introspection, and choose a more civilized, enjoyable and wise path: the path of unity. Such a path is derived from nature's key element—connection—where nature as a whole operates in total balance. We can replicate this harmonious system by replacing our egoistic relations with altruistic ones.

The transition between the two paths—from torturous torment to a fast path of human connection—is what the wisdom of Kabbalah teaches. As threats increase and crises continuously emerge, the wisdom of Kabbalah becomes revealed and accessible to all. It is the strongest weapon against any threat in the world, a powerful, positive, spiritual force that unites people by balancing good and evil. It is the "weapon of mass connection," the only one we need for a peaceful existence.

Dr. Michael Laitman *is a Professor of Ontology, a PhD in Philosophy and Kabbalah, and an MSc in Medical Bio-Cybernetics. He was the prime disciple of Kabbalist, Rav Baruch Ashlag (the RABASH). Prof. Laitman has written over 40 books, translated into dozens of languages; he is the founder and president of the ARI Institute, and a sought after speaker.*

Radioactive sheep said to prove Israel illegally tested nuclear weapons

Source: https://www.middleeastmonitor.com/20180815-radioactive-sheep-said-to-prove-israel-illegally-tested-nuclear-weapons/

Aug 15 – **A science journal has claimed that radioactive sheep found in Australia could prove that Israel tested nuclear weapons, an action which would be in contravention of international law.**

The study, which was published by Princeton University's Science and Global Security journal, claims that Israel conducted an illegal nuclear test on 22 September 1979 near

Prince Edward Islands, located in the Indian ocean off the southern tip of Africa. At the time, a "double flash" of light was recorded by an American satellite named Vela 6911, a sign thought to indicate that a nuclear test had taken place. Theories have speculated since that the flash could have been caused by natural phenomena, for example by a meteor shower, but the journal's new study claims to have proof that this was not the case.

Dimona nuclear research facility in Israel

The new research, led by Christopher Wright of the Australian Defence Force Academy and Lars Erik de Geer, a former member of the Swedish Defence Research Agency, claims that a few weeks after the mysterious flash, "traces of radioactive Iodine (I-131) had been discovered in several dead sheep in Australia". Samples from the sheep's thyroid glands were then sent for tests in the United States, "but the test's results were never made public," Ynet reports.

It is thought that due to stormy weather at the time the "double flash" was recorded, the fallout from the alleged nuclear test was scattered throughout parts of Australia. The study believes the sheep in question may have eaten some grass in the affected area, causing them to become radioactive. If the journal's theory is correct, this marks the most concrete evidence to date that Israel conducted illegal nuclear testing during the height of the Cold War. That this was done in cooperation with South Africa, at that time ruled by an Apartheid regime, will likely raise further eyebrows.

Israel has long sought to conceal its alleged nuclear capabilities, neither confirming nor denying its possession of nuclear weapons. However, it is widely believed that Israel possesses nuclear WMDs (weapons of mass destruction) and is one of four nuclear-armed countries not recognised by the international Non-Proliferation Treaty. The other three are India, Pakistan and North Korea.

Israel's forays into the nuclear arena came under the spotlight in July when an exposéby the *Wall Street Journal*(WSJ) revealedthat in 1999 North Korea demanded Israel pay $1 billion in cash in return for halting its nuclear missile sales to Iran. It is believed that Israel refused the offer, instead offering to provide North Korea with food aid. The Israeli government refused requests to comment on the revelations.

Israel has also sought to prevent its regional foes from obtaining nuclear capabilities, most notably Iran and its proxies in Lebanon and Syria. In March, *Haaretz* revealed a 2007 strike on a North Korean made nuclear reactor near the Syrian town of Deir Ez-Zor, the details of which were subsequently censored by Israel for over a decade. Israel has also sought to quell Saudi Arabia's nuclear potential, in July setting outa number of "red lines" to the US administration over planned sales of nuclear reactors to its regional ally. These red lines included that Israel must know all the details of the plan in advance and that it be involved in preliminary consultations on the planned location of the nuclear reactors in Saudi Arabia.


ICI International
CBRNE INSTITUTE
CBRNE-Terrorism Newsletter
W M O D
C²BRNE DIARY
EXPLOSIVE NEWS

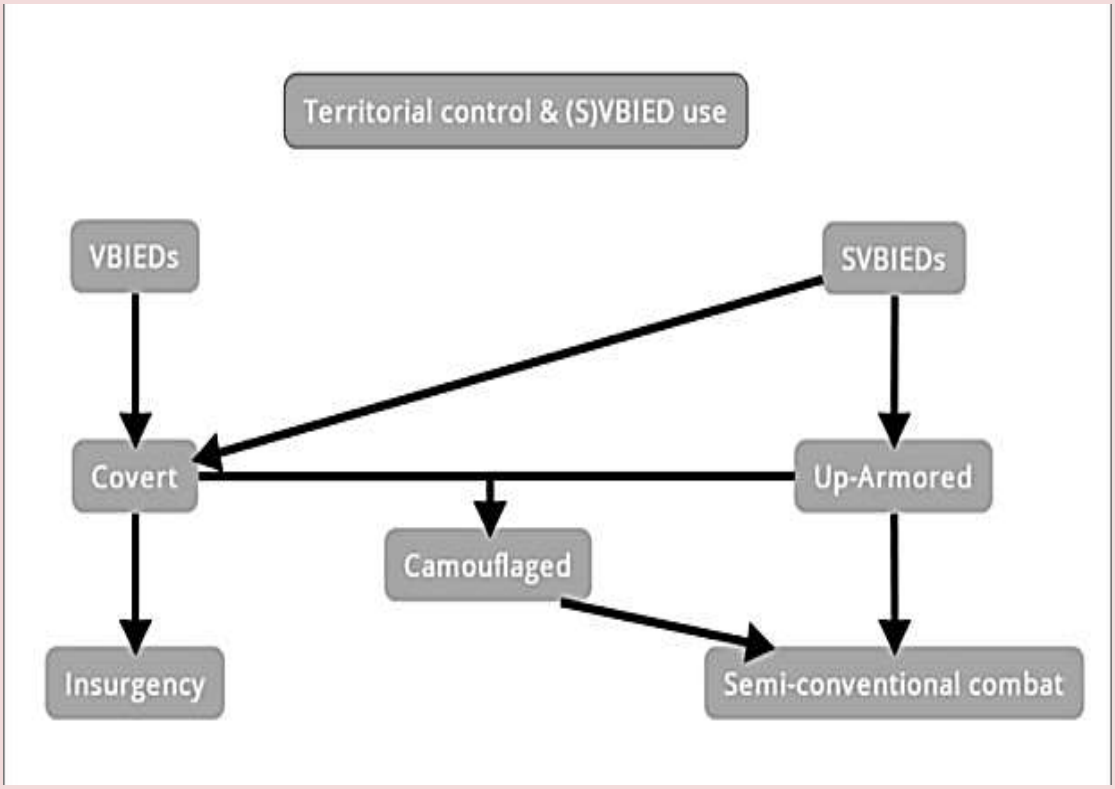
Through the desert & down the Euphrates – Islamic State SVBIED use & innovation

Source: https://zaytunarjuwani.wordpress.com/2018/05/29/through-the-desert-down-the-euphrates-islamic-state-svbied-use-innovation/

This is the second part of a series of articles covering the IS development and innovation of SVBIEDs from the battle of Mosul to the current situation. The first part covered the similarities between the battles of Mosul and Raqqah, while this part will cover the Islamic State's use of SVBIEDs (Suicide Vehicle Borne Improvised Explosive Devices) during the loyalist central & eastern Syrian desert offensives, as well as in the parallel loyalist and SDF offensives southwards along the Euphrates river toward the Iraqi border. Before I begin, I would recommend those who aren't completely familiar with the topic to read through my past articles on the history of Islamic State's use of SVBIEDs, as well as how their use of SVBIEDs developed during the battle of Mosul:

Introduction

The battle of Mosul was extremely important for the Islamic State (hereafter IS). Yes, the Iraqi Army achieved a decisive victory and eventually managed to completely eradicate the group's territorial presence nationwide. However, the battle of Mosul itself allowed IS to adapt and develop new SVBIED designs and tactics, subsequently field testing them on a grand scale, spurring further innovation. IS employed a total of 482 SVBIEDs during the nine month long battle, with at least 130 of those being confirmed via drone footage as successful attacks. In the battle of Mosul, IS introduced the "camouflaged" SVBIED, a blend of covert and up-armored SVBIEDS – featuring the stealthiness of the former and the armor of the latter. This new design was meant to emulate civilian vehicles while at the same time offering



the same protection as up-armored SVBIEDs once the Iraqi forces realise it's an SVBIED.

Stage 1 'camouflaged' SVBIEDs: Up-armored SVBIEDs with the added armor painted in the same color as the vehicle. Introduced in Eastern Mosul.

Stage 2 'camouflaged' SVBIEDs: Up-armored SVBIEDs with the added armor painted in the same color as the vehicle, as well as fake windshields, side windows, grilles & wheels painted in black on top of the already painted armor. Introduced in Western Mosul.

Stage 3 'camouflaged' SVBIEDs: Up-armored SVBIEDs where the armor is mounted on the interior of the vehicle as opposed to the exterior, dramatically increasing stealth. Used a single time in Eastern Mosul but later refined and used on a larger scale in the Eastern Aleppo countryside and during the battle of Raqqah.

Each of these stages were extensively field tested, and then innovated upon for the next battle. Stage 1 and 2 'camouflaged' SVBIEDs are relatively similar in design and were IS go-to designs during the battle of Mosul. Later, it appears the IS contingent in Raqqah continued where the IS contingent in Mosul left off, further innovating and refining the stage 3 'camouflaged' SVBIED while still also using stage 1 and stage 2 'camouflaged' SVBIEDs. Looking at some of the SVBIED designs used in the battle of Raqqah, they were eerily similar to those used in Mosul.

An excerpt from the first part of this article series gives a reasonable explanation as to how this likely played out:

In the 12th issue of the English-language IS magazine "Rumiyah", released on August 6, 2017, a clue was given about the Raqqah-Mosul connection regarding camouflaged SVBIEDs. In an interview with the (unnamed) IS military commander of Raqqah, he is asked about what effect the battle of Mosul has on the battle of Raqqah. He answers that *"the brothers in Mosul employed new tactics[…]"*, and that "*the brothers' experiences have been passed on to all the wilayat (provinces) so they could benefit from them, both militarily and in terms of iman (faith)[…]"*. While he doesn't specifically mention SVBIEDs, it's highly likely that information about new SVBIED designs was shared by the IS contingent in Mosul with the one in Raqqah, especially since it's their most important type of weapon. Considering that Raqqah was the only major city left under IS control after the recapture of Mosul city, it's only natural that they would be the ones to continue innovating within camouflaged SVBIED designs, as they were the only province with enough resources to continue doing so on a larger scale. This speaks volumes about the level by which inter-province cooperation with regard to military innovations across IS former territories took place.

SVBIED designs & corresponding surroundings

'Camouflaged' SVBIEDs are an interesting phenomenon, but many overlook the way they fit into the bigger picture regarding IS philosophy on SVBIED use. There are general rules for what type of SVBIED is used in what type of surroundings. The purpose of 'camouflaged' SVBIEDs was to confuse enemy air support and ground troops by emulating visual characteristics of civilian vehicles. The surroundings in which the battle of Mosul took place – Dense urban areas with endless blocks of houses shooting off in every direction – was extremely advantageous to IS. It allowed IS to sneak up on unsuspecting Iraqi contingents set up in civilian houses in the city with SVBIEDs, frequently appearing from around corners that the Iraqis presumed were cleared. Basically, the urban terrain dramatically lowered the Iraqi forces' response time in dealing with incoming SVBIEDs. The introduction of 'camouflaged' SVBIEDs was an attempt at lowering that response time even more. Furthermore, the IS tactic of using SVBIED support teams with quadcopter drones that were in constant radio contact with SVBIED drivers meant that SVBIEDs could easily be guided around threats in realtime, changing its attack course whenever needed. Now, let's compare that to the type of SVBIED used by IS in the open plains outside the city limits. Here, the vast and almost completely unobstructed terrain favoured the advancing Iraqi forces. Their response time in dealing with incoming SVBIEDs was a lot higher than in the city, as they were typically able to spot the SVBIEDs from far away. In an attempt to blend in with the desert surroundings, IS only deployed up-armored SVBIEDs painted in a tan color.

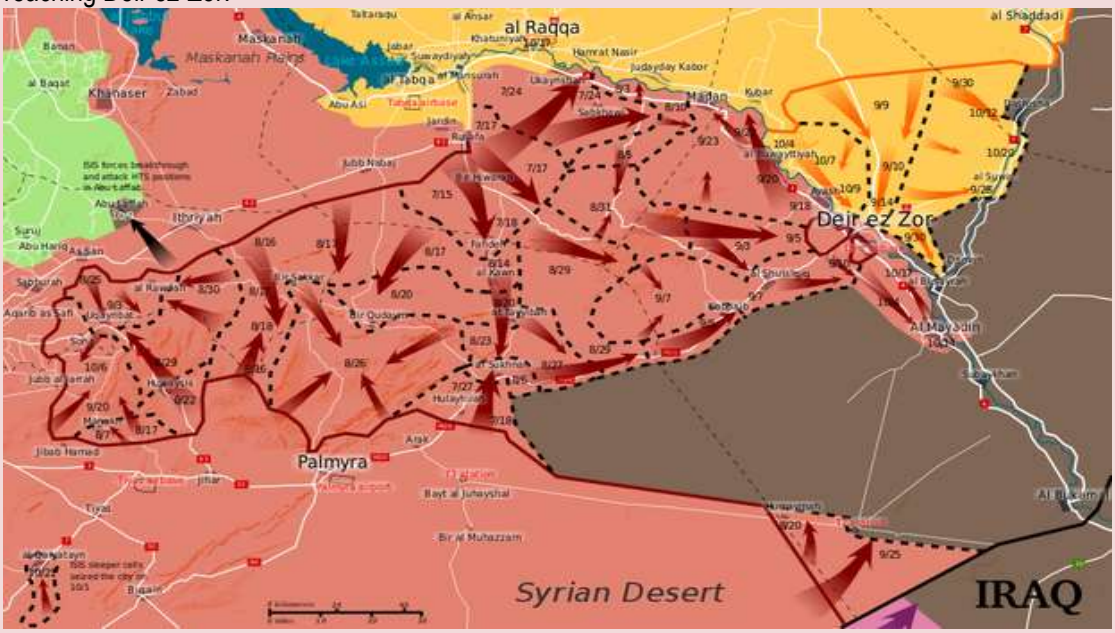
IS used the tan up-armored SVBIEDs up until the Iraqi forces reached the city limits, where they switched to using 'camouflaged' SVBIEDs. This strategy was used in both Eastern Mosul, Western Mosul, in Tal Afar, as well as in Raqqah. Throughout the years it's become apparent that IS very clearly pays attention to the surroundings in which they use their SVBIEDs and modify the SVBIED designs used in each corresponding type of surrounding accordingly.

- **Up-armored SVBIEDs** = Used everywhere
- **Tan up-armored SVBIEDs** = Primarily used in desert areas
- **Camouflaged SVBIEDs** = Primarily used in cities

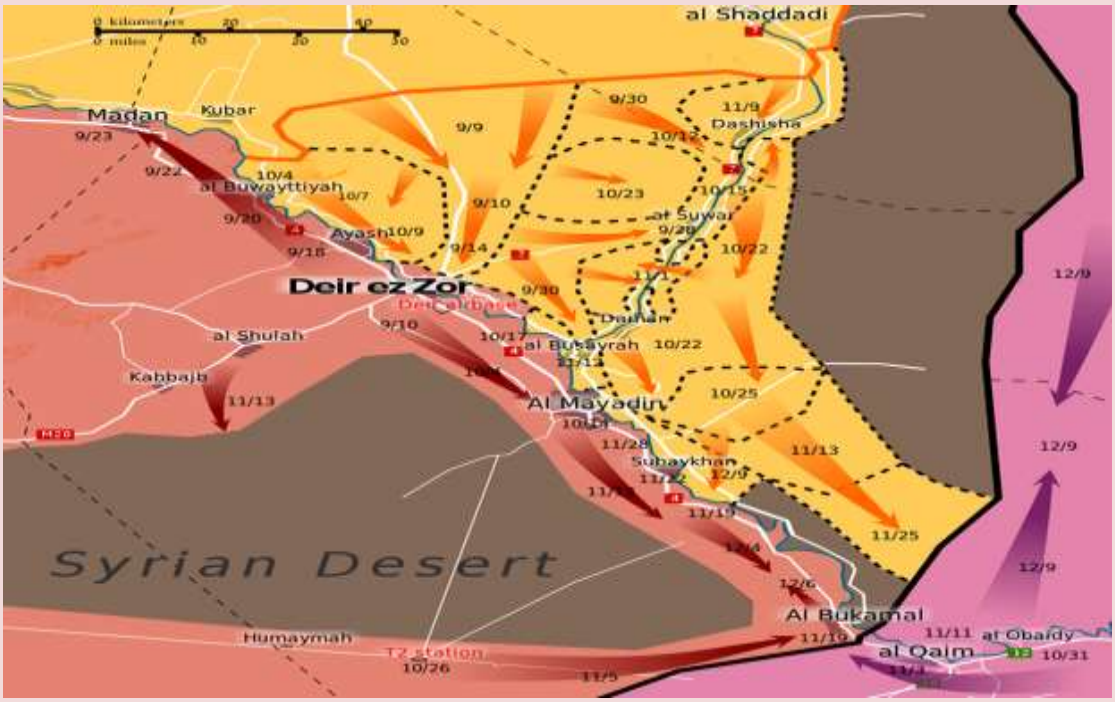
Through the desert & down the Euphrates

After lifting the siege on Kweires Airbase, capturing Deir Hafer, Maskaneh and eventually capturing all of Eastern Aleppo from IS, Syrian loyalist forces set about one of the largest anti-IS offensives seen in recent years. Beginning in July and ending in October 2017, the central Syria offensive resulted in the capture of more than 17000 square kilometres of territory from IS, including the seizure of the strategic town of al-Sukhnah and the surrounding of Deir ez-Zor city. Loyalists made heavy gains in Southern Raqqah, Eastern and Northern Homs, Eastern Hama, and Northwest/Southwest Deir ez-Zor provinces – Eventually reaching the city of Mayadin. On the other side of the Euphrates river, the US-backed and Kurdish-led Syrian Democratic

Forces (SDF) also advanced in the desert and along the river, capturing swathes of territory before reaching Deir ez-Zor.



The subsequent loyalist Eastern Syria campaign, which took place between September and December of 2017, resulted in the lifting of the siege of Deir ez-Zor and the complete recapture of the city, as well as the capture of Mayadin and al-Bukamal.



As can be seen in the above maps, Syrian loyalists were engaged in a "race" down the Euphrates river with the SDF, with each party aiming for the oil fields in Eastern Syria. After capturing Raqqah, the SDF steadily advanced southward along the Euphrates river beginning in September 2017, eventually reaching the Iraqi border. However, despite the success of these offensives, pockets of IS territorial control remained.

SVBIEDs

Looking at IS videos, pictures, along with footage of captured SVBIEDs, I was able to identify at least 43 separate SVBIEDs that were either used by IS or captured by loyalists or SDF

during these offensives. The majority of the SVBIEDs included were either used against or captured by Syrian loyalists.

September 28, 2017 – Captured by loyalists near Qanbar, E. Hama

** Note that the dates included in the above slideshow correspond to when the footage was uploaded, not when each SVBIED was used or captured.*

Here's a breakdown of vehicle and SVBIED types:

Vehicle types

- 27 4×4 vehicles (62,8%)
- 12 SUVs (27,9%)
- 1 Flatbed truck (2,3%)
- 1 Heavy truck (2,3%)
- 1 Van (2,3%)
- 1 Main battle tank (T-55) (2,3%)

SVBIED types

- 18 Up-armored SVBIEDs (41,9%)
- 13 Tan up-armored SVBIEDs (30,2%)
- 7 Stage 1 'camouflaged' SVBIEDs (16,3%)
- 4 Stage 3 'camouflaged' SVBIEDs (9,3%)
- 1 Main battle tank (T-55) (2,3%)

Analysis

After the fall of Raqqah, there was speculation concerning what types of SVBIEDs would be used by IS going forward, especially as Raqqah was the last city formerly under IS control with enough resources to continuously produce large numbers of high-quality SVBIEDs. Looking at the pictures and statistics, the majority of SVBIEDs used during these offensives were standard up-armored and tan-colored SVBIEDs based on 4×4 pick-up trucks and SUVs. As the fighting in these offensives took place almost exclusively in desert areas, this makes sense and fits into the overall IS philosophy of SVBIED usage. Tan-colored SVBIEDs made up more than 30% of the total SVBIEDs featured in the data set, but the fact that not more SVBIEDs were tan-colored can be explained by the loss of Raqqah causing IS in the remaining territories to revert to sub-standard SVBIED workshops littered around the area which eventually ended up being captured by loyalists and SDF.






All of the SVBIEDs used by IS against SDF that were included in this data set are from January/February of this year and were used in the remaining IS pocket along a strip of the Euphrates river, mainly around the towns of al-Bahra and Gahranij. I was not able to document any footage of SVBIEDs captured by SDF during the entire offensive along the Euphrates river, past Deir ez-Zor, until the current frontline. The reason for that may be stricter media regulations in SDF territory, or a tactic favouring immediate destruction of said SVBIEDs instead of organising photo shoots.

The most interesting aspect of this data set is the fact that 'camouflaged' SVBIEDs remained in IS arsenal post-Raqqah, together making up more than 25% of all SVBIEDS documented. The 7 stage 1 'camouflaged' SVBIEDs featured were mostly based on 4×4 vehicles and SUVS, and were deployed by IS in close vicinity to Deir ez-Zor city, as well as

around the towns of al-Bahra and Gahranij in al-Bukamal countryside. While the siege of Deir ez-Zor saw quite a limited use of SVBIEDs in its final 18 months, it's a very strong possibility that information about 'camouflaged' SVBIEDs was sent from the IS contingent in Mosul to both Raqqah and Deir ez-Zor, or from Raqqah to Deir ez-Zor – Allowing IS contingents along the Euphrates the ability to produce similar designs.






Then there was also 4 stage 3 'camouflaged' SVBIEDs featured. These were all different designs, and were not used in the same places.


The example pictured left was captured by loyalists in Eastern Homs (Qanbar), the top right example was used in Homs province, and the bottom right example was used in Deir ez-Zor city. A fourth example (not pictured) was also used in the al-Bukamal countryside. Yet again, this reinforces the idea of IS spreading knowledge of innovations to existing SVBIED designs between its provinces, allowing the receiving IS contingents to make the best out of it. Raqqah city was clearly best suited for the continued development of stage 3 'camouflaged' SVBIEDs because of the resources, facilities, and manpower present there. However, the IS contingents in the central and Eastern Syrian desert, near Deir ez-Zor and along the Euphrates river still attempted to produce these innovative SVBIED designs to the best of their abilities despite the lack of available resources.

In early September 2017, loyalists captured a T-55 main battle tank hull converted into an SVBIED.

Tanks are very rarely used as SVBIEDs, mainly because it's more beneficial to use them in their intended roles. There's an array of other vehicle types that are better suited for use as

SVBIEDs, and even if IS were to use an armoured vehicle as an SVBIED it makes more sense to use a BMP-1 armoured personnel carrier which doesn't offer the same offensive

capabilities as a tank. When tanks are used as SVBIEDs, the turret is always removed, either because they want to salvage a working piece of equipment that doesn't serve a purpose on an SVBIED or because of damage rendering it in-operational. When IS use SVBIEDs based on BMP-1s the turret is also almost always removed, and sometimes fitted on the back of a pick-up truck instead:

Payload innovations

On November 18th, 2017, loyalists captured an interesting SVBIED near al-Bukamal. It appeared to be a tan up-armored 4×4 SVBIED, with one addition:

The SVBIED had an IED mounted forward-facing on the hood armor, connected to the rest of the payload. The SVBIED also had two large IEDs in the trunk of the vehicle, aimed forward and to the sides. This very

obvious attempt at directing the explosive energy toward the target is a relatively new phenomenon, with

similar designs observed in Mosul, Tal Afar, and Raqqah. Pictured below is a variety of examples:

Another new payload phenomenon is the addition of one or more oil barrels connected to the main payload of the SVBIED:

Although not confirmed at the time, many SVBIED attacks that

were filmed with quadcopter drones during the battle of Mosul produced enormous fireballs atypical of your standard payload – Something that raised a lot of suspicion. These pictures from the Eastern Syrian desert and the Syrian-Iraqi border region at least confirms that it's something IS are actually doing. It remains unclear how effective it is.

Continued use of established tactics

One of the SVBIEDs in the data set was a two-man SVBIED, featuring both a driver

and a gunner:

What's interesting about this particular two-man SVBIED is that both the driver and the gunner were handicapped IS fighters.

Handicapped fighters manning SVBIEDs is nothing new. It's been heavily documented in both Raqqah and Mosul, and even well before both those battles.
Using handicapped fighters to man SVBIED missions makes sense. While IS has been keen to show handicapped fighters participating in combat, their combat effectiveness is often dramatically reduced. That's not the case when they're driving an SVBIED. In a video from the battle of Mosul, it became apparent how even paraplegics can operate an SVBIED with only minor adjustments. The body and legs are tied to the vehicle, with crutches tied to the pedals allowing the fighter to operate the SVBIED without using his legs.

While SVBIED support teams with quadcopter drones was a very common sight during the battles of Raqqah and Mosul, that was naturally not the case during these offensives. The tactical advantage of using such support teams works best in an urban environment (short range), while its use in open desert plains serves as more of a propaganda tool. Still, there was around a dozen SVBIED attacks recorded via quadcopter drones.

In this picture from an SVBIED attack on SDF near al-Bahra village (al-Bukamal countryside) in early February this year a motorcycle-borne guide can be seen driving ahead of the SVBIED. His purpose is to guide the SVBIED driver from the forward hide site to the frontline.

This tactic has also been observed countless times, both in Mosul, Raqqah, and elsewhere:
IS have also continued to brief SVBIED drivers on the target just before departure using satellite imagery. This is also sometimes done with pre-recorded quadcopter drone footage of the target site.

Again, this tactic is not new, and has been observed many times before:

Conclusion

The continued use of 'camouflaged' SVBIEDs in what remains of IS territories is testament to the importance of IS inter-provincial military cooperation. And while they're bound to be left without any territorial presence in Syria and Iraq in the near future, their legacy lives on.

For some people it's easy to dismiss the Islamic State's use of SVBIEDs as nothing more than a "Jihadi Mad Max" re-enactment, but there's so much more to it. A lot of thinking has gone into designing, developing and field-testing all the different types of SVBIEDs we've seen used in the past years. There's a grand philosophy behind it all, clearly determining the most appropriate type to be used for each type of surrounding or target. All the different SVBIED designs currently in existence have been developed with a clear thought behind them. A change in battlefield circumstances, type of fighting or the introduction of new counter-SVBIED tactics all spur IS innovation of SVBIEDs, with the introduction of new SVBIED designs causing reactions and counter-reactions, further spurring innovation.

Front-end loader SVBIEDs breaching berms, two-man SVBIEDs suppressing targets, stage 1-3 'camouflaged' SVBIEDs fooling the enemy, payloads with aimed interior or exterior charges and oil barrels, SVBIED support teams with quadcopter drones, standardisation of armor kits, and more. These are just some of the things introduced by IS. Inter-provincial military cooperation within IS former territories made sure all IS contingents were made aware of and continued innovating and developing new SVBIED designs and tactics to counter the counter-SVBIED tactics used by their enemies. The SVBIED is without a doubt the most powerful type of weapon that can be constructed with ease and deployed by a non-state actor, but the vast scope by which IS

have employed SVBIEDs (more than 2000 in the last 2 years) is unparalleled in the history of the weapon's use.
Geography, territorial control, resource availability and surroundings are all important factors determining what type of SVBIED is used. It's not a black or white issue. Covert and up-armored/camouflaged SVBIEDs are used simultaneously by IS in different areas depending on varying degrees of territorial control and the other factors mentioned above.
The most dangerous aspect of all this is the legacy they leave behind. All of these different SVBIED designs, tactics and details have been neatly documented over the years, technically allowing any non-state group in the future with an ideology allowing for such attacks to be inspired and continue where IS left off. That's not even counting all the unpublished knowledge that continues to spread between IS provinces worldwide.
It remains to be seen what the future holds, but one thing is sure. SVBIEDs will continue to be used.

Bike spark plugs being used to trigger IEDs

Source: https://www.tribuneindia.com/news/nation/bike-spark-plugs-being-used-to-trigger-ieds/629465.html

July 30 – Security forces have stumbled upon the use of commonly available spark plugs in automobile engines being used by terrorists and Naxals to detonate improvised explosive devices (IEDs).

A motorcycle spark plug with two electric cables attached to it was recovered on Monday by the Indo-Tibetan Border Police Force (ITBP) from a site where a large IED was detected during anti-Naxal operations in Chhattisgarh.
"This is for the first time that such a contraption has been recovered, which shows improvisation is being done with easily and cheaply available material and that technically savvy minds are at work," an ITBP officer said. "It is also possible that such items may have been used in other parts of the country to trigger IEDs," he added.
IEDs are increasingly being used by Maoists in India and these have been a major threat to the Army as well as paramilitary personnel deployed in anti-terrorist and anti-naxal operations in Jammu and Kashmir, north-east as well as Maoist-affected areas in Central India. Scores of personnel have lost their lives to IEDs.

How it works

- Experts say plugs may have been used to ignite detonator embedded into IED
- Intense heat generated in spark channel causes the ionised gas to expand quickly like a small explosion
- It in turn sets off the thermo-chemical reaction chain that causes the explosion
- Wires attached to plug would have been connected to a battery for power source to produce spark

Heathrow scanner trial could ease airport liquid ban

Source: https://www.bbc.co.uk/news/uk-44925635

July 23 – A trial of new scanners at Heathrow Airport could mean passengers will not have to remove liquids from their hand luggage.
The machines take a 3D X-ray, allowing security staff to check items without requiring them to be removed from bags, and can detect explosives.
The worldwide rules began in 2006 after a terror plot was stopped by UK police.
The Department for Transport said a "small number" of trials was set to last between six and 12 months.
A DfT spokesperson said: "The UK has some of the strictest security measures in the world, and we are leading the way in using new technology to improve security screening and provide a better experience for passengers.
"If successful, this could lead in future to passengers no longer needing to remove items from hand luggage for screening."

The DfT added: "We continue to work closely with our international counterparts to harness the latest advances in technology."
The **new computerised tomography (CT) scanners** have also reportedly been tested at Amsterdam's Schiphol airport and John F Kennedy airport in New York. It comes five years after the European Commission said it hoped the restrictions across Europe could be ended through "technological screening".

'Rules remain'
The current rules specify that containers of liquid must hold no more than 100ml and fit in a small transparent, resealable plastic bag, which needs to be removed from hand luggage during pre-flight security checks.
They were introduced amid fears transatlantic flights could be brought down by terrorists hiding liquid explosives in small drink bottles.
But it has resulted in longer security checks, and has coincided with the rise in travel on low-cost airlines where many passengers only carry hand luggage.
Security policy for all UK airports is set by the DfT.
The DfT said the new technology allows baggage screeners "to use 3D imagery to look at objects from all angles".
It said while the the trials take place, the rules remain the same and passengers should expect to remove items if requested during the security screening purposes.
A Heathrow spokeswoman confirmed the airport was "looking at new technologies that can both improve the passenger experience and strengthen our security".

TSA considering eliminating screening at smaller airports

Source: https://edition.cnn.com/2018/08/01/politics/tsa-considering-eliminating-screening-at-smaller-airports/index.html

Aug 01 – The Transportation Security Administration is considering eliminating passenger screening at more than 150 small and medium-sized airports across the US, according to senior agency officials and internal documents obtained by CNN.

The proposal, if implemented, would mark a major change for air travel in the US, following nearly two decades of TSA presence since the terrorist attacks of September 11, 2001, and comes as the Trump

administration has stepped up screening measures for items such as laptops and tablets. Internal documents from a TSA working group say the proposal to cut screening at small and some medium-sized airports serving aircraft with 60 seats or fewer could bring a "small (non-zero) undesirable increase in risk related to additional adversary opportunity."

"This is so dangerous," a TSA field leader at a large airport said. The individual is not authorized to discuss the matter publicly.

Two senior TSA officials, who asked not to be identified, expressed serious national security concerns over the proposal. They said the idea was explored as far back as 2011 and has been resurrected. The documents referred to some

The internal documents from June and July suggest the move could save $115 million annually, money that could be used to bolster security at larger airports.

According to the proposal, passengers and luggage arriving from these smaller airports would be screened when they arrive at major airports for connecting flights instead of the current practice of joining the already screened population at the larger airport. The high-volume airports have greater capacities and more advanced security measures than smaller locations, the documents say.

CNN terrorism analyst Paul Cruickshank said it was "stunning that this is even seriously being considered."

"Al Qaeda and ISIS still regard aviation as a priority target -- that includes aircraft where you have fewer than 60 people on board," he said. "They would see that as a way to hit the headlines. They would see that as a way to inflict severe economic damage on the United States. If you have an aircraft of 50 or so people being blown out of the sky there is going to be a great amount of panic and there will indeed be significant economic reverberations, and of course significant loss of life."

150 small airports in addition to some midsize ones. TSA currently screens passengers at 440 airports, according to its website.

The working group determined that the policy change would affect about 10,000 passengers who are screened by 1,299 TSA employees daily, which amounts to about 0.5% of the people who fly out of US airports on any given day. The report not list specific airports that could be affected by the policy change.

TSA spokesman Michael Bilello said the study reflects a recurring debate within the agency about its legal requirements.

"This is not a new issue," he said via email. "The regulations which established TSA does not require screening below a certain level, so every year is 'the year' that TSA will reconsider screening." Bilello did not respond to a request for the text of the regulations.

The two TSA senior officials said the level of activity around the proposal this year -- the formation of a working group to conduct a risk and cost analysis -- mean this is more than an annual exercise.

The documents said a TSA working group of 20 people, including a representative of the agency's administrator's office,

met on June 21 to examine the potential risks of the policy change. An internal TSA memo dated July 17 from TSA Director of Enterprise Performance and Risk Strategy Jerry Booker to the TSA administrator's chief of staff, Ha Nguyen McNeill, outlines the group's findings. It contains no formal recommendation.

Small airport security issues

The concept of rolling back security at regional airports recalls the coordinated attacks that brought the TSA into existence.

Two of the September 11 attackers first flew from an airport in Portland, Maine, to Boston before boarding American Airlines flight 11, forcing entry to the cockpit and steering it into the North Tower of the World Trade Center. While Portland's airport likely would not be included in the proposal because of its volume of passengers, the 9/11 attackers perceived the airport to be less secure because of its relatively small size.

The proposal asserts that small aircraft would not be "attractive" to terrorists. The documents conclude that attacks with small aircraft would not as attractive a "payoff" because "the potential for loss of life" would be lower than terrorists could achieve with larger planes.

Juliette Kayyem, who was an assistant secretary for intergovernmental affairs at the Department of Homeland Security in the Obama administration, said small planes could still be weaponized to cause major loss of life.

"People, weapons, dangerous goods and what's boarding the plane are all potential risks," said Kayyem, a CNN analyst. "TSA is falling into the trap that this is just about terror. A gun could be brought on board too."

Shift from earlier administration rhetoric, policy

The proposal under consideration by TSA is different from the agency's current approach to screening passengers.

Since TSA's inception in 2001, the trend has mostly been toward more enhanced security measures, including limiting gels and liquids in carry-on bags, requiring more advanced screening and directing passengers to remove shoes and belts for screening.

In June 2017, then-DHS Secretary John Kelly announced a laptop ban from carry-ons affecting nearly 280 airports in more than 100 countries.

"Terrorists want to bring down aircraft to instill fear, disrupt our economies and undermine our way of life," Kelly said. "And it works, which is why they still see aviation as the crown jewel target."

He continued, "The threat has not diminished. In fact, I am concerned that we are seeing renewed interest on the part of terrorist groups to go after the aviation sector -- from bombing aircraft to attacking airports on the ground."

EDITOR'S COMMENT: When you strengthen the door the windows are becoming weaker. Remember that person [Esteban Santiago] who put his gun in his baggage in Alaska and started shooting when he arrived at this destination airport [Florida's Fort Lauderdale/Hollywood International Airport] (2017)?

Venezuelan President survives apparent drone assassination attempt

Source: https://edition.cnn.com/2018/08/04/americas/venezuela-maduro/index.html

Aug 05 – Venezuelan President Nicolas Maduro survived an apparent assassination attempt Saturday after several drones armed with explosives flew toward him during a speech at a military parade.

Live footage of the event showed him suddenly looking up startled mid-speech, while beside him his wife, Cilia Flores, winces after a loud bang.

Dozens of soldiers are also seen scattering during the event to commemorate the 81st anniversary of the Venezuelan national guard in the capital of Caracas.

Seven members of the national guard were hurt during the attack, which the president blamed on far-right elements and Colombia's outgoing president, Juan Manuel Santos.

A Colombian presidential source told CNN that Maduro's accusations were "baseless."

"I'm alive and victorious," Maduro said in a national television address hours after what he described as an assassination attempt.

The president added that there were two explosions, seconds apart, and that he initially thought they were fireworks as part of the military parade.
Venezuela's Minister of Communication, Jorge Rodriguez, said preliminary information showed the explosions came from several "drone-type flying devices" containing explosive charges that detonated in the vicinity of the presidential stage and in some areas of the parade.
A photo posted on Twitter by Freddy Nanez, head of the Venezuelan state run news channel VTV, shows bodyguards shielding Maduro following the explosions.

Investigation underway
Venezuela's attorney general, Tarek William Saab, told CNN he had ordered an investigation into the incident, assigning three prosecutors to the investigation.
Saab was close to the president during the event, and says the drone responsible for filming the event exploded. He added that a second explosion followed.
During his speech to the nation following the incident, Maduro said the investigation started immediately and that some of those involved in the attack had already been captured and charged, although he did not specify the charges against them.
Speaking in front of members of the military and other government officials, Maduro also said that authorities were able to obtain evidence of the attack and said the investigation was in an advanced stage.
He blamed the Venezuelan political far right in collaboration with the Colombian far right, and the current Colombian President Santos of being behind the assassination attack.
He also blamed Venezuelans living in the US.
"The preliminary investigation indicates that many of those responsible for the attack, the financiers and planners, live in the United States in the state of Florida," Maduro said.
"I hope the Trump administration is willing to fight terrorist groups that commit attacks in peaceful countries in our continent, in this case Venezuela."
The Venezuelan government has long blamed Colombia for plotting overthrows and, and far-right elements in Bogota and Miami for attempting to undercut Maduro. Ivan Duque takes over as the Colombian President next week.
A Colombian presidential source told CNN that Maduro's accusations were "baseless," adding Santos was "dedicated to his granddaughter's Celeste baptism, and not taking down foreign governments."
A senior US State Department official traveling with US Secretary of State Mike Pompeo in Indonesia said the US "had heard the reports," and was following closely.

How the remarkable attack unfolded
The military parade took over most of the Avenida Bolivar, one of the main thoroughfares in Caracas, and the president's speech came toward the end of the event.

Video broadcast live on Venezuelan state-run news channel, VTV, showed Maduro talking about an economic recovery, when the audio cuts mid sentence.
Cilia Flores, Maduro's wife, was standing next to him. She looks up and winces.

The crowd at the parade in Caracas disperses after what officials called an attack on the President.

Shortly after, VTV shows video of soldiers and National Guardsman scattering along the avenue.
Manuel Berbín lives nearby and told CNN en Español that he and his wife thought the first explosion were fireworks.
"We heard the first explosion, and we were there thinking that it could have been a firework that exploded close to our apartment" he said. "Then we heard the second explosion, that was very strong. We went to the window, and at that time we saw the soldiers start to run, they started to move the cars quickly, the sirens started going."
Berbin says he saw smoke rising from the area shortly after.
He adds the explosions were very close to each other.

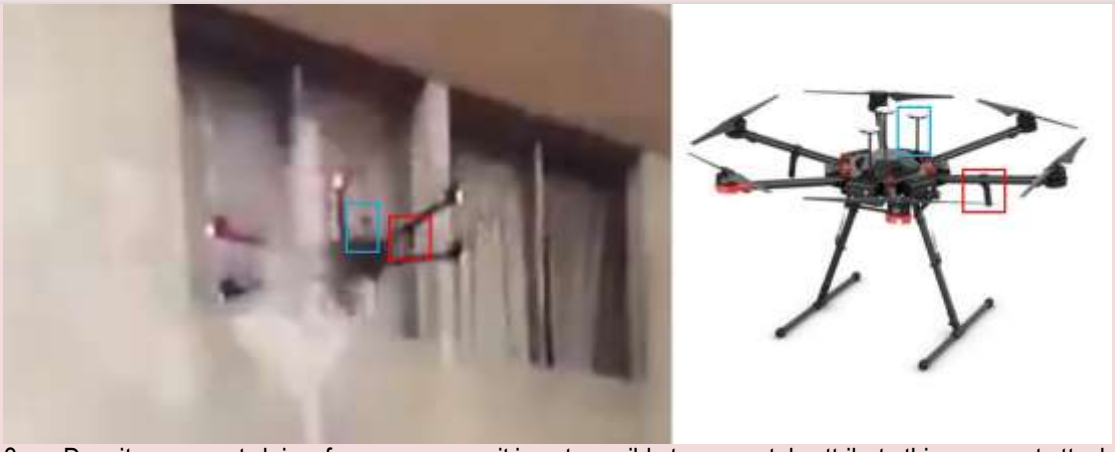
EDITOR'S COMMENT: A bit of surprise to have the first IED drone attack (?) (some speak about a drone carrying a suicide bomb vest) in S. America instead of Europe. But if you examine in depth the current local situation one might take into account that the nexus between cartels and terrorists possesses narco submarines and activities in the Triborder Region along with a known group that could provide "experts" from ME, might provide the know-how related to aerial drone attackes as well. **And if it happened there, it can happen everywhere!**

Did Drones Attack Maduro in Caracas?

August 7, 2018
By Nick Waters
Source: https://www.bellingcat.com/news/americas/2018/08/07/drones-attack-maduro-caracas/

Summary

1. Open source information indicates two drones (DJI Matrice 600?) attempted to attack a parade at which President Maduro was speaking.
2. Both drones likely carried some form of explosive device. One detonated near the parade, the other crashed and then likely detonated, causing a fire.



3. Despite apparent claims from one group, it is not possible to accurately attribute this apparent attack without further information.

▶▶ Read more at source's URL.

***Nick Waters** is an ex-British Army officer and open source analyst. He has a special interest in the conflicts in Syria, as well as social media, civil society, intelligence and security.*
This article was written in collaboration with Giancarlo Fiorella, who runs the In Venezuela Blog and Twitter account, and the Bellingcat Investigation Team.

High- and low-tech solutions for bomb disposal

Source: http://www.homelandsecuritynewswire.com/dr20180808-high-and-lowtech-solutions-for-bomb-disposal

Aug 08 – To ensure bomb techs are on the cutting edge of technology as they address evolving threats, the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) created the

Response and Defeat Operations Support (REDOPS) program. REDOPS connects the 466 bomb squads of varying sizes and budgets across the country with the tools and information they need to perform their duties better, faster and more safely. They look at a variety of sources—including the commercial marketplace, responder communities and international partners—for high- and low-tech solutions.

The reach and impact of REDOPS

The program's creation followed the Boston Marathon bombing in 2013 with the goal of providing support to state and local bomb technicians.

"That was the genesis of the REDOPS program," said William Stout, Deputy Director of First Responder Technologies. "Since that time, we have been able to successfully create and establish relationships with the bomb squad community in conjunction with other federal agencies like the Federal Bureau of Investigations (FBI), the Department of Defense and the Department of Energy."

S&T says that it leverages its relationship with the FBI and other agencies to reach the whole of the bomb squad community across the nation. All bomb technicians receive training and certification from the FBI Hazardous Devices School, which is where the REDOPS program transitions its tools and technologies.

"In essence, this program reaches 100 percent of the community we set out to help," Stout said.

The REDOPS mission is more than delivering tools and technologies; the program also evaluates existing tools to give technicians the peace of mind that their equipment will work as intended in the event of a bomb threat.

"We want to make sure existing tools work safely and effectively by providing objective feedback to better inform the bomb squad community as a whole," said Byung Hee Kim, S&T program manager for REDOPS.

To do that, REDOPS evaluates commercially-available technologies such as X-ray systems, robots or remote firing systems through hands-on operational field assessments. After that the program provides feedback to vendors regarding effectiveness, quality and pricing.

"The feedback comes directly from bomb technicians that are using and evaluating the equipment during the testbed assessments. This feedback is then used to improve the tested technology," said Kim. "So, we are driving vendor innovation to benefit the community."

Finding the best tech for varying bomb squad sizes and budgets

With critical incidents happening in communities nationwide, having tools for all budgets and all sizes of bomb squads is essential for this diverse responder community.

To address these varying needs, REDOPS finds, develops, and evaluates a range of high- and low-tech solutions from various sources. REDOPS regularly scans the marketplace to find the right tools for bomb technician needs. For example, the REDOPS team has found inspiration from other first responder communities such as firefighters, as their tools can be dual use.

"There are times when bomb squads run into challenges for which there are limited technical solutions, so they develop their own solutions," said Kim. "These technicians are very smart. At times they use off-the-shelf commercial materials to build the necessary solution — we then test them for safety and share them across the bomb squad community."

Handmade tools for handmade bombs

"We realized in this program that just because a bomb technician has an expensive piece of technology, it doesn't mean that they can do their job effectively," said Kim. "Sometimes handmade tools can do the job equally well, if not better; and they are more cost effective."

Instead of purchasing expensive technology that may not work in the field, they make it from materials found in their local home improvement stores. Bomb technicians frequently develop tools to meet their evolving needs, save their bomb squad money and when shared, support the broader bomb squad community.

Following are some of the cost-effective tools the REDOPS team has recommended for bomb squads across the nation to incorporate into their toolbox:

Rubber grip for door handles/knobs (approx. $10). One issue bomb technicians have is that they often cannot access doors or pull doors effectively from a distance or with a robot due to its linear movement. The rubber grip provides the robot with a tight grip that can be used on door handles and car doors.

Remote key/Remote door opener (approx. $20). Current robot models cannot turn a key in the door to open it and sometimes even break the key. Bomb technicians use this long-rod key holder to insert and turn a key.

Fiber optic hinge holder (approx. $5). Bomb-disarming robots are tethered on long fiber optic cables, which are expensive, very fragile and hard to repair. This tool adds a protective layer for the cable to ensure maximum maneuverability for the robot without the risk of damaging the cable.

Kite reel for lines (approx. $15-$60). One of the challenges that

bomb technicians have, even the tactical community, is how to carry lines; and lines can have multiple uses. Kite reel strings with ultimate strength of 200 lbs. are commercially available.

Underwater cutting tool (approx. $30-$40). This sharp tool is used on dry land by the safety community to cut a seatbelt under which someone is stuck; it can also cut clothing, Kevlar ropes, cotton ropes, and plastics. But REDOPS recommends it for underwater situations as well. If there is a bomb underwater with a supporting line, this tool can cut it.

"We found this simple tool through our market research on a safety website," said Kim. "One of the things we do, when we look for things like this, is evaluate every single possibility."

Finding solutions internationally

The bomb squad community isn't limited to the United States, which is why the REDOPS program works with international partners to develop technologies that can benefit localities worldwide. A recent example of this is the program's partnership with the Israeli National Police. Together they are working on a dual-arm robot project.

Bomb robots currently in use are single-arm robots.

"So, when looking at how to negotiate a bomb, the bomb squad will have two appendages to work with instead of just one," said Kim.

To ensure the dual-arm robot meets the needs of both countries, several U.S. bomb squads from New Jersey State Police, Fairfax County Police and Michigan State Police are participating in the various stages of development to provide user feedback for the final product. Multiple prototypes will be available in December 2018 for the bomb squad community to test and to be able to continue to refine the secondary robotic arm.

Join the community!

The bomb squad community is in great need of solutions at various price points and capabilities. REDOPS aims to meet these needs by working with the community and delivering information and tools in an effective and efficient way to combat homeland security threats.

"If you are a bomb technician, you may be interested in joining the REDOPS community at S&T's First Responders Communities of Practice (FRCoP)," S&T says. "FRCoP is a network of vetted, active and retired first responders, emergency response professionals and federal, state, local or tribal homeland security officials. This network not only offers information repositories and content creation tools, but also provides networking capabilities for practitioners across the country to connect with one another in a trusted, online environment."

CBRN(E): With or Without the (E)xplosive

By George Javier McKerrow

Source: http://nct-magazine.com/august18/cbrne-with-or-without-the-explosive/

Debates around whether CBRN teams are also responsible for devices containing explosives have gone on for years, hence some groups being CBRN while others are CBRNE. Certain groups will even refer to it as CBRNe, with the lowercase "e" minimizing their association with explosives.

In some cases, hazardous CBRN devices containing explosives often require cooperation between the CBRN team and an EOD team. However, there is the opportunity for a stalemate when it comes to handling or defeating a device if neither team can agree on the correct approach. For example, the EOD team may have protocols limiting their approach on devices that contain radiological elements, and the CBRN team's protocols may restrict their procedures for IEDs, regardless of whether a radiological threat is also suspected. It is crucial that training between these two groups take place in a safe, controlled environment so the teams can develop cooperative standard operating procedures.

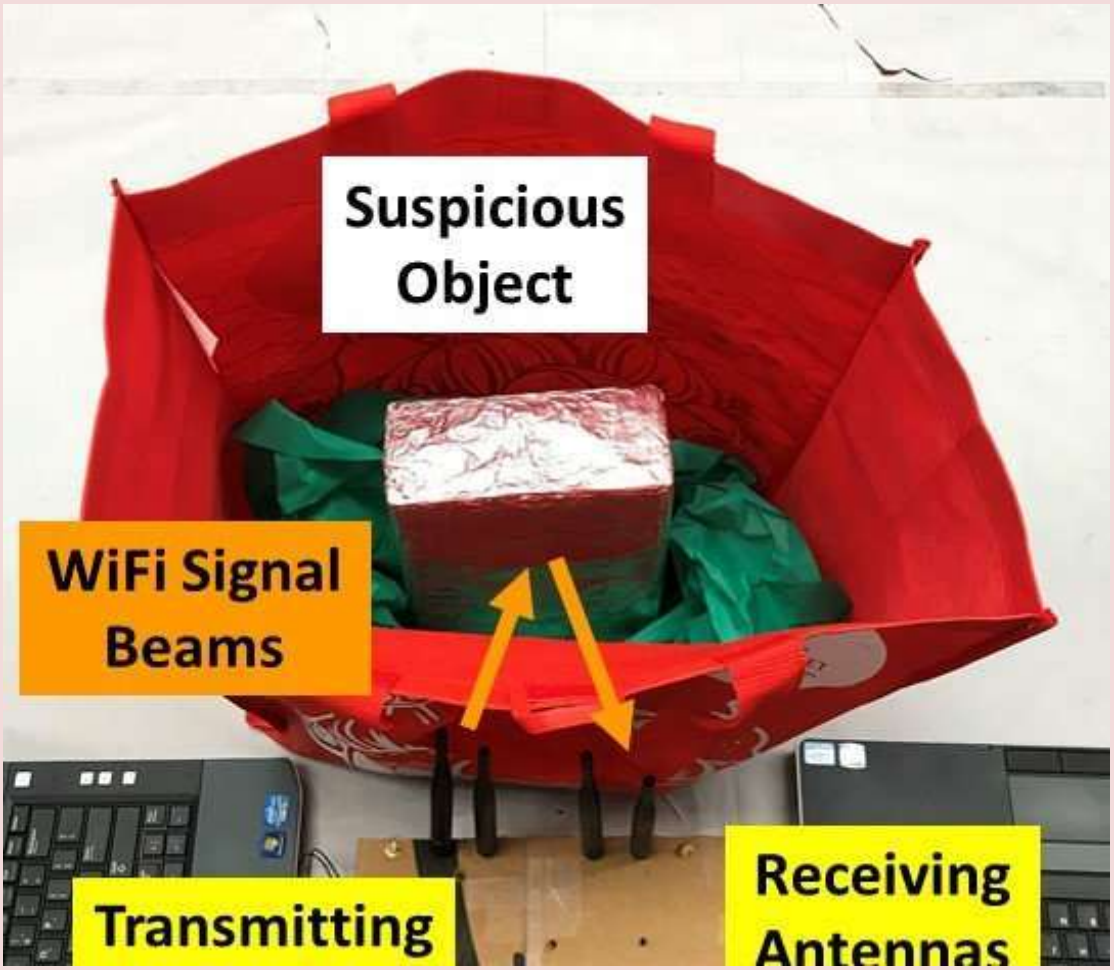
▶▶ Read the rest of this article at source's URL.

George McKerrow *is a certified counter terrorism practitioner who continues to conduct training, develop equipment, organize international training events. He has been a guest speaker at numerous global counter terrorism conferences and workshops all around and has conducted training in US, Canada, UK, SE Asia,*

Europe & the Middle East. He enlisted into the British Army in 1984 and attended training to be a Paratrooper, Explosive Ordnance Disposal Officer and a High-Risk Search Advisor. He attended extensive training at the UK Defense Explosive Ordnance Disposal School (DEODS) and the UK National Search Academy. George has been deployed operationally on EOD and HRS missions in Northern Ireland, Bosnia, Kosovo, Afghanistan & Iraq.

Common WiFi can detect weapons, bombs and chemicals in bags

Source: https://news.rutgers.edu/common-wifi-can-detect-weapons-bombs-and-chemicals-bags/20180814



Aug 15 – Using common WiFi, this low-cost suspicious object detection system can detect weapons, bombs and explosive chemicals in bags, backpacks and luggage. Credit: Data Analysis and Information Security (DAISY) Lab led by Professor Yingying Chen

Ordinary WiFi can easily detect weapons, bombs and explosive chemicals in bags at museums, stadiums, theme parks, schools and other public venues, according to a Rutgers University-New Brunswick-led study.

The researchers' suspicious object detection system is easy to set up, reduces security screening costs and avoids invading privacy such as when screeners open and inspect bags, backpacks and luggage. Traditional screening typically requires high staffing levels and costly specialized equipment.

"This could have a great impact in protecting the public from dangerous objects," said Yingying (Jennifer) Chen, study co-author and a professor in the Department of Electrical and Computer Engineering in Rutgers-New Brunswick's School of Engineering. "There's a growing need for that now."

The peer-reviewed study received a best paper award at the 2018 IEEE Conference on Communications and Network Security on cybersecurity. The study—led by researchers at

the Wireless Information Network Laboratory (WINLAB) in the School of Engineering—included engineers at Indiana University-Purdue University Indianapolis (IUPUI) and Binghamton University.

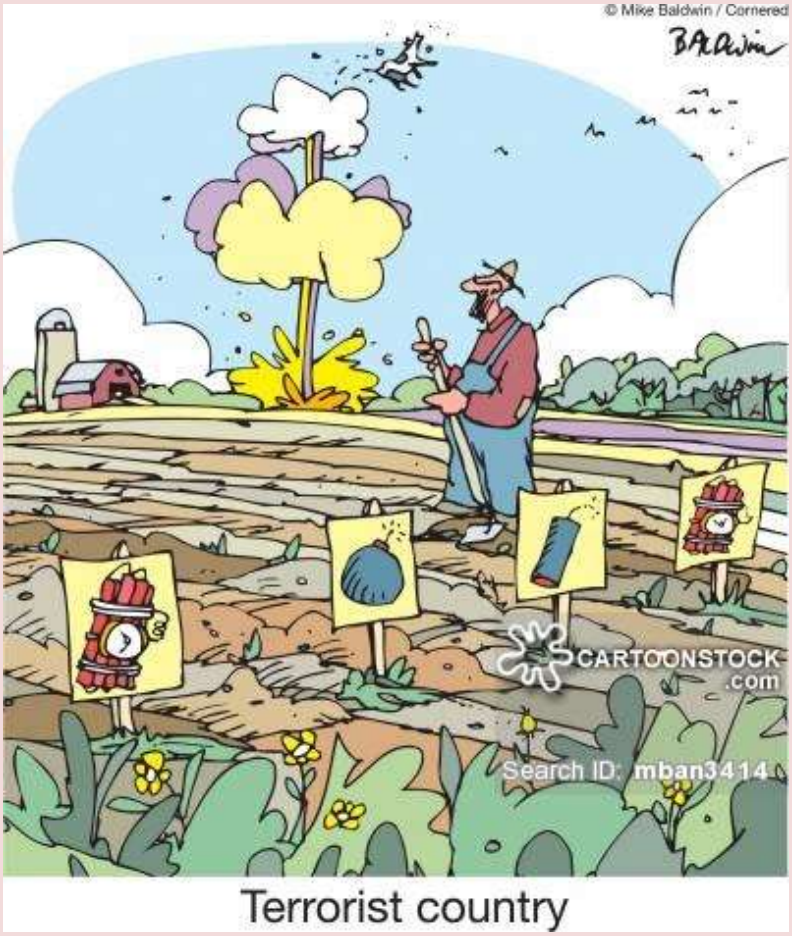
WiFi, or wireless, signals in most public places can penetrate bags to get the dimensions of dangerous metal objects and identify them, including weapons, aluminum cans, laptops and batteries for bombs. WiFi can also be used to estimate the volume of liquids such as water, acid, alcohol and other chemicals for explosives, according to the researchers.

This low-cost system requires a WiFi device with two to three antennas and can be integrated into existing WiFi networks. The system analyzes what happens when wireless signals penetrate and bounce off objects and materials.

Experiments with 15 types of objects and six types of bags demonstrated detection accuracy rates of 99 percent for dangerous objects, 98 percent for metal and 95 percent for liquid. For typical backpacks, the accuracy rate exceeds 95 percent and drops to about 90 percent when objects inside bags are wrapped, Chen said.

"In large public areas, it's hard to set up expensive screening infrastructure like what's in airports," Chen said. "Manpower is always needed to check bags and we wanted to develop a complementary method to try to reduce manpower."

Next steps include trying to boost accuracy in identifying objects by imaging their shapes and estimating liquid volumes, she said.



ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C²BRNE DIARY

CYBER NEWS

Report: Russian hackers came close to causing U.S. blackouts last year

Source: http://www.homelandsecuritynewswire.com/dr20180724-report-russian-hackers-came-close-to-causing-u-s-blackouts-last-year

July 24 – Hackers working for Russia claimed "hundreds of victims" last year in a major, long-running campaign that enabled them to gain control over some U.S. electric utilities, where they could have caused blackouts, the *Wall Street Journal* is reporting.

Citing officials at the U.S. Department of Homeland Security, the *Journal* reported on July 23 that the Russian hacking campaign has likely continued this year and involves a state-sponsored group known as Dragonfly or Energetic Bear.

The hackers broke into supposedly secure networks owned by utilities with relative ease by first penetrating the networks of vendors who had trusted relationships with the power companies, the *Journal* reported.

"They got to the point where they could have thrown switches" and disrupted power flows, Jonathan Homer, a department analyst, told the *Journal*.

"Hundreds" of victims

The department has been warning utility executives with security clearances about the Russian threat to critical infrastructure since 2014.

But on July 23, the department gave out detailed information about the intrusions publicly for the first time at an unclassified briefing for the industry. It did not provide the names of alleged victims, but said there were "hundreds."

It also said some companies still may not know they were compromised, because the attacks used credentials of actual employees to get inside utility networks, potentially making the intrusions more difficult to detect.

"They've been intruding into our networks and are positioning themselves for a limited or widespread attack," Michael Carpenter, former deputy assistant secretary of defense, who is now a senior director at the Penn Biden Center at the University of Pennsylvania, told the *Journal*. "They are waging a covert war on the West."

Russia has denied targeting critical infrastructure.

Homer told the *Journal* that the long-running cyberattack, which surfaced in the spring of 2016 and continued throughout 2017, exploited relationships that utilities have with vendors who have special access to update software, run diagnostics on equipment, and perform other services that are needed to keep millions of pieces of gear in working order.

He said the attackers began by using conventional tools — spear phishing e-mails and watering-hole attacks, which trick victims into entering their passwords on malware-infected websites — to compromise the corporate networks of suppliers, many of whom were small companies without big budgets for cybersecurity.

Automated attacks?

Once inside the vendor networks, they pivoted to their real focus: the utilities, officials told the *Journal*. They said it was a relatively easy process, in many cases, for the intruders to steal credentials from vendors and gain direct access to utility networks.

Then they began stealing confidential information. For example, the hackers vacuumed up information showing how utility networks were configured, what equipment was in use and how it was controlled.

The hackers also familiarized themselves with how the facilities were supposed to work, because attackers "have to learn how to take the normal and make it abnormal" to cause disruptions, Homer told the *Journal*.

The department said it plans three more industry briefings and hopes to determine whether there are any new network infections, and whether the hackers have figured out ways to defeat security enhancements like multifactor authentication.

In addition, the department is looking for evidence that the Russian hackers are automating their attacks, which investigators worry could presage a large increase in hacking efforts.

It isn't yet clear whether the hackers used their access to prepare for some future, devastating blow to the U.S. electric grid, investigators told the *Journal*.

Cyberwar: What happens when a nation-state cyber attack kills?

Source: https://www.zdnet.com/article/cyberwar-what-happens-when-a-nation-state-issued-cyber-attack-kills/

July 24 – The increasing sophistication and power of state-backed cyber attacks has led some experts to fear that, sooner or later, by design or by accident, one of these incidents will result in somebody getting killed.

It might sound far-fetched, but a former head of the UK's intelligence agency has already warned about the physical threat posed by cyber attacks and the potential damage they could do.

"Nation-states are getting more sophisticated and they're getting more brazen. They're getting less worried about being caught and being named -- and of course that's a feature of geopolitics," said Robert Hannigan, who served as director general of GCHQ from 2014 to 2017.

"The problem is the risk of miscalculation is huge," he said, speaking at a security conference in London last month. "If you start to tamper with industrial control systems, if you start to tamper with health systems and networks, it feels like it's only a matter of time before somebody gets hurt and somebody is ultimately killed."

The mention of health systems is a reminder perhaps of last year's WannaCry ransomware outbreak, which crippled large parts of the UK's National Health Service. Thousands of appointments were cancelled, causing disruption and inconvenience for patients around the country.

No critical systems were hit, but given the nature of WannaCry -- which the US, UK, and others have blamed on North Korea -- that was likely due to luck rather than planning.

With attacks against hospitals, transport, power plants, or other critical national infrastructure, attackers are playing a dangerous game -- but that hasn't stopped clandestine, targeted campaigns against infrastructure.

Perhaps the most famous example is Stuxnet, malware designed to damage Iranian uranium centrifuges which was uncovered in 2010. The destructive attack on the industrial systems put Iran's nuclear program back by years, and is believed to have been a joint cyber operation by the US and Israel.

However, Stuxnet was designed to be limited in its impact: in the years since, those attacking industrial control systems are becoming more reckless. This was demonstrated in December last year when hackers used malware to disrupt emergency shutdown systems at a critical infrastructure firm in the Middle East.

Analysis of the Triton malware by researchers at security company FireEye suggests that the shutdown was unintentional and that it was inadvertently caused while preparing the malware to do physical damage.

The shutdown came as a result of a fail-safe mechanism and no physical damage was done -- but the unpredictable nature of the malware could have resulted in much worse.

"If the intent of the attacking group was to make the plant explode, lives lost by cyber attack could've happened," Jing Xie, senior threat intelligence analyst at Venafi, told ZDNet.

"I have no doubt it's just a matter of time that someday cyber attacks will definitely cause direct harm to people," she added.

So what happens when a cyber attack by one nation-state leads to loss of life inside another country?

In 2014, NATO updated its policy so that a serious cyber attack could be covered by Article 5, its collective defence clause. Legal experts have also made it clear that a serious digital attack could be considered to be the equivalent of an armed attack. But what would happen in reality is still uncertain.

"It's been a debate in policy circles for over a decade, if not longer: when does cyber activity cross over into a domain which needs a kinetic response from a military source?" said Jon Condra, director of Asia Pacific Research at Flashpoint.

"The current legal system which exists around war isn't necessary up to date with this type of problem. The borders of cyberspace are much more malleable and unclear, so it's not entirely clear when a nation-state has a moral or ethical right to react in a forceful way."

If one of these attacks did cause a substantial loss of life and could be clearly attributed to a nation-state, there would have to be some sort of very serious response, said Condra. "Even outside the ethical and moral factors, the political pressure inside the country affected to do something substantial would probably force hands."

Others take a more straightforward view.

For Giovanni Vigna, professor in the Department of Computer Science at the University of California in Santa Barbara and co-founder of security firm Lastline, it's simple: "It's an actual war," he said.
"It would very likely trigger hostilities," said Jonathan Reiber, chief strategy officer for cyber policy in the Office of the Secretary of Defense under the Obama administration, and now head of cyber security strategy at Illumio.
"That's because it's like an attack in any other domain," he continued, adding: "In 2015, we declared that cyber attacks of significant consequence will require a response and the US will respond in a time, manner, and place of its choosing to an attack on the United States. The response may not be through cyber means," he added, referring to the DoD cyber strategy report he authored.
One of the key issues with cyberwar is that it's often difficult to provide proof of who is behind attacks. Cyber attackers operating at all levels do as much as possible in order to cover their tracks and avoid being hit with the blame.
In the case of the Triton incident, the attacks haven't been formally attributed -- other than by researchers pointing to it being the work of a state-sponsored group.
"Attribution is the sticky bit. Attribution is broken to some extent," said Reschke.
A case in point is the Olympic Destroyer malware which targeted South Korea during this year's Winter Olympics. In the days following the attack, research firms published conflicting reports on attribution -- China, North Korea, and Russia were all claimed as the origin of the malware.
"The problem with attribution is it's extremely difficult, it becomes almost a guessing game," said Vigna. "You might find artefacts that suggest a particular operation, but what if somebody left these to deceive -- somebody left something in Russian to blame the Russians? So, unless you have some sort of side channel to confirm this happened, it becomes very difficult to determine who did what."
But sometimes attackers do slip up and the authorities can determine who conducted the campaign: WannaCry was traced to North Korea and NotPetya has been attributed to the Russian military. In the case of a cyber attack which causes loss of life and can be traced to a perpetrator, it's highly likely that the victim would want to react, though not necessarily by another cyber attack.
The United States has issued sanctions against Russia for its involvement in cyber attacks, and an attack that resulted in loss of life would demand a greater response.

The Petya ransom note. Image: Symantec

In the most extreme circumstances, a nation could decide that the only response to a harmful cyber attack on its soil could be a military response. Such a response would probably be in reaction to a substantial loss of life, but in the complex world of international geopolitics, even the smallest spark could lead to an unprecedented reaction.

"I don't know what point we get to when things start to get destructive and when that tipping point is. It's always hard to measure those tipping points when a country decides enough is enough," said Reschke.
Speaking at the Infosecurity Europe conference in London, Hannigan suggested an attack that lead to the death of citizens would lead to a physical response.
"If one of their attacks had ended up with patients in the US dying or being seriously harmed, the pressure on a US government to do something and to do something pretty physical and decisive would be huge. It would be for any Western politician, but particularly in the US," he said.
Fortunately, there has yet to be a nation-state backed cyber attack which is thought to have directly led to the harm or death of citizens in another country -- which means it isn't too late to come to agreements to what an appropriate response to such an event could be.
"The international community needs to come to some sort of consensus about how these types of activities are going to be responded to, what kind of consequences there will be for them," said Condra.
For Reiber, one way stop escalation is to ensure cyber attacks are punished to act as a deterrent.
"Any kind of cyber intrusion that occurs -- whether it's the theft of $50, a destructive attack, or election manipulation -- requires some sort of punitive cost back on the actor," he said.
"If actors perceive that a range of actions are permissive, they'll pursue a whole range we can't necessarily imagine. But if you begin to impose costs for all of them, then that says the world is rallying against what they're doing and need to stop."
But for all this talk of aggression and punishment, there's likely only one thing which could prevent a destructive cyber attack by a nation-state causing loss of life in the first place.
"Technology doesn't kill people, people kill people: to a degree, you have to take a step back and set the political conditions for resolving disputes between states or between peoples within a state at a political level," said Reiber.
"Over time, that will decrease the chance that a group will use cyberspace operations against an opposing party. Clearly, peace between a pair of states will decrease the likelihood of attacks."

Countering 'Smart' Terrorists Who Use Online Gaming Platforms

Source: https://intpolicydigest.org/2018/07/27/countering-smart-terrorists-who-use-online-gaming-platforms/

On July 12th 2018, the Jakarta Globe reported that terrorists could potentially use online gaming platforms such as World of Warcraft and Clash of Clans to communicate covertly with each other for the purpose of planning attacks. According to Indonesia's National Cyber and Encryption Agency (BSSN), there are signs suggesting that the terrorists were responsible for the

coordinated terrorist attacks which shook Paris on November 13, 2015 and could have used the PlayStation 4 console to communicate with each other ahead of the attacks.

Indeed, the Paris attacks continue to offer important lessons for security and intelligence agencies worldwide in the fight against smart terrorists. Besides the need to keep pace with improvised terror tactics, agencies should find a balance between countering threats and protecting the interests of ordinary people – online gamers in this case – who are the majority and use technology for innocuous and beneficial purposes.

The possible use of online gaming platforms as a digital tactic that enables criminals to assume anonymity and evade detection while planning unlawful activities is hardly a new idea. A Criminal Tradecraft Alert by the U.S Federal Bureau of Investigation (FBI) dated May 25, 2011 and titled "Bronx Bloods Members Communicating Through PlayStation Network (PSN)" stated that gang members in New York were able to circumvent house arrest and chat with each other by using the communication features in the PlayStation network.

PlayStation and Xbox consoles allow players to meet, chat and form virtual communities according to an article "How to join a game's online community" by softonic.com dated 17 July 2018. These communication features extend to online games such as Fortnite and Roblox which can be played on desktops and laptops, and are currently popular among youths. Players can also take their discussions further either by meeting on internet chat rooms and social media, or in person.

It would hence be conceivable for terrorists to take a leaf out of the criminals' digital playbook. In this regard, The Telegraph on December 9, 2013, reported that the Snowden leaks included documents revealing operations by the U.S National Security Agency (NSA) and U.K Government Communications Headquarters (GCHQ) to infiltrate online gaming platforms for the purposes of detecting criminal and terrorist communications and recruiting informants. Following the Paris attacks, Sony responded in an official statement that PlayStation 4 like "all modern connected devices" enables communication and hence "has the potential to be abused."

If it is true that the Paris attackers had used PlayStation to help plot their attacks, the success of the attacks further underscores three challenges that security and intelligence agencies will encounter in relying on online surveillance which has its limitations.

First, online gaming platforms – like any other digital technology such as social media and messaging apps – are part of the vast cyberspace which criminals and terrorists will constantly try to exploit to find new opportunities and avenues for concealment and subterfuge. Expectedly, security and intelligence agencies are beefing up their cyber capabilities to keep up with the evolving digital tactics of criminals and terrorists. However, these capabilities should not be unnecessarily invasive and there must be safeguards to ensure responsible and ethical usage.

Second, the use of digital avatars for fake identities as well as local languages and cultural lingo in the content of discussions could constrain the ability of intelligence efforts to detect and monitor suspicious activities and assess the reliability of informants. It will not be a straightforward process – even with the use of machine learning algorithms – to distinguish suspicious communications from other communications that are happening in online gaming communities that are populated largely by ordinary gamers. Hence, agencies should not be overly reliant on surveillance as a tool to counter threats especially when the results are not guaranteed.

Third, even if security and intelligence agencies have state-of-the-art technical capabilities, they will have to balance security priorities with issues of privacy that could limit their legal authority to conduct surveillance and transnational intelligence-sharing. A research paper, "Playing in the Dark: How Online Games Provide Shelter for Criminal Organisations in the Surveillance Age" by the Arizona Journal of International and Comparative Law, highlighted that privacy issues present a new battlefield in the relationship between law enforcement and individual privacy.

This battlefield has grown more arduous in the current climate as the Cambridge Analytica debacle has heightened the voices of free speech and privacy advocates – including technology companies – who clamor for the protection of consumers' personal data and the right to privacy. However, agencies should not dismiss these issues which are crucial to the well-being of people living in free and democratic societies.

Given these challenges, security and intelligence agencies will have to devise better approaches for Prevention which relates to intelligence-gathering to thwart attacks from

happening, and secondly enhance Response which relates to existing capabilities to protect people when attacks happen.

Prevention could be a two-fold approach. First, it will be strategically efficient for national-level agencies to leverage international law enforcement organizations such as INTERPOL and EUROPOL to partner with technological companies – game creators – to jointly examine the problem of criminals and terrorists misusing gaming platforms. Given the nature of the online gaming environment, these companies should be in a better position to develop fair and transparent user policies and tools that enable the monitoring of gamers' communications to foster a safer gaming environment by detecting and deterring unlawful activities. Such partnerships could also help to ameliorate the privacy and free speech issues stemming from surveillance and intelligence-sharing.

Second, national-level agencies can reach out to the local gaming communities – specifically the youth – during crime prevention and cyber wellness campaigns for the purpose of leveraging them as assets rather than viewing them only as a demographic group that is vulnerable to negative online influences. The youths' perspectives and familiarity with the online gaming environment could be useful in examining the problem and devising ways to detect and report suspicious communications, while protecting the consumer rights of online gamers.

Response would require the enhancement of first responders' capabilities, particularly private security officers, who would be at the scene of the incident – to detect possible threats and evacuate people – even before emergency response forces could arrive. The crucial role of private security officers was highlighted during the Paris attacks in two instances: officer Salim Toorabally stopped a suicide bomber from entering the national stadium during a football match, and officer Didi helped several concert-goers escape when gunmen stormed the Bataclan theatre.

In this respect, countries could take a leaf out of Singapore's book on transforming the private security industry by enhancing the professional skills of private security officers and facilitating the adoption of digital technology to support security operations in the face of a shrinking workforce and the heightened threat of terrorism. On July 18, 2018, Singapore launched the Security Industry Digital Plan (IDP) that aims to empower small and medium-sized private security companies with digital capabilities – such as surveillance robots and artificial intelligence for threat prediction – over the next decade.

These two counter-terrorism areas – prevention and response – are not sufficient on their own but could form a comprehensive strategy when developed in concert. This strategy is necessary to stay ahead of smart terrorists who exploit any form of digital technology to conceal their machinations, while concurrently protecting the interests of ordinary people such as online gamers.

As Russians hack the U.S. grid, a look at what's needed to protect it

By Manimaran Govindarasu and Adam Hahn

Source: http://www.homelandsecuritynewswire.com/dr20180808-as-russians-hack-the-u-s-grid-a-look-at-what-s-needed-to-protect-it

Aug 08 – The U.S. electricity grid is hard to defend because of its enormous size and heavy dependency on digital communication and computerized control software. The number of potential targets is growing as "internet of things" devices, such as smart meters, solar arrays and household batteries, connect to smart grid systems.

As researchers of grid security, we believe that current security standards mandated by federal regulations provide sufficient protection against observed threats. But recent incidents demonstrate the ongoing challenge of ensuring everyone follows the guidelines, which themselves must change over time to keep up with technological shifts.

The threat is real: In late 2015 and again in 2016, Russian hackers shut down parts of Ukraine's power grid. In March 2018, federal officials warned that Russians had penetrated the computers of multiple U.S. electric utilities and were able to gain access to critical control systems. Four months later, the *Wall Street Journal* reported that the hackers' access had included privileges that were sufficient to cause power outages.

Specific technical details have not yet been made public, so it's hard to know exactly what the hackers

did or gained access to. What has been revealed is that these breaches were accomplished with common hacking techniques, such as sending spearphishing emails to specific employees. Apparently, and reassuringly, the U.S. attacks didn't involve more advanced techniques seen in the Ukraine incidents, including custom-made software to target specific systems.

In addition, human errors will inevitably lead to mistakes that will weaken the security of some of the thousands of digital devices needed to protect the grid. And more sophisticated attackers may still find and exploit currently unknown vulnerabilities. Therefore, it's important for electric utilities, grid operators and vendors to remain vigilant and deploy multiple layers of defense.

Major players have some protections

There are two main aspects to grid architecture that need defending in different ways. The first element is the bulk power system, often referred to as the "transmission grid." It connects high-capacity power plants, transmission wires and substations that collectively generate and transport huge quantities of electricity over hundreds or thousands of miles. The rest of the grid is made up of smaller distribution grids – connected with the bulk power system – delivering electricity to homes and businesses around the country. The strongest standards for protection apply only to the bulk power system; though many distribution systems follow the same guidelines, they remain optional.

U.S. federal rules, as well as those set by the agency that governs the North American grid – which also includes large parts of Canada – require companies operating elements of the bulk power system to follow certain basic cybersecurity measures, including monitoring their networks to detect intrusions and mandating two-factor authentication for user logins.

Many large utilities do even more, assessing their risks in standardized ways and practicing responses to computer intrusions. These exercises often include hundreds of companies and organizations rehearsing how to collaborate to detect and confine attacks and restore service to customers.

Smaller companies are more vulnerable

Because transmission grid utilities should already have some protections against network intrusions, it is likely that the Russian hackers looked elsewhere, infiltrating smaller distribution utilities. If that's so, any potential power shutdown or other problems in those systems would be confined to smaller areas – like towns or cities. That, in turn, means fewer customers would be affected, with less work needed to get power back on.

But it highlights a worrying reality: Smaller and midsized companies that operate electricity distribution systems often have inadequate resources to invest in full cybersecurity protections. The more than 3,000 utilities in the U.S. have trouble finding sufficiently skilled workers who understand how the computerized and physical components of the grid work together and how to protect them.

In addition, utilities rely on complex supply chains to provide equipment, software, maintenance and other business functions. These external contractors and vendors may not implement protections as rigorous as the utilities. And their computer systems often have connections to the utilities' networks, which may be considered trusted and safe, rather than potential avenues of attack.

Stepping up defenses

Fixing all these potential problems is complex. First, all utility companies – even the smallest – should adopt basic security protections like those required of large utilities. Some states are moving to require this of the power companies serving their residents, but many aren't yet. Further, we recommend all companies that are part of the grid participate in coordinated grid exercises to improve cybersecurity preparedness and share best practices.

In addition, all utility companies need to take steps to ensure the hardware and software they use are from trustworthy sources and have not been tampered with or modified to allow unauthorized users in.

It won't be enough to protect against today's threats. Adversaries are likely to employ increasingly sophisticated techniques that exploit both computer and human vulnerabilities. Companies need to ensure they engage in what might be called sustainable cybersecurity – ongoing processes that let systems and staff adapt over time, to stay ahead of the threats.

Researchers have an important role too, exploring ways that emerging technologies like cloud

computing, blockchain and big-data analytics could help reduce risks without introducing any additional weaknesses. Further, researchers should identify more advanced ways to secure the grid, and reduce these systems' complexity, which would limit both current risks and future unknowns.

Manimaran Govindarasu *is Professor of Electrical and Computer Engineering, Iowa State University.*
Adam Hahn *is Assistant Professor of Electrical Engineering and Computer Science, Washington State University.*

Smart city systems are riddled with critical security vulnerabilities

Source: https://www.zdnet.com/article/smart-cities-are-riddled-with-critical-security-vulnerabilities/

Aug 09 – IBM has discovered 17 zero-day vulnerabilities in smart city systems which could debilitate core services.

At the Black Hat conference in Las Vegas on Monday, the cybersecurity firm's X-Force Red team of penetration testers and hackers demonstrated how old-school threats are placing the cities of the future at risk in the present day.

Smart city technology spending is predicted to hit $80 billion this year and become as high as $135 billion by 2021. Water and filtration systems, smart lighting, traffic controllers, utilities, and more all become intertwined in smart cities, which aim to make urban living more energy efficient, eco-friendly, and manageable.

However, connecting all of these critical elements can have devastating effects should something go wrong -- such as a successful cyberattack.

We've already seen the damage which can be caused when threat actors target core country systems, such as in the case of Ukraine's power grid, and unless security is considered every step of the way, every future city will be placed at similar levels of risk.

Together with researchers from Threatcare, IBM X-Force Red discovered that smart city systems developed by Libelium, Echelon and Battelle were vulnerable to attack.

Libelium is a wireless sensor network hardware manufacturer, while Echelon specializes in industrial IoT, and non-profit Battelle develops and commercializes related technologies.

According to IBM X-Force Red researcher Daniel Crowley, out of the 17 previously-unknown vulnerabilities discovered in systems used in four smart cities, eight are deemed critical in severity.

Unfortunately, many of the bugs were due to poor, lax security practices -- such as the use of default passwords, authentication bypass, and SQL injections.

In total, the researchers uncovered four instances of critical pre-authentication shell injection flaws in Libelium's wireless sensor network, Meshlium.

In addition, Echelon's i.LON 100/i.LON SmartServer and i.LON 600 SmartServers, which are used for energy conservation, contained two critical authentication flaws, unencrypted communications issues, default credentials were in use, and plaintext passwords were uncovered.

When it comes to Battelle, the non-profit's V2I (Vehicle-to-Infrastructure) Hub, version 2.5.1, was also found wanting when it comes to adequate security.

The worst vulnerability discovered was a hard-coded administrator account, followed by permitted access to sensitive functionality without authentication, default API keys and authentication bypass, SQL injection security flaws and reflected XSS issues.

After rounding up the bugs which were immediately apparent in the various smart city systems, the team found that dozens -- and in some cases, hundreds -- of the vendor devices were left exposed to remote access online.

"Once we located an exposed device, using some standard Internet searches we were able to determine, in some instances, who purchased the devices and, most importantly, what they're using the devices for," the researchers added.

The findings were disclosed to Libelium, Echelon, and Battelle. IBM says all three were "responsive" and security patches have been issued to resolve the vulnerabilities.

Update 16.06 BST: A Libelium spokesperson told ZDNet:
"Several weeks ago Libelium was informed by IBM about some web vulnerabilities which had been found in the Meshlium Manager System. As Libelium considers security as a fundamental and essential core element for all its development projects new actions were taken immediately.
Responding to Libelium's commitment to the security of IoT devices, the company took action instantaneously and all vulnerabilities detected were automatically amended with a new software version released on August 1st which is ready to be downloaded from the Manager System.
Libelium truly appreciates IBM work in the detection as well as their responsible communication about this discovery."

11-year old took 10 minutes to hack a replica of Florida's election reporting website

Source: http://www.homelandsecuritynewswire.com/dr20180815-11year-old-took-10-minutes-to-hack-a-replica-of-floridas-election-reporting-website

Aug 15 – The world's largest hacking convention took place in Las Vegas over the weekend, and an 11-year-old was able to hack into a replica of Florida's election reporting website in less than 10 minutes and change votes.
PBS:

> The boy, who was identified by DEFCON officials as Emmett Brewer, accessed a replica of the Florida secretary of state's website. He was one of about 50 children between the ages of 8 and 16 who were taking part in the so-called "**DEFCON Voting Machine Hacking Village**," a portion of which allowed kids the chance to manipulate party names, candidate names and vote count totals.
> Nico Sell, the co-founder of the non-profit r00tz Asylum, which teaches children how to become

> hackers and helped organize the event, said an 11-year-old girl also managed to make changes to the same Florida replica website in about 15 minutes, tripling the number of votes found there.
> Sell said more than 30 children hacked a variety of other similar state replica websites in under a half hour.
> "These are very accurate replicas of all of the sites," Sell told the PBS NewsHour on Sunday. "These things should not be easy enough for an 8-year-old kid to hack within 30 minutes, it's negligent for us as a society."

CNN:

> "Unfortunately, it's so easy to hack the websites that report election results that we couldn't do it in this room because [adult hackers] would find it boring," said Jake Braun, one of the event's organizers.
>
> So on Friday, almost 40 child hackers between the ages of 6 and 17 were let loose on the mock sites, and most of them were able to tamper with vote tallies, some even changing candidates names to things like "Bob Da Builder" and "Richard Nixon's Head."

National Association of Secretaries of State (NASS) issued a statement in response, welcoming help from DEFCON participants in securing elections but also claiming their actual sites are not as vulnerable as the replicas.

> "While it is undeniable websites are vulnerable to hackers, election night reporting websites are only used to publish preliminary, unofficial results for the public and the media. The sites are not connected to vote counting equipment and could never change actual election results.'"
>
> (…)
>
> "To me that statement says that the secretaries of states are not taking this seriously. Although it's not the real voting results it's the results that get released to the public. And that could cause complete chaos," [Sell] said. "The site may be a replica but the vulnerabilities that these kids were exploiting were not replicas, they're the real thing."
>
> "I think the general public does not understand how large a threat this is, and how serious a situation that we're in right now with our democracy," she said.

Adults who participated in the second annual "voting village" at DEFCON took at crack at hacking voting machines.

CNN:

> After a few hours on Friday, one hacker was essentially able to turn a voting machine into a jukebox, making it play music and display animations. While such hacks are a cause of concern for election officials, they are increasingly looking beyond the threats against traditional election infrastructure like voting machines and voting databases and more to the threat of disinformation.
>
> (…)
>
> If state election boards were to be targeted in this way, where voter information or voting systems were hacked, and then a coordinated campaign to disseminate or weaponize that information were to follow on social media, it could lead to widespread confusion that could undermine the integrity of an election could ensue, some officials fear.

The Role Al Qaeda Plays in Cyberterrorism

Source: http://smallwarsjournal.com/jrnl/art/role-al-qaeda-plays-cyberterrorism

Aug 22 – One specific example of how Al Qaeda uses the internet to further their agenda is through an English-written online magazine called *Inspire*—which is run by Al Qaeda in the Arabian Peninsula (AQAP); the online magazine is decently folowed, provides information on Al Qaeda's viewpoints as well as the jihadist movement, and commentates on the group's kill list (Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K.C., 2015). Because Al Qaeda's *Inspire* does a great job at publishing content that resonates with likeminded individuals, they are victorious in "spreading the call for jihad" online (Rudner, 2017).

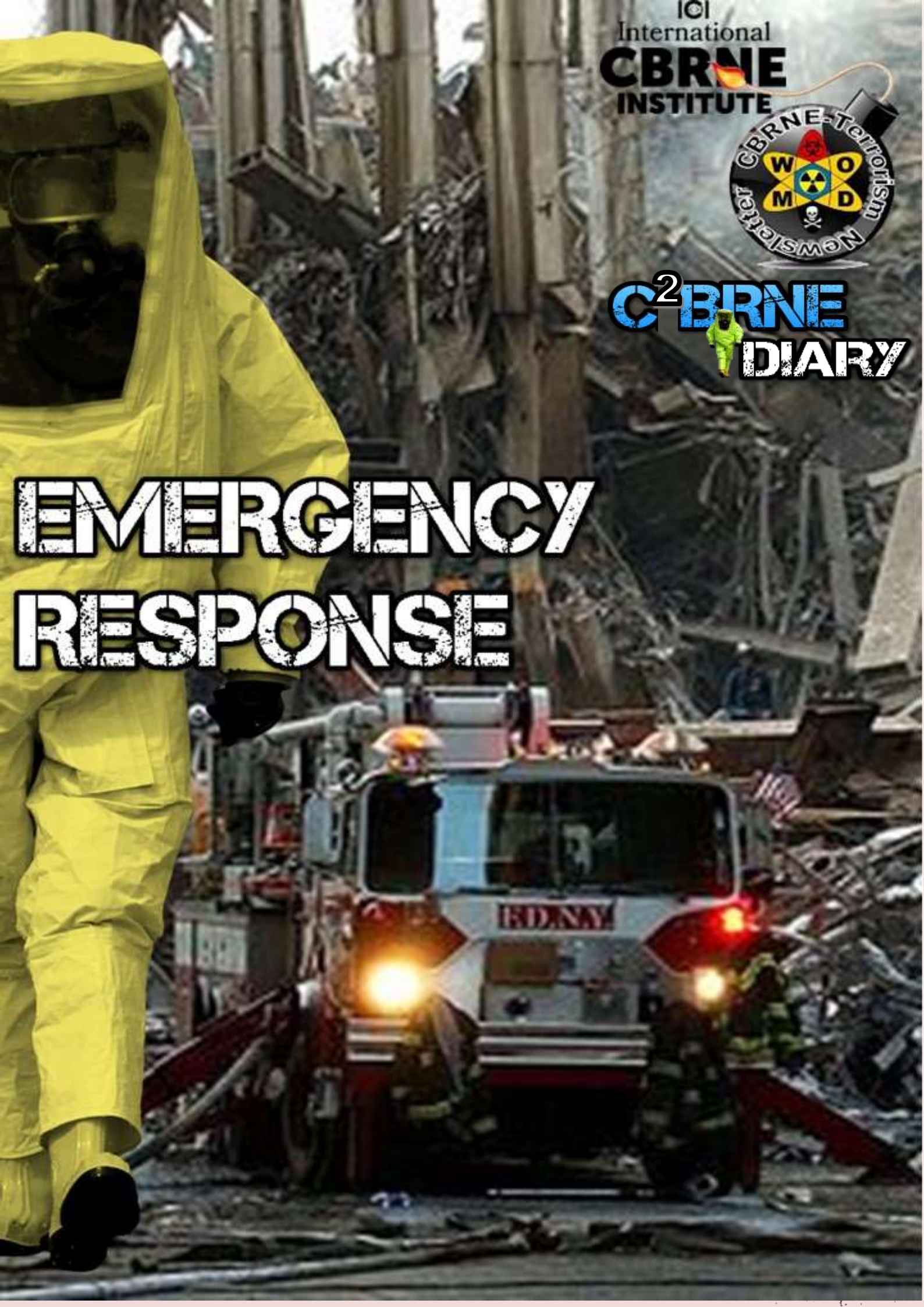
Another example of Al Qaeda's success in the cyber realm is how effectively the terrorist organization reaches its target audience through film and on-the-ground reporting (Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K.C., 2015). By recording their experiences at Arab Spring protests, videoing beheading executions (such as Jewish journalist Daniel Pearl's death), and releasing several video games (targeted to the youths) that place the player in the role of a jihadist fighting against Jews, Westerners, and the U.S. military, Al Qaeda makes themselves more relatable, gives themselves some relevance, shows people that they are a force to be reckoned with, and attempts to normalize or justify their behavior—which is beneficial to the terrorist group's survival (Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K.C., 2015).

With their success at luring people online (especially the "homegrown" terrorists in Western societies) to accept as well as follow their radical jihadist views, Al Qaeda has become one

of the poster children for not using the internet as simply an attack vehicle to fulfill their agendas (Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K.C., 2015 and Rudner, 2017). In fact, Al Qaeda does not necessarily need to be the best at cyberattacks when their unregulated presence on the internet alone plays such a significant role in fostering violent Islamic extremism—more so than prisons, universities, and places of worship (Rudner, 2017).

Instead of primarily using the internet to implement cyberterrorist attacks, this terrorist group tends to use cyberspace more for communicating/spreading their jihadist agenda globally, cultivating support for their initiatives through social media or web forums, offering theological justification for actions of terror on online platforms, providing technical instructions and operational guidelines on the internet for their terrorist attacks, inciting violence through their media forums, engaging in online fundraising activities to support their cause, and web defacing their so-called enemies' websites (Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K.C., 2015 and Rudner, 2017).

Because of the terrorist organization's limited cyber capabilities and the many ways Al Qaeda uses the cyber realm to further their ideology, criminologists such as Marjie Britz have had to create a more expansive definition for cyberterror to encompass the many ways organizations like Al Qaeda utilize technology to further their missions (Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K.C., 2015). According to her, cyberterror is "the premeditated, methodological, ideologically motivated dissemination of information, facilitation of communication, or attack against physical targets, digital information, computer systems, and/or computer programs which is intended to cause social, financial, physical, or psychological harm to noncombatant targets and audiences for the purpose of affecting ideological, political, or social change; or any utilization of digital communication or information which facilitates such actions directly or indirectly" (Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K.C., 2015). With this definition, scrappy cyberattacks and social media incitements can still be acts of cyberterror, which makes Al Qaeda fall under not only the terrorist organization category, but also the cyberterrorist category.


ICI
International
CBRNE
INSTITUTE
CBRNE-Terrorism Newsletter
W
O
M
D
C2BRNE
DIARY
EMERGENCY
RESPONSE

Fighting fire with fire: How controlled blazes are used to avert a greater catastrophe

As wildfires wreak havoc in California and leave 90 dead in Greece, Robert Matthews looks at why 'putting out the fire with gasoline' is often the only option

Source: https://www.thenational.ae/uae/science/fighting-fire-with-fire-how-controlled-blazes-are-used-to-avert-a-greater-catastrophe-1.758853

Firefighters battle the Ferguson Fire, the largest fire in the Sierra National Forest's history, in California on August 8. Courtesy US Forest Service

Aug 11 – Searing heat, high winds, years of drought - the driving forces of the biggest wildfire ever to strike California seem obvious. But it's equally clear that the standard ways of dealing with it are barely able to cope.

Around 14,000 fire-fighters have spent a fortnight battling fires that are expected to burn for the rest of the month.

Worse, there's a growing belief that such fires will become – as one hard-pressed fire-fighter put it last week – "the new norm".

But that, in turn, is sparking renewed interest in a radical approach to dealing with the threat.

And it involves literally fighting fire with fire.

For years, the key idea behind preventing conflagrations has been one of zero tolerance through measures like banning camping and setting up networks of lookout-towers that could stop small fires getting traction.

When the majority of fires had natural causes like lightning, this worked. But with increasing urbanisation it's doomed to failure.

Since the early 2000s, California has tried to deal with the increasing threat through laws requiring homeowners to strip the land around their homes of vegetation that could turn into kindling.

But around the same time, researchers began taking an interest in a more radical approach, and switching from fire prevention to fire management.

Studies revealed that the zero-tolerance approach had an unintended consequence: a build-up of colossal amounts of dead wood in forests which themselves were becoming ever denser.

As a result, if a fire did break out there was a much higher risk of it turning into a conflagration.

In 2006, a four-year international research programme was set up by the European Union to investigate an idea already being used in parts of the US.

At its heart is the so-called fire triangle, which describes the three key requirements for a blaze: heat, oxygen and fuel. Remove any one, and fire becomes impossible.

And one of the best ways of removing fuel is to burn it – in a fire.

A plane dumps fire retardant over a fire as it spreads in Lake Elsinore, California on Wednesday, August 8. Reuters

During the four years, the aptly-named Fire Paradox project showed that small, controlled fires set during the winter months consumed fuel that could otherwise feed a far bigger event.
The project also backed a strategy used by some fire-fighters in the US and Australia for dealing with major fires once they've begun.

A wildfire burns in the Cleveland National Forest in Lake Elsinore on Wednesday, August 8. Jae Hong / AP Photo

This involves setting a controlled blaze ahead of the main one, and using it to clear vegetation that would otherwise feed the bigger fire. It's a method now being used to contain some parts of California's blaze.
But the project also uncovered the most paradoxical approach of all. This involves setting up a second line of fire close to the main blaze. The resulting inrush of air then drives the two fronts together so violently they put each other out.
While crazy-sounding, demonstrations of such "fire-fights" in Argentina showed they can work.

The sheer size of the California blaze means there's no hope of surrounding it and attempting anything like this.

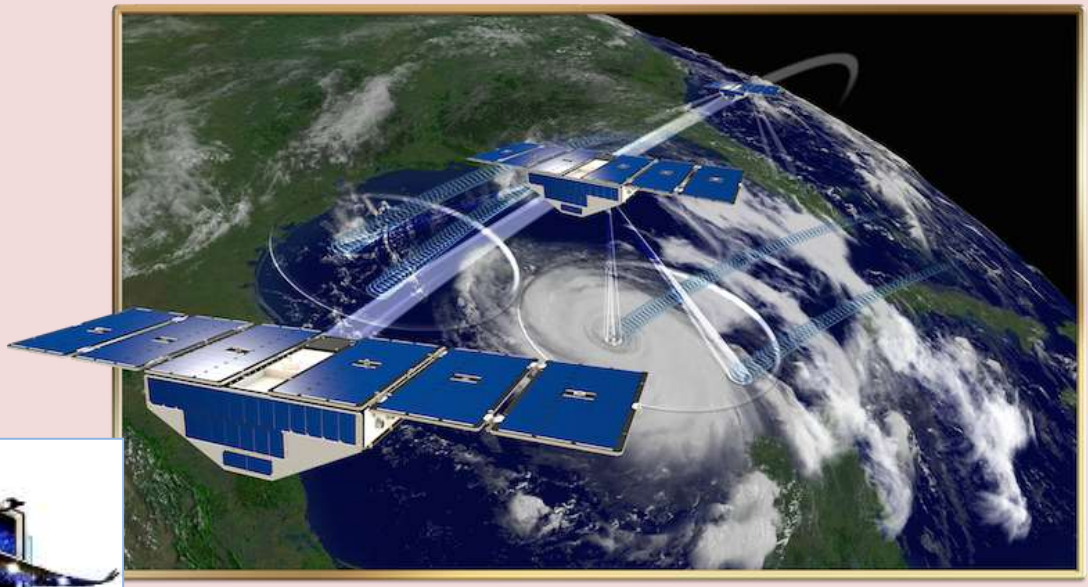
Even so, the lesson is clear: the solution to some natural disasters lies in thinking well outside the box.

It's an approach that's now being used to deal with that other existential threat to Californian life: earthquakes.
For decades, scientists looked for ways of predicting when the state's notorious San Andreas fault would next give way, triggering a devastating earthquake.
Yet despite spending billions of dollars, they found no tell-tale signs they could rely on.
But now the US West Coast is going to benefit from a neat bit of lateral thinking. It exploits the fact that the most reliable indicator of any earthquake is the quake itself.
While no-one knows for certain when the San Andreas fault will next wreak destruction, one thing is for sure: it will release waves of seismic energy through the ground.
Some of these waves are relatively harmless, while others cause the deadly up-and-down motion that wreaks most of the damage.

Microsatellites help in flood detection

Source: http://www.homelandsecuritynewswire.com/dr20180727-microsatellites-help-in-flood-detection

July 27 – Hurricanes bring heavy rainfall and strong winds to coastal communities, a potent combination that can lead to devastating damage. In 2016 NASA launched a set of eight satellites called the Cyclone Global Navigation Satellite System, or CYGNSS, mission to gather more data on the winds in these tropical cyclones as part of an effort to increase data coverage of hurricanes and aid forecasts. As the first year of data is being evaluated, a new and unexpected capability has emerged: the ability to see through clouds and rain to flooded landscapes.



NASA says that the flood maps are possible thanks to one of the innovations of the CYGNSS constellation. The microwave signal the CYGNSS satellites use to detect wind speed based on the choppiness of the ocean is actually not generated by the satellites at all. Instead the satellites use the constant and ubiquitous signals from the Global Positioning Satellite (GPS) system, which is also responsive to reflections from standing water and the amount of moisture in the soil.
"Before about 2015, people had inklings that you could use GPS reflection data over land to look at

various things, but there hadn't been many observations to prove it," said Clara Chew, a researcher at the University Corporation for Atmospheric Research in Boulder, Colorado. "With the launch of CYGNSS we've finally been able to really prove that yes, these signals are very sensitive to the amount of water either in the soil or on the surface."

Chew developed flood inundation maps of the Texas coastline after Hurricane Harvey and of Cuba after Hurricane Irma, as well as flood maps of the Amazon River in Brazil, which overflows its banks seasonally.

"When we made our first complete map of the Amazon, everyone was really shocked because you can see a lot of the tiniest, tiniest rivers throughout the basin, and nobody knew that we were going to see rivers a hundred meters wide or so in the data," Chew said, noting that the native resolution of data over the ocean varies between 10 and 15 km and it is averaged to a consistent 25 kilometers.

"When I saw the first land images of inland water bodies, I was amazed at their quality," said Chris Ruf,

CYGNSS's principal investigator at the University of Michigan in Ann Arbor. "We had known beforehand that there would be some instances of coherent scattering possible. That's the phenomenon that creates such high-resolution images. It rarely happens over the ocean and we hadn't really considered how often it might happen over land. It turns out that it happens quite frequently, and almost always when observing small inland water bodies. This promises to open up entirely new areas of scientific investigation."

CYGNSS's advantage over other space-based sensors for flood detection is its ability to see through clouds, rain and vegetation that may otherwise obscure floodwaters. Currently, flood detection is generally done by optical sensors on the U.S. Geological Survey-NASA Landsat satellites, which can't see through clouds, and the microwave sensors on the European Space Agency's Sentinel 1 and 2, which can't see through vegetation. Capturing data from eight satellites instead of one is another advantage because it decreases the time between observations for locations, meaning more coverage, more rapidly, of flooding in the tropics. Together this means CYGNSS could bridge gaps in current coverage.

"Flooding from hurricanes can happen really quickly," Chew said. "You can go from dry to a complete flood within a matter of hours. So even with satellites that observe Earth every two to three days you can miss a lot of information such as how quickly an area flooded and the maximum extent of flooding. But if you have more samples, like what CYGNSS gives you, then you can start to really pinpoint these types of things."

However, this type of detection is still in its early days of development, and Chew and others are exploring how to infer the amount of water present and other parameters to complement soil moisture and flood data from other satellites. In addition, CYGNSS data currently takes two days to go from observation to data users.

"It's very fitting that one of the new things that CYGNSS is unexpectedly good at determining, the extent of flood inundation, is very often a direct consequence of the thing it was designed to measure, namely hurricanes," Ruf said. "So now, not only will we be able to observe the hurricanes while they are over the ocean, we will now also be able to map much of the damage they cause from flooding after landfall."

Take part in a training exercise that covers the whole world and all disciplines

Source: https://www.crisis-response.com/comment/blogpost.php?post=394

July 24 – Long-term power outages are their own serious emergencies with catastrophic secondary and tertiary orders of effects. One key method of preparing and thinking about this can be done through the Electric Infrastructure Security Council (EIS) Council, which hosts national and international collaboration on resilience and whole community restoration and response planning, addressing severe, national and global scale hazards to lifeline infrastructures.

I highly recommend clicking on the 'Library' tab at the top as your first order of business. You'll be able to see its industry standard conference notes from previous collaboration efforts, along with manuals prepared for various types of events that could be used at the local, state, and national government levels for planning purposes.

However, I believe the real gem of working with EIS is coming up in the form of its annual exercise called Earth/Ex 18 on August 22, 2018.

This event is billed as an: "Interactive all-sector whole-of-world" exercise. The venue is 'Earth' and invitees include: "All of humankind, all organisations from all nations." So, please consider this your invitation to play!

One may choose to participate in any number of languages, including English, Spanish, French, German and Hebrew. No preparation or special industry expertise is required for the exercise. It's a locally facilitated, come as you are experience.

The facet of this particular exercise that I like in particular is that one may choose to register and participate as an organisation or as an individual. As an out-of-the-box senior level exercise, it provides an opportunity to examine and rehearse critical executive and operational decisions required before a full operational exercise. As an individual (or family or community group), the exercise will help with basic preparations and with planning that can help secure and sustain participants during an extreme disaster. Some of the scenarios may include, but not be limited to, cyberattacks, extreme weather, electromagnetic pulses (EMP), earthquakes, extreme terrestrial weather, and kinetic attacks on key infrastructure.

All of them will be great learning opportunities.

Train today, live tomorrow. Good luck!

FIREMAN BOOT GTX

Source: https://alfaoutdoor.com/shop/pro/safety-high/stovel-brann-gtx

Norway's bestselling fire boot has been redesigned. This leather boot that was developed in collaboration with firefighters and the HMS Straum Safety Center has received a GORE-TEX® membrane and become waterproof. The model has a heat and puncture resistant sole, chainsaw protection and seams with Nomex thread. It also features no laces or zippers that could get caught – everything is made for optimal safety. It fits very well on the foot and a sturdy shank ensures that it does not chafe. The durable straps make it easy to get on, and a well-padded top edge with nappa leather keeps it comfortable on the shin. The boot has a contemporary design with reflectors on the front, rear shaft and sides.

Weigth: 1415 g pr shoe/boot (EU 42)

International Journal of Disaster Risk Reduction 31 (2018) 750–757

Contents lists available at ScienceDirect

International Journal of Disaster Risk Reduction

journal homepage: www.elsevier.com/locate/ijdrr

Wisdom of (using) the crowds: Enhancing disasters preparedness through public training in Light Search and Rescue

Kobi Peleg[a,b,*], Moran Bodas[a], Gilead Shenhar[a], Bruria Adini[a]

[a] The Department of Disaster Management & Injury Prevention, School of Public Health, Sackler Faculty of Medicine, Tel-Aviv University, Israel
[b] Israel National Center for Trauma & Emergency Medicine Research, The Gertner Institute for Epidemiology and Health Policy Research, Sheba Medical Center, Tel Hashomer, Ramat-Gan, Israel

Source: https://www.sciencedirect.com/science/article/pii/S2212420918303005

Highlights

- Light Search and Rescue training for Israeli high-school students were performed.
- The trainings were found to be beneficial in improving resilience, self-efficacy and knowledge.
- The effect of the training on these measurements ranges from medium to high.
- Participants finish the trainings with equally high levels of performance.

Abstract

Following major earthquakes, the vast majority of trapped survivors are rescued by layperson with the first 24–48 h. Most trapped individuals require only Light Search and Rescue (LSR). Therefore, there is sense in training members of the public in LSR competencies to upsurge survivability rates. Since the beginning of the school year 2017–8, all Israeli 10th graders have been undergoing such training. The purpose of this study was to evaluate the efficacy of these training in terms of resilience, self-efficacy and knowledge. A cluster randomized study involving 19 clusters comprising of 35 schools was performed during the first semester of the school year. Students were asked to complete a self-reporting questionnaire before and after the LSR training. In total, 1758 questionnaires were collected, of which 1279 (~ 73%) were paired with both pre and post data. A significant increase was found in all indices. Resilience score increased from a mean of 2.85 (± 0.70 SD) pre-training to 3.95 (± 0.63 SD) following it ($W = 29.451$, $p < .001$). This difference constitutes a very large effect size of $d = 1.652$ (95%CI: 1.525, 1.779). Significant increases were observed also for self-efficacy and knowledge. Differences across demographic variables were observes, e.g. between the genders, with boys reporting greater levels of resilience than girls. This study demonstrates that SLR trainings for high school students are capable of benefiting students' perception of resilience, self-efficacy and knowledge to perform during crisis. Moreover, the trainings have an equalizing effect on participants resulting in equally high levels of performance following training, despite pre-training differences.

Durable Medical Equipment in Disasters

August 06, 2018

This fact sheet provides information on general durable medical equipment (DME) categories and focuses on electricity-dependent DME that may be affected by disasters and emergencies, including power failures. It also includes information to assist healthcare system preparedness stakeholders plan for medically vulnerable populations who rely on DME.

View Full Report

New laser solution could slow spread of forest fires

By Abigail Klein Leichman

Source: http://www.homelandsecuritynewswire.com/dr20180808-new-laser-solution-could-slow-spread-of-forest-fires

Aug 08 – Aggressive wildfires are rampaging through many countries this summer, bringing death and destruction in their wake. In California alone, firefighters are scrambling to control 18 separate blazes. Texas, Oregon, Florida, New Jersey, as well as Canada, Greece, India, Mexico, Portugal, Spain, Sweden and the UK are among other areas battling massive forest fires, a phenomenon experts expect will only increase due to climate change.

It was the massive forest fires in Israel over the past several years that gave electro-optics physicist Daniel Leigh the idea of using algorithm-controlled laser beams from helicopters or trucks to zap leaves, thin branches and pine needles off treetops in the path of fire. The flames are forced downward, where they can be more easily controlled by conventional methods.

Greece 2018

Leigh explains that leafy treetops provide a highly combustible smorgasbord for hungry forest fires. Fanned by extreme wind and weather conditions, a forest fire that rises to the treetops spreads out of control in the blink of an eye.

When Leigh shared his idea with ecologist Zvika Avni, former chief of the Keren Kayemeth LeIsrael-Jewish National Fund (KKL-JNF) Forestry Department, Avni agreed to be the ecology and the wildfire fighting specialist for Leigh's startup, Fighting Treetop Fire (FTF).

California 2018

Founded in 2012 and bootstrapped by Leigh, FTF developed its laser technology in consultation with Hebrew University academics and with professionals. Several years later, management consultant Noach Cholev joined as a cofounder.

The company of four is now in the engineering, modeling and testing phase. It's not yet clear when the technology will reach the market. This depends on finding a strategic partner.
Laser (which stands for "light amplification by stimulated emission of radiation") uses concentrated light to cut or perforate anything from metal to human tissue.
One might think this heat would just make a fire worse, but Leigh explains that the laser works lightning fast and then switches off. The moisture remaining in the foliage immediately extinguishes the combustion. In preliminary lab experiments, FTF's laser technology sheared off targeted pine needles without igniting them or the remaining pine needles.
Moreover, the fallen foliage – while still flammable — forms a compact high-moisture bed with restricted airflow. With less oxygen and densely packed fuel, the ground fire loses intensity and speed, and is easier to extinguish.
"We now aim at large-scale experiments and later on prototype development so that we can do outdoor real-life proof of concept testing," Leigh says. "We are now seeking partnerships, licensing agreements and/or investments. The firefighting community is all excited to try it out but they need a demo tool to work with."
The technology at the heart of FTF is patented in Israel, Australia and Europe; a US patent is pending. There is already interest in the technology from Australia, which suffers devastating wildfires every summer.

Safe zone

Leigh isn't a firefighter, but he couldn't bear to sit back and watch forest fires wreak destruction.
"My background in electro-optics brought me to ask what I could do," says Leigh. Learning that canopy leaves are igniters and can regrow after being cut, he immediately thought of laser.
"While it's not possible to cut down whole trees with a laser, I analyzed the process and realized I could use laser beams, sent from a safe distance, like a knife to cut off leaves remotely," Leigh says.
He envisions FTF as a unique rescue tool to create a safe zone or an escape route for trapped firefighters or residents.
The same algorithm-controlled laser technology – which can work continuously in all weather conditions with no need to refill anything — theoretically could be used for cutting back lower-to-the-ground foliage in the path of fire, and could prove a valuable firefighting tool for sensitive worksites such as power companies and utilities.

Triangle of fire

Rami Zaretski, head of KKL-JNF Forest Fire Department, confirms that treetops' combustible materials and halo of oxygen feed forest fires, often causing firestorms whipped by air currents created by the high-energy blaze itself, as well as firebrands — sources of heat that can create spot fires.
"This is the basic triangle of fire: heat, oxygen and combustion material," Zaretski tells ISRAEL21c. "When we remove one of the components from this equation, or change the ratio, the burning will stop."
He therefore likes the FTF concept but raised some questions about the approach on a practical level. For example, can it work fast and efficiently enough to prevent firebrands?
Leigh and Avni believe it will, thanks to the algorithmic control process. And the technology can enhance the capability of existing methods to isolate and control spot fires, they add.
How would the proposed process affect wildlife?
"Treetop fires are extremely hot and therefore kill all the animals in their vicinity," Avni says. "The FTF tool will affect or injure some animals in the process. However, this will amount to a small fraction of the number of animals killed not using the FTF tools."
In answer to Zaretski's concern about the helicopter delivery method's ability to function in high-smoke conditions and extreme wind, Leigh explains that measures would be taken to protect the engine from smoke, and the aircraft would maintain a safe distance from the fire front. The laser beams would be guided through the smoke by special imaging systems.
"FTF's new 'out of the box' method and tool is designed exactly for such extreme weather conditions that lead to fires uncontrollable with today's wildfire fighting tools using chemicals and water for fire suppression," says Leigh.

Abigail Klein Leichman *is a writer and associate editor at ISRAEL21c.*

Disaster planning saves lives

Source: http://www.homelandsecuritynewswire.com/dr20180810-disaster-planning-saves-lives

Aug 10 – There are a lot of scary threats in the world—extreme weather, terrorist attacks, deadly infectious diseases, mass shootings—but if health care organizations plan ahead for such disasters, lives can be saved.

That was the key message from emergency preparedness expert Paul Biddinger, who spoke to a Harvard T.H. Chan School of Public Health audience in Kresge G-2 on 31 July 2018 as part of the Hot Topics summer lecture series. Biddinger is director of the Center for Disaster Medicine and Vice Chairman for Emergency Preparedness in the Department of Emergency Medicine at Massachusetts General Hospital (MGH); Medical Director for Emergency Preparedness at MGH and Partners Healthcare; and director of Harvard Chan School's Emergency Preparedness Research, Evaluation & Practice (EPREP) Program.

The first step for health care organizations preparing for emergencies is to accurately assess the kinds of hazards they may face, such as flooding, power outages, or violence, Biddinger said. They have to develop a plan that takes those hazards into account. They need to train staff about the plan and hold exercises that simulate disasters. **"No plan ever looks in practice the way it looks on paper,"** said Biddinger. "You have to train and exercise constantly—and everybody has to know what the plan looks like."

Harvard notes that in 2005, Biddinger and colleagues learned from consultants from **Israel**—who'd dealt with bombings that resulted in mass casualties—that the average **time from when a bomb goes off until the first person reaches the closest emergency department is four minutes**. Experts from other places that had dealt with bombings, including London, Madrid, and Mumbai, confirmed that events unfold incredibly quickly during a disaster. Realizing that once a disaster struck there wouldn't be time to do much of anything—such as clear space in emergency departments for incoming wounded, or call doctors and nurses in to help—Biddinger and his colleagues developed a plan so that hospital staff would know what to do during a disaster without having to be told. "It becomes muscle memory," Biddinger said.

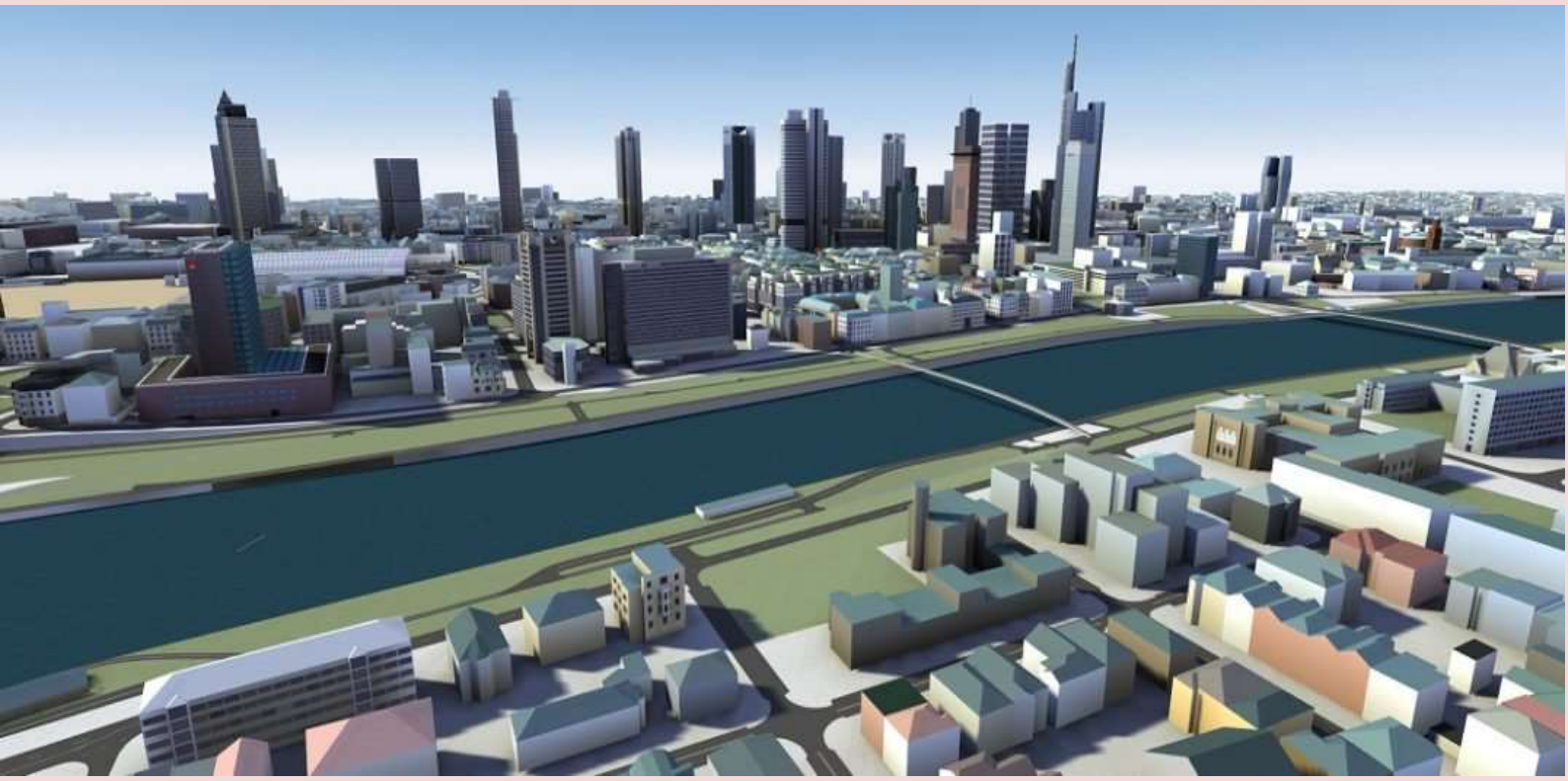
In 2013, the Boston Marathon was bombed, injuring 275 and killing three. "None of us ever thought someone would bomb the Boston Marathon," said Biddinger. "Why would you bomb a road race?" But Boston-area emergency responders' planning and preparation helped—not a single person who wasn't killed at the scene died later at a hospital, Biddinger said.

Fostering coordination among health care organizations that normally operate independently of each other is an important factor in good emergency preparedness, Biddinger said. **It's also important during a disaster for hospitals and health care centers to maintain primary care services such as dialysis or cancer treatments.**

When Biddinger meets people at cocktail parties and they realize he works in emergency preparedness, they invariably ask: "Well, are we prepared?" He said there's no "yes or no" answer to the question. "We will never have enough money, enough time, enough resources, to be fully prepared for everything," he said. **"Therefore, we have to do the best we can with what we have…..** We try to identify our greatest threats, identify our greatest vulnerabilities, improve our plans, test our plans, learn lessons—and do it all over again." Ideally, he added, the plans are guided by the best available science, "so that hopefully we get better and better and better."

Mapping to Revolutionize Emergency Response

Source: https://i-hls.com/archives/84748



Aug 10 – Emergency responders rely on real-time and accurate information for enhanced situational awareness and safety. Now they will be able to have better information about the places they are dispatched to. HERE Technologies, a global leader in mapping and location platform services, has joined together with Motorola Solutions to equip public safety responders with detailed venue maps for enhanced situational awareness.

The comprehensive digital map coverage goes beyond the road network. It includes the "spaces between the roads and streets" – shopping malls, corporate campuses, hospitals, universities, stadiums, manufacturing facilities, museums, apartments, airports, train stations, and more.

Motorola Solutions' CommandCentral Aware software, used by public safety command centers, integrates HERE Technologies' venue maps to guide first responders to the right locations, while adapting to dynamic events in real-time. Adding building mapping intelligence will equip command centers with better information so that they can coordinate faster, and provide more accurate responses when seconds matter.

Before entering a building, police, fire and EMS personnel can automatically access the latest authorized venue map of the building to know the best entrance and fastest route to someone in need. Venue maps also include the locations of fire extinguishers, defibrillators, and medical kits on-premise for quick access.

Motorola Solutions CommandCentral Aware aggregates and integrates streaming video, geospatial data, real-time alerts, resource tracking, analytics, voice, computer-aided dispatch and records information so public safety command center staff can communicate actionable intelligence to field responders, according to automotiveworld.com.
The system will provide the public safety community with a layer of real-time information that will aid in the speed and safety of first responders.

Drop Kits Supply Communication in Emergency

Source: https://i-hls.com/archives/84884

Aug 16 – Due to communications challenges during the response to the 9/11 terrorist attacks in the US, the 9/11 commission recommended the establishment of a single, interoperable network for public safety. For this purpose, FirstNet was founded; a nationwide public safety communications platform dedicated to America's first responders.
In an emergency, communication is critical to response efforts. That's why former public safety officials and first responders at FirstNet, in collaboration with Sonim, are creating Emergency Drop Kits According to prnewswire.com, these portable kits will envelop first responders in a 90 meter "connected bubble," letting them maintain constant communication to better coordinate their response. The Emergency Drop Kits are being designed for use during emergencies in rural and remote areas, as well as areas where communications may be temporarily unavailable like wildfires or hurricanes.
Incident commanders will be able to drop in the kits for rapid connectivity to FirstNet. First responders will also be able to take the kits with them in the field. Ideal for short-term situations or as an interim solution until a FirstNet dedicated deployable arrives.
"This is a great example of how FirstNet is driving focused innovation for first responders," said Chris Sambar, senior vice president, AT&T-FirstNet. "To create the Emergency Drop Kits, we're pulling in expertise from public safety and across the industry. The kits will make it even easier for first responders to stay connected to the full capabilities of their network – no
matter where their mission takes them." The kits are currently moving from a proof of concept to a reality for future availability to purchase.
The AT&T FirstNet team is currently working to meet with every state in the US to properly tailor the program to their distinct needs. During incidents, dedicated liaisons will be available to provide 24/7 support to the state EOCs (Emergency Operation Center). Liaisons will serve as the primary link between public safety and their FirstNet resources, coordinating across federal, state, local and tribal agencies. This will give public safety agencies a level of support during emergencies that are far beyond anything they've ever seen.
This close integration with public safety and EOCs will enable the AT&T FirstNet team to better solve first responders' communications challenges.

Technology Behind the Next Heat Emergency

By Tashawn Brown

Source: https://www.domesticpreparedness.com/preparedness/technology-behind-the-next-heat-emergency/

Aug 15 – According to the National Weather Service, there were 107 fatalities across the United States related to heat in 2017 – more than the deaths related to tornados, hurricanes, and cold weather combined. Local emergency management agencies must work closely with the National Weather Service – as well as other agencies and organizations – to monitor extreme heat and related threats that can affect local communities.

Extreme heat is a significant hazard. Exposure to extreme heat over an extended period can lead to heat stroke, heat exhaustion, heat cramps, sunburn, heat rash, even death. Older adults, individuals with chronic health conditions, and people who use certain medications or abuse drugs or alcohol are among those at highest risk for heat-related illness.

Keeping Residents Cool

Cooling centers can help community members avoid the adverse effects of extreme heat. These centers are air-conditioned spaces such as senior centers, community centers, public libraries, and other public facilities that typically operate during normal business hours. Through partnerships with city agencies and organizations such as the Department for the Aging, Parks Department, Housing Authority, The Salvation Army, and public libraries, these spaces are available to the public during a heat emergency.

Before each summer, emergency management agencies should collaborate with city agencies and organizations to identify potential cooling center facilities throughout their jurisdictions.

> *"Much of our work is in identifying air-conditioned spaces that are already being utilized by community members such as senior centers and libraries," said New York City Emergency Management Advance Warning System Program Manager Christopher Pagnotta. "Residents are more likely to go to facilities that they know and trust. Many of these facilities also have daily programs and activities to engage the public and provide them relief from the heat."*

Signage to cooling center facilities in multiple languages helps the public identify cooling center site locations within their neighborhoods and understand the dangers of extreme heat.

Technological Solutions for Heat Emergencies

New York City employs several campaigns that could be adapted to the needs of other jurisdictions to inform the public and mitigate the consequences of heat-related injuries and deaths:

- New York City Emergency Management's Beat the Heat campaign encourages residents to know the hazards they may face, have a plan, and stay informed about potential heat-related injuries. This campaign includes print and digital ads featuring personal preparedness tips from older New Yorkers.
- Notify NYC is the city's free, official source for information about emergency events and important city services. Notify NYC alerts include information about National Weather Service and issued heat advisories, which provide safety tips and general information about the hazards associated with the emergency. Residents can also download a mobile application for Notify NYC, or receive emergency notification through Twitter @NotifyNYC.
- The Advance Warning System (AWS) allows New York City Emergency Management to communicate directly with organizations that serve people with disabilities, access, and functional needs before, during, and after an emergency.
- The Cooling Center Finder, which is only activated during a heat emergency, is a public online portal to view available cooling centers in the area. Once The City of New York determines the need for cooling centers, New York City Emergency Management's Geographic Information Systems (GIS) division activates the finder and is responsible for all mapping and data needs. GIS also works with cooling center partners to provide real-time updates.

During extreme heat, New York City Emergency Management officials urge individuals to go to an air-conditioned space during the hottest parts of the day. For those who may not have access to an air-conditioned space, cooling centers throughout the area offer respite, but only if they are accessible and easy to locate.

> *"The Cooling Center Finder is a map-based online tool that allows New Yorkers to get up-to-date information on cooling centers in their area," said New York City*

Emergency Management Geographic Information Systems Director Joshua Friedman. "The online portal can be activated instantaneously and is a great tool in combatting extreme heat for those without air-conditioners."

With interagency planning and collaboration, cities can minimize the impact of heat-related emergencies within their jurisdictions. Staying in constant contact with cooling center facilities and frequently updating the roster based on changes in availability – for example, if the air-conditioner at a cooling site is out of order – emergency management agencies and others charged with protecting the public can mitigate heat-related threats.

Tashawn Brown *is the press assistant at the New York City Emergency Management Department, where he has responded to various disasters and emergencies. As press assistant, he assists the press secretary and deputy press secretary in day-to-day press operations and serves as one of the agency's spokespersons, helping to develop and distribute information to the news media. He has been at the forefront of expanding the reach of New York City Emergency Management, connecting with relevant academic and trade publications to promote agency content. Prior to joining NYC Emergency Management, he worked as a research analyst at The City of New York, Mayor's Office of Media and Research Analysis.*

Preparing for a Severe Earthquake in Israel: What Can Be Done Now?

By Hilik Sofer and Meir Elran

Source: http://www.inss.org.il/publication/preparing-severe-earthquake-israel-can-done-now/

Aug 15 – Following the mild earthquakes in the Sea of Galilee area in July 2018, there was increased public awareness – albeit perhaps temporary – regarding the possibility of a powerful earthquake in Israel.

The cost of a major earthquake, which could occur in the near future, has been estimated in the assessment adopted by the government in 2012, based on a study by a professional committee headed by Dr. Benny Begin, to reach some 7,000 fatalities, 8,600 people injured, 9,500 people trapped in collapsed buildings, 28,000 severely damaged buildings, and about 170,000 individuals left homeless. Is it possible to prepare for such a severe scenario? The answer is complicated, but clearly positive. What must be done to mitigate the damage is well known - and yet, much remains to be done.

Earthquakes are natural phenomena that occur in the Middle East, as well as elsewhere. The most extensive and deadly event in the region occurred in July 1927, and before that in 1837. A powerful earthquake in Israel could be a multi-faceted disaster, largely due to the lack preparedness, and particularly because of the unstable condition of many old buildings, which were not constructed according to the anti-seismic standards published in 1980. Hence it is imperative to strengthen these edifices as part of the preventive process.

Over the last decade, Israel has invested increased efforts to prepare for earthquakes, including through two national exercises (2012 and 2017) that were dedicated entirely to this challenge. The Home Front Command's search and rescue capacities have been enhanced, as were those of the firefighters and other first responders, through the improvement of inter-organizational coordination. In addition, civilian voluntary rescue teams (SAAR – from the Hebrew acronym for Initial Self Help) have been established in several local authorities, and tenth grade pupils have been trained in rescue techniques. However, in at least two critical fields the government cannot point to adequate achievements:

a. Early warning: about 18 months ago deployment began of "tru'ah," the national early warning system for earth shocks (sensors placed along the Syrian-African rift). The current estimate is that the system will be completed by 2019; however, the budget allocated by the government for the purchase of sound alarms is insufficient for the planned scope of purchases. Moreover, notwithstanding the government decision in 2009, establishment of the Seismology Unit in the Geological Institute is not yet complete. The unit is designed to provide ongoing assessments on earthquakes for the sake of taking the necessary rescue and mitigation decisions.

b. Preventing and mitigating damage: in striking contrast to the Israeli investment of billions of shekels in sheltering, particularly in the area around the Gaza Strip, and in promoting preparedness to face the threat of rockets and missiles, including through active defense, an early warning system, reinforced Home Front Command capabilities, exercises, and enhanced coordination, the investment in preparedness for earthquakes is negligible, particularly relative to the severe risk. Ninety-nine percent of public buildings that require reinforcement – such as hospitals – remain unattended. Out of 80,000 residential buildings that have been defined as old and requiring reinforcement against earthquakes, only 2.4 percent (2780 buildings, mostly in costly high demand areas) have been reinforced as part of the TAMA 38 national plan. Recently the cabinet decided to adopt a reinforcement plan for 2019-2030 that includes a special budget allocation to reinforce buildings in high risk areas.

The considerable gaps between the level of risk and the related needs and the required response show that Israeli governments are apparently more concerned with the risks of a war and the political consequences of a war scenario than with the consequences of a destructive earthquake, which could actually be far more severe in terms of loss of life, property, and infrastructure but happens less frequently. These gaps reflect the centrality of the security challenges in the Israeli mindset, which also explains the decisive role of the IDF in the decision making process, and its natural tendency to give priority to implementing a military approach, even in this civilian context. This gap represents a failure of national magnitude.

The failure is not due to any lack of knowledge about the threat of a powerful earthquake and the enormous potential for damage to the country's population and its critical infrastructure. This has been clear from many studies and reports published over the last twenty years. The report of the State Comptroller in July 2018 states expressly that "the State is not properly prepared for a severe earthquake." In July 2017, the Internal Affairs Committee of the Knesset received a report from its Center for Research and Information that showed that an absolute majority of local authorities were not ready to cope with an earthquake. According to the figures, in 2015 only about a quarter of local authorities were ready to handle emergencies. In a Knesset debate, the Minister of the Interior stated that the government was not doing enough to prepare for a disaster.

What can be done, in the short range, to improve readiness for a severe earthquake?

a. The subject of preparing for earthquakes must be promoted to a much higher position on the national agenda. In this framework, it will be important in the first stage to ensure that all existing government resolutions on this matter are fully budgeted and actually implemented, in a reasonable timetable, and with close supervision by the relevant ministries. It is also necessary to prepare a policy of educating the public about the severity of the risk and what

can be done in advance and during the event. Public knowledge and awareness play a decisive role in saving lives in the event of a large scale disaster.

b. Define a senior national body to be affiliated with the (existing) ministerial committee on National Earthquake Readiness. This organ will be responsible for implementing government policy and for the necessary coordination between the relevant ministries, first response agencies, and local authorities. The existing steering committee is mainly an advisory body to the ministerial committee, and as such has no executive powers or legal means of obliging any sector to prepare for an earthquake. Until recently, the National Emergency Management Authority (NEMA) was also assigned to promote the preparedness for earthquakes, but the recent decision of the Minister of Defense to limit its areas of operation raises a question about its scope of responsibility, or that of the Home Front Command, in this matter. In any event, the proposed organ must be responsible for coordination between the relevant agencies before, during, and following an earthquake, to include the long and complex stage of recovery. Presently, the Prime Minister's Office is responsible for recovery; this arrangement should be revisited in this context. At any rate, this entire issue should be regulated by legislation, so as to ensure that the organization in charge will have enforcement authority.

c. Local authorities must have the executive responsibility for managing the disaster on the ground, as it occurs. This is a difficult, complex task, especially since many of the relevant localities lack the capacity to stand up to the mission. Therefore the government must help them with resources and training, to develop the required overall capability.

d. There must be an immediate change in the concept and method of reinforcing construction. Implementation of existing plans to reinforce public buildings must be revived and prioritized according to their necessity and location with respect to the expected earthquake. At the same time, it is essential to update the concept regarding reinforcement of residential buildings, with preference given to areas close to earthquake risk zones, particularly in peripheral areas, where TAMA 38 and the "Vacate & Construct" plans are not economically viable. For this purpose, the Ministries of the Interior and Housing should oblige the relevant local authorities to define and implement a quota of building reinforcement, where the cost will be divided between the owners of the assets, the local authorities, and the government.

The current state of preparedness for a powerful earthquake is lacking and worrying, but it can be improved greatly, including by utilization of the far greater preparedness for security disruptions. This requires the government to make the right decisions in the immediate term, and to invest a concentrated and ongoing effort to remedy the situation. The process will probably be long, but it must be launched immediately. Public awareness and pressure could help advance this matter.

***Colonel Dr. (res.)* Hilik Sofer** *is a former member of the National Steering Committee for Earthquake Readiness and a senior member of Home Front Command.*
***Brig. Gen. (ret.) Dr.* Meir Elran** *is a senior research fellow at INSS, and head of the Homeland Security program at INSS.*

New first-responder safety, efficiency systems on the way

Source: http://www.homelandsecuritynewswire.com/dr20180817-new-firstresponder-safety-efficiency-systems-on-the-way

Aug 17 – Two homeland security technologies will be developed jointly by American and Israeli companies to increase the safety and efficiency of first-responders (law enforcement, firefighters and emergency medical services) after getting funding from the Israel-U.S. Binational Industrial Research and Development (BIRD) Foundation.

ELTA Systems (Ashdod, Israel), a group and subsidiary of Israel Aircraft Industries, and TLC Solutions (St. Augustine, Florida) will develop an advanced drone-mounted search-and-rescue system for locating victims under ruins and in disaster areas by accurate location of their cellular phones.

HiRiseTech (Petah Tikva, Israel) and Allstate Sprinkler (Bronx, New York) will develop a first-responder emergency radio repeater system for existing high-rise buildings.

These projects were selected by the US Department of Homeland Security Science and Technology Directorate and the Israeli Ministry of Public Security. In addition to the BIRD

grants, the two projects will access private sector funding, boosting their total value to approximately $4.5 million.

"Our interactions with the First Responder communities in the U.S. and Israel have revealed a critical need for innovation and affordable technology that can be used in the field," said BIRD Foundation Executive Director Eitan Yudilevich.

"Our cooperation with the BIRD Foundation serves as a strategic channel for the development and implementation of innovative Israeli technologies for first-responders by improving and advancing their emergency preparedness," said Gad Frishman, chief scientist of the Israeli Ministry of Public Security.

The BIRD Foundation works to encourage and facilitate cooperation between US and Israeli companies in a wide range of technology sectors and offers funding to selected projects. BIRD has approved 967 projects over its 41-year history.

Texas Students Undergo Drone Training for Public Safety Use

Source: http://www.govtech.com/em/preparedness/Sharyland-Students-Undergo-Drone-Training-for-Public-Safety-Use.html

Aug 15 — "When you take the test, make sure you read and understand the question and answers and draw the scenario out," John David Franz Jr. reminded the incoming high school seniors seated in front of him.

While applicable to almost any testing situation, Franz's advice wasn't geared toward the typical exam most students take. Rather, he was helping a dozen or so Sharyland High School students prepare for their remote pilot certificate exam — the first step toward operating drones legally for a law enforcement agency or private company.

The students spent last Thursday reviewing airspace, weather and aircraft performance, all topics on the Federal Aviation Administration's (FAA) Unmanned Aircraft Systems Drone Knowledge Test.

As president of S.O.A.R.D. Solutions LLC, a drone operations and consulting firm in McAllen, Franz frequently gives certification courses to working professionals in law enforcement, emergency operations and engineering fields.

Through a new partnership between the company and Sharyland Independent School District, students will receive this training, and then some.

"When they graduate, they're not only going to be certified, but they'll have logged training hours to show they've actually put the work in," Franz said of the partnership, the first of its

kind in Texas. "These students will have more experience and flight time than most of your first responders and public safety drone pilots."

Taking the 40-hour certification course, administered through a four-day period, and passing the drone knowledge test are just the first steps: Sharyland High School and Pioneer High School students in the Career and Technical Education (CTE) program's Law, Public Safety, Corrections & Security practicum will spend the rest of the school year learning how drones are used for search and rescue operations and damage assessments, and will be exposed to 3-D mapping and thermography.

"People might see (drones) as a toy because you can buy one at Best Buy or at Walmart. They're not really seeing it as a tool yet," Franz said. "There have been some early adopters … but for the most part, I don't think we've really capitalized in South Texas with drones to their full capability."

Mostly, S.O.A.R.D. has helped launch drone programs at smaller agencies, such as the Brooks County Sheriff's Office and volunteer fire department, and the Falfurrias and Raymondville police departments. Drones "empower the smaller agencies," Franz said. "Resources are scarce and they need to use them to their full capacity to be effective."

The company has also provided training to Weslaco's police and fire departments, the Edinburg and Mission fire departments, Cameron County Emergency Management & Fire Marshal Service and U.S. Fish and Wildlife Service's law enforcement division. S.O.A.R.D. also hopes to partner with more Valley school districts in the near future.

Because drone technology is relatively new, public safety agencies and commercial drone operators, such as realtors and engineers, may not be familiar with the laws regarding drone use, Franz said.

"While (inadvertently violating a law) may help you on the ground, it's going to hurt you in the long-run," he said, giving the example of how evidence illegally collected by a drone is later inadmissible in court.

The Law, Public Safety, Corrections & Security practicum is one of the district's top three most popular career clusters, Sharyland ISD CTE Director Yoelia Nava said.

"We ask business and industry partners what's trending, what's the newest technology," Nava said of some of the factors the district considered when adding this component to the existing year-long practicum course. "We were looking at how we could redesign, enhance and improve what we already have (for students)."

Eternity Garcia, 17, hopes to work as a firefighter when she graduates from Sharyland High School next spring and only recently learned drones could be used for search and rescue operations after seeing a video on YouTube.

"I always wanted to be in law enforcement," Garcia said, noting that she narrowed down her career interest after competing in a firefighter search and rescue competition this past spring. Finding a baby in a timed obstacle course simulating a house fire was the objective of the competition, which required her to wear full protective gear while identifying tools.

"It's hard and time consuming," she said of the remote pilot certification course. "It's not just the in-class hours, it's after class hours when you're reading over the materials."

Representatives from the law enforcement agencies that S.O.A.R.D. has worked with will attend the practicum class throughout the year, Nava said, so "students (not) only have the certification and know how to fly a drone, but know how the actual entities here near us are using (drones) for security and law enforcement purposes."

"Because they will have this skill set, they're going to be that much better at the job," Franz said of students who may find employment with an agency without a drone program, adding that they'll have the know-how to introduce drone technology to their future employer.

Garcia took her remote pilot certification exam Monday and passed. The multiple-choice exam consisted of "almost exactly everything we went over (in the certification course)," she said.

EDITOR'S COMMENT: Drone classes are good and a clever thematic introduction addressing future professionals. I hope one day to read that univercities' medical and nursing schools will embrace

"CBRN Medicine" into their curricula. Do not forget that all casualties, patients, and victims finally end up at the hospitals – ALL hospitals!

rescEU: a new European system to tackle natural disasters

Source: https://ec.europa.eu/echo/news/resceu_en

Nov 23, 2017 – Today the European Commission revealed ambitious new plans to strengthen Europe's ability to deal with natural disasters.

The proposal is a central part of President Juncker's agenda of a Europe that protects. The initiative comes in light of more complex and frequent natural disasters that have seriously affected many European countries over recent years. A key part of the proposal is the creation of rescEU, a reserve at European level of civil protection capabilities such as aerial forest fighting planes, special water pumps, urban search and rescue and field hospitals and emergency medical teams. These will complement national assets and will be managed by the European Commission in order to **support countries hit by disasters such as floods, forest fires, earthquakes and epidemics.** Alone in 2017, over 200 people were killed by natural disasters in Europe and over one million hectares of forest have been destroyed.

President Jean-Claude Juncker said: *"Europe can't be on the side-lines when our Member States suffer from natural disasters and need help. No country in Europe is immune to natural disasters which have sadly become the new normal. When a disaster strikes, I want the European Union to offer more than condolences. Europe is a continent of solidarity and we must be better prepared than before, and faster in helping our Member States on the frontline."*

"The tragedies of last summer and the past few years have shown that our current disaster response system has reached its limits in its existing voluntary format. The challenges we face have evolved, and so must we. It is a matter of solidarity and shared responsibility at all levels. This is what European citizens expect from us and I now look to European governments and the European Parliament to embrace this proposal," said Christos Stylianides**,** Commissioner for Humanitarian Aid and Crisis Management.

The Commission proposal focuses on two complementary strands of action: creating a stronger collective response at the European level, and improved prevention and preparedness capacities.

Strengthening European response capacities: rescEU

An EU civil protection response reserve of civil protection assets will be established to assist Member States in responding to disasters, when national capacities are overwhelmed. This reserve will be called rescEU and will include assets, such as firefighting aircraft and water pumping equipment, which will complement national capacities. All costs and capacities of rescEU would be fully covered by EU financing, with the Commission retaining the operational control of these assets and deciding on their deployment.

In parallel, the Commission will assist Member States in boosting their national capacities, by financing the adaptation, repair, transport and operation costs of their existing resources – whereas today only transportation costs are covered. These assets would become part of

a shared pool of emergency response resources under the European Civil Protection Pool, and would be made available for deployment when disaster strikes.

Stepping up disaster prevention and preparedness

Under today's proposal, Member States will be asked to share their national prevention and preparedness strategies, in order to collectively identify and address possible gaps.The proposal strengthens cooperation and coherence with existing EU policies dealing with prevention and preparedness. This includes for example the EU Strategy on Adaptation to Climate Change, the European Structural and Investment Funds, the Solidarity Fund, environmental legislation (e.g. flood management plans and eco-system based solutions), research and innovation and policies to address serious cross-border threats to health and more.

Finally, the proposal will streamline and simplify administrative procedures in order to reduce the time needed to deploy life-saving assistance.

Background

The EU's Civil Protection Mechanism is currently based on a voluntary system, through which the EU coordinates the voluntary contributions of participating states to a country that has requested assistance. Offers of assistance are coordinated by the European Emergency Response Coordination Centre, based in Brussels. In recent years, extreme weather conditions and other phenomena have stretched the ability of Member States to help each other, especially when several Member States face the same type of disaster simultaneously. In such cases, the EU does not have a reserve capacity to assist overwhelmed Member States.

2017 has seen a wide range of disasters. In total, over 200 people were killed by natural disasters in Europe in 2017. But natural disasters have also a severe economic impact. Since 1980, as well as the human cost, EU Member States have lost over €360 billion in weather and climate extreme events. In Portugal alone, the direct economic damage of forest fire events between June and September is estimated at close to €600 million, representing 0.34% of Portugal's gross national income.

Since its establishment in 2001, the EU Civil Protection Mechanism has monitored over 400 disasters and has received over 250 requests for assistance. The EU Civil Protection Mechanism can be activated in response to man-made and natural disasters, but also supports disaster preparedness and prevention. The EU Civil Protection Mechanism includes all EU Member States as well as several other participating states outside the EU, namely, Iceland, Norway, Serbia, the former Yugoslav Republic of Macedonia, Montenegro and Turkey. rescEU would be extended to these participating states as a sign of European solidarity.

EDITOR'S COMMENT: Floods, forest fires, earthquakes and epidemics in the same basket? Really? Floods can be seen coming ([relatively] enough time for assistance); erthquakes' response will take some day (enough for assistance); epidemics (progressive emergency – enough time for assistance; pandemic is a better word) BUT fires burn forests, houses and people at no time! Unless if we are talking about wild fires on top of mountains in the middle of nowhere. Do you think you transfer a mobile hospital in 1 hour? Even fire planes need a day to relocate and those with experience in fires or have been victims of wild fires [like myself] know very well how fire progresses in just a few minutes.


ICI
International
CBRNE
INSTITUTE
CBRNE-Terrorism Newsletter
W
O
M
D
C2BRNE
DIARY
ASYMMETRIC
THREATS

Climate change and wildfires – how do we know if there is a link?

By Kevin Trenberth

Source: http://www.homelandsecuritynewswire.com/dr20180814-climate-change-and-wildfires-how-do-we-know-if-there-is-a-link

Aug 14 – Once again, the summer of 2018 in the Northern Hemisphere has brought us an epidemic of major wildfires.

These burn forests, houses and other structures, displace thousands of people and animals, and cause major disruptions in people's lives.The huge burden of simply firefighting has become a year-round task costing billions of dollars, let alone the cost of the destruction. The smoke veil can extend hundreds or even thousands of miles, affecting air quality and visibility. To many people, it has become very clear that human-induced climate change plays a major role by greatly increasing the risk of wildfire.

Yet it seems the role of climate change is seldom mentioned in many or even most news stories about the multitude of fires and heat waves. In part this is because the issue of attribution is not usually clear. The argument is that there have always been wildfires, and how can we attribute any particular wildfire to climate change?

As a climate scientist, I can say this is the wrong framing of the problem. Global warming does not cause wildfires. The proximate cause is often human carelessness (cigarette butts, camp fires not extinguished properly, etc.), or natural, from "dry lightning" whereby a thunderstorm produces lightning but little rain. Rather, global warming exacerbates the conditions and raises the risk of wildfire.

Even so, there is huge complexity and variability from one fire to the next, and hence the attribution can become complex. Instead, the way to think about this is from the standpoint of basic science – in this case, physics.

Global warming is happening

To understand the interplay between global warming and wildfires, consider what's happening to our planet.

The composition of the atmosphere is changing from human activities: There has been over a 40 percent increase in carbon dioxide, mainly from fossil fuel burning since the 1800s, and over half of the increase is since 1985. Other heat-trapping gases (methane, nitrous oxide, etc.) are also increasing in concentration in the atmosphere from human activities. The rates are accelerating, not declining (as hoped for with the Paris agreement).

This leads to an energy imbalance for the planet.

Heat-trapping gases in the atmosphere act as a blanket and inhibit the infrared radiation – that is, heat from the Earth – from escaping back into space to offset the continual radiation coming from the sun. As these gases build up, more of this energy, mostly in the form of heat, remains in our atmosphere. The energy raises the temperature of the land, oceans and atmosphere, melts ice, thaws permafrost, and fuels the water cycle through evaporation.

Moreover, we can estimate Earth's energy imbalance quite well: It amounts to about 1 watt per square meter, or about 500 terawatts globally.

While this factor is small compared with the natural flow of energy through the system, which is 240 watts per square meter, it is large compared with all other direct effects of human activities. For instance, the electrical power generation in the U.S. last year averaged 0.46 terawatts.

The extra heat is always the same sign and it is spread across the globe. Accordingly, where this energy accumulates matters.

Tracking the Earth's energy imbalance

The heat mostly accumulates ultimately in the ocean – over 90 percent. This added heat means the ocean expands and sea level rises.

Heat also accumulates in melting ice, causing melting Arctic sea ice and glacier losses in Greenland and Antarctica. This adds water to the ocean, and so the sea level rises from this as well, rising at a rate of over 3 millimeters year, or over a foot per century.

On land, the effects of the energy imbalance are complicated by water. If water is present, the heat mainly goes into evaporation and drying, and that feeds moisture into storms, which produce heavier rain. But the effects do not accumulate provided that it rains on and off.

However, in a dry spell or drought, the heat accumulates. Firstly, it dries things out, and then secondly it raises temperatures. Of course, "it never rains in southern California" according to the 1970s pop song, at least in the summer half year.

So water acts as the air conditioner of the planet. In the absence of water, the excess heat effects accumulate on land both by drying everything out and wilting plants, and by raising temperatures. In turn, this leads to heat waves and increased risk of wildfire. These factors apply in regions in the western U.S. and in regions with Mediterranean climates. Indeed many of the recent wildfires have occurred not only in the West in the United States, but also in Portugal, Spain, Greece, and other parts of the Mediterranean. The conditions can also develop in other parts of the world when strong high pressure weather domes (anticyclones) stagnate, as can happen in part by chance, or with increased odds in some weather patterns such as those established by either La Niña or El Niño events (in different places). It is expected that these dry spots move around from year to year, but that their abundance increases over time, as is clearly happening.

How big is the energy imbalance effect over land? Well, 1 Watt per square meter over a month, if accumulated, is equivalent to 720 Watts per square meter over one hour. 720 Watts is equivalent to full power in a small microwave oven. One square meter is about 10 square feet. Hence, after one month this is equivalent to: one microwave oven at full power every square foot for six minutes. No wonder things catch on fire!

Attribution science

Coming back to the original question of wildfires and global warming, this explains the argument: there is extra heat available from climate change and the above indicates just how large it is.

In reality there is moisture in the soil, and plants have root systems that tap soil moisture and delay the effects before they begin to wilt, so that it typically takes over two months for the effects to be large enough to fully set the stage for wildfires. On a day to day basis, the effect is small enough to be lost in the normal weather variability. But after a dry spell of over a month, the risk is noticeably higher. And of course the global mean surface temperature is also going up.

"We can't attribute a single event to climate change" has been a mantra of climate scientists for a long time. It has recently changed, however.

As in the wildfires example, there has been a realization that climate scientists may be able to make useful statements by assuming that the weather events themselves are relatively unaffected by climate change. This is a good assumption.

Also, climate scientists cannot say that extreme events are due to global warming, because that is a poorly posed question. However, we can say it is highly likely that they would not have had such extreme impacts without global warming. Indeed, all weather events are affected by climate change because the environment in which they occur is warmer and moister than it used to be.

In particular, by focusing on Earth's Energy Imbalance, new research is expected to advance the understanding of what is happening, and why, and what it implies for the future.

***Kevin Trenberth** is Distinguished Senior Scientist, National Center for Atmospheric Research. Transboundary River Basins and Political Tensions," Sustainable Security (13 July 2017).*