Dedicated to Global First Responders

CBRNE NEWSLETTERRORISM

January 2018

www.cbrne-terrorism-newsletter.com

Dirty R News

Forget North Korea: Russia Is Now Building EMP Weapons

Source: http://nationalinterest.org/blog/the-buzz/forget-north-korea-russia-now-building-emp-weapons-23760

Image: Russian RS-24 Yars/SS-27 Mod 2 solid-propellant intercontinental ballistic missiles during the Victory Day parade, Moscow, May 9, 2015. Reuters/RIA Novosti.

Dec 22 – Amid all the recent fears about North Korea building an electromagnetic-pulse weapon that could disrupt America's electronic backbone, another potential threat has been ignored: Russia's new Alabuga EMP weapons program.

Russian media describes a program that appears to be aimed at developing tactical EMP weapons that would affect a small area, rather than strategic arms that would disable, say, a nation's entire electrical grid.

"One component of the program involves the development of an EMP missile that emits an electromagnetic pulse 200-300 meters above an enemy position by means of a high-frequency high-power electromagnetic field generator," according to an article in *Rossiyskaya Gazeta* and translated by the U.S. Army's Foreign Military Studies Office. "This EMP would create an ultra high frequency (UHF) field of approximately 3.5 kilometers, not only disabling computers, radars, communications systems and precision weapons, but also making them unusable by damaging their electronic components. Although the system is nonlethal and causes no adverse effects to humans, the electromagnetic effects of the missile (up to 100 gigawatts) are reportedly comparable to a nuclear weapon."

The U.S. Army also translated a *Svobodnaya Pressa* article on a Russian ground-based EMP weapon designed to bring down aircraft. "The Ranets-Ye is based on a MAZ-543 wheeled chassis, weighing around 5 tons. The Ranets-Ye is essentially a short-range surface-to-air system in which the kill element utilized is not a missile, but a 60 degree cone of 500 megawatt SFH radiation that lasts 20 nanoseconds. This EMP is capable of neutralizing all aircraft, cruise missiles, and any munition with electronics. At a range of 8-14 kilometers [4 to 8 miles] the EMP destroys electronic components, and disrupts electronic at a range of up to 40 kilometers [24 miles]. The Ranets-Ye consists of a diesel generator, electromagnetic pulse generator, and targeting radar. The system is also reportedly capable of integrating into air defense networks, in order to obtain targeting data."

Russian media suggested that Ranets-Ye would be very effective as an air-defense weapon against stealth aircraft and UAVs. Yet significantly, Russian media also noted that the

Russian military had not adopted Ranats-Ye because it needs a direct line of sight to the target, and because it needs twenty minutes to recharge its capacitors between pulses.

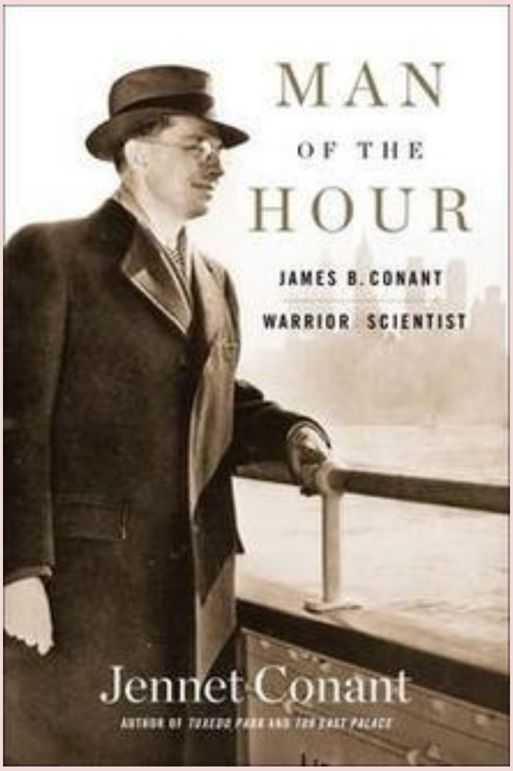
Meanwhile, the United States is working on its own EMP weapons. The Counter-electronics High-powered Microwave Advanced Missile Project, or CHAMP, aims to mount a microwave emitter on a cruise missile. Such a weapon has been touted as a less violent means of disabling the electronics on a North Korean ICBM before it could be launched at the United States. Critics reply that if America were to attack North Korean WMDs, it might just as well use conventional munitions from the start.

***Michael Peck** is a contributing writer at Foreign Policy Magazine and a writer for the War is Boring defense blog.*

Is atomic bomb scientist James Conant's "nightmare scenario" taking shape?

Source: https://www.cbsnews.com/news/atomic-bomb-chemist-james-conant-nuclear-war-granddaughter-jennet/

Dec 27 – James Conant, the American scientist who played a key role in the creation of the first atomic bomb, never regretted dropping it on Hiroshima, Japan, at the end of World War II. But he was afraid of a nuclear standoff, similar to the one brewing today between the United States and North Korea.



Now Conant's granddaughter, the best-selling author Jennet Conant, is writing about his life and career in the new book, "Man of the Hour: James B. Conant, Warrior Scientist," published by Simon & Schuster, a division of CBS.

"This was his nightmare scenario, that we would have this enormous arms race and that it would just increase sort of unabated, and that we would inevitably find ourselves, as he said, 'like two gunmen with itchy trigger fingers,'" she told CBS News correspondent Tony Dokoupil.

James Conant wasn't the kind of person given to fear or exaggeration, and yet, "My grandfather was really so terrified of a nuclear conflict… I think the idea that mutually assured destruction would have held for almost 70 years would have surprised him," Jennet said.

In the late '30s, Conant was a brilliant chemist, a veteran of poison gas production during World War I, and a successful president of Harvard University. But his life changed course after Albert Einstein warned the White House about the potential for "extremely powerful bombs."

That triggered a desperate race to build a nuclear weapon before Hitler's Germany could do so. The task of winning fell to Conant and a secret team of scientists.

"He was the supervisor of everything that happened in terms of the bomb's development," Jennet said.

What happened in the summer of 1945 was the first open-air test of a nuclear weapon – a blast so shocking that Conant, from a nearby bunker, was sure the team had miscalculated.

"He thought, in that moment, the world is over," Dokoupil said.

"He did. Terrifying. Absolutely terrifying," Jennet Conant said.

Three weeks later, Hiroshima and then Nagasaki became the targets of the only wartime uses of a nuclear weapon.

"We have spent more than $2 billion on the greatest scientific gamble in history – and we have won," then-President Harry S. Truman said.

Hundreds of thousands died in the blasts and their aftermath.

"People always ask me, you know, 'Did they feel guilty?' They really felt that they had done the right thing in building that bomb. It did shorten the war. It did save lives," Jennet said.

Conant and his colleagues warned of the need to control the bomb by sharing the science and striking a global deal to curtail production. But the scientists were overruled, and today, nine countries have confirmed or suspected nuclear arsenals, including the rogue regime of North Korea, which is testing missiles and threatening nuclear destruction.

"Do you feel safer or less safe?" Dokoupil asked.

"Oh, we're less safe. We have this massive destructive force out there… and ultimately, he said, we have no sane option but for the international community to come together and try and find a way to control these weapons," Jennet said.

"There hasn't been a mushroom cloud seen live in seven decades," Dokoupil pointed out.

"'Don't tempt fate,' that's what my grandfather would say. These are not weapons to play with," she responded. "We must find a more sane way forward."

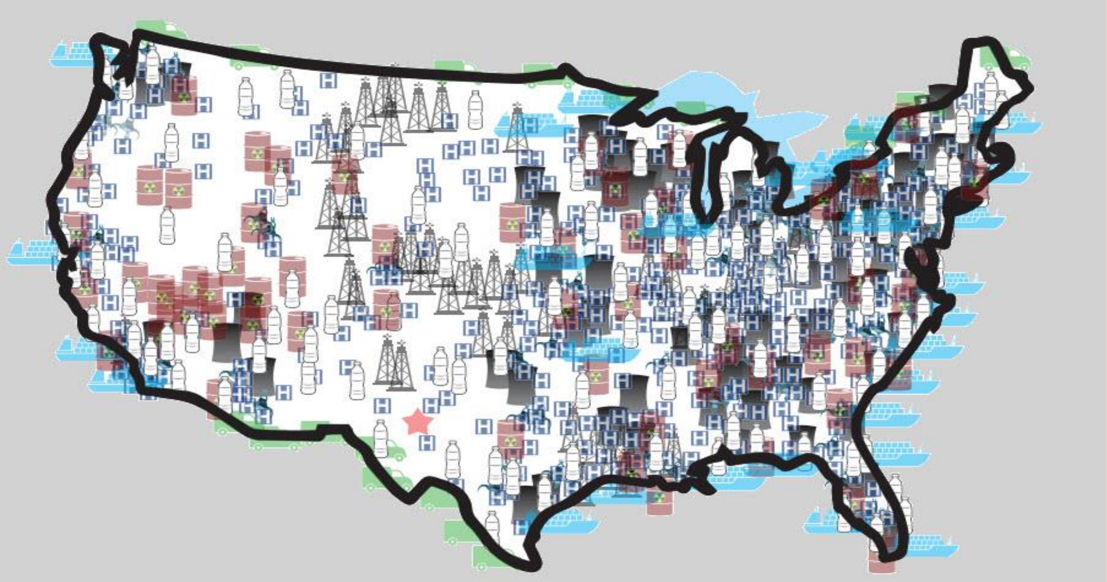
"We must, but will we?"

"I hope and pray," she said.

This year's Nobel Peace Prize went to an organization hoping to ban nuclear weapons, and last summer the United Nations advanced the first treaty to do so. The U.S., however, boycotted the talks, saying the timing is not right to lay down nuclear arms.

Where Can Radiation Be Found in the U.S.?

Source: https://www.thermofisher.com/blog/identifying-threats/2018/01/02/where-can-radiation-be-found-in-the-u-s/



Jan 02 – Radiation sources are more common than you might realize. In addition to nuclear power plants and waste sites, radiation can be found in thousands of locations across the United States. Would you guess that radiation can be found at:

- ports and border crossings
- food and packaging analysis and testing facilities
- construction sites
- scrap metal recycling yards
- oil and gas exploration locations
- medical facilities

Those sources are also on the move via highways and railways.

Knowing where they are, and being able to monitor, detect, and respond is critical to public safety. We've developed a poster and a video map that outline the various locations of radiation threats. Be aware, view the map, and make a plan.

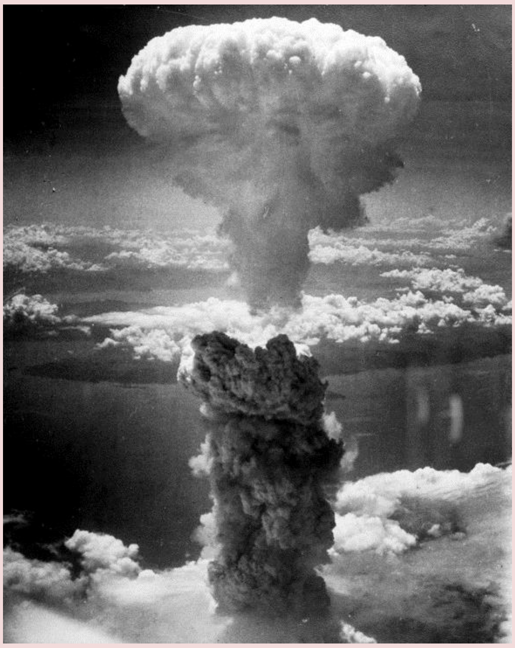
View the video map and a PDF poster: U.S. Map of Radiation Threats

The Photograph That Showed Us What Nuclear Destruction Could Look Like

Source: https://www.artsy.net/article/artsy-editorial-photograph-nuclear-destruction

Jan 05 – "I too have a Nuclear Button," United States President Donald Trump wrote in a recent tweet directed at North Korea's leader, Kim Jong-un. "But it is a much bigger & more powerful one than his, and my Button works!"

As such public tensions continue to ratchet up the threat of a future nuclear war, one iconic photograph from World War II endures as a frightening reminder of the devastating force of weapons of mass destruction.



The photograph, taken on August 9th, 1945, shows a 45,000-foot-tall mushroom cloud erupting over Nagasaki, Japan, in the wake of an atomic bomb. The explosion came just days after the detonation of the world's first deployed atomic bomb, codenamed "Little Boy," which was dropped by the U.S. on Hiroshima, killing an estimated 140,000 people. Three days, later, this second atomic bomb ("Fat Man") claimed the lives of nearly 80,000 people in Nagasaki. (These figures don't take into account long term radiation effects that have persisted for decades.)

Twenty-six-year-old lieutenant Charles Levy captured the photograph of the devastation of Nagasaki with his personal camera while aboard the B-29 aircraft *The Great Artiste,* an observation plane that flew near the strike plane *Bockscar* to record the power of the blast. And it's fortunate that Levy did. According to the book *Critical Assembly*, a physicist with a high-speed Fastax camera had originally been scheduled to capture the explosion from the camera plane, *Big Stink,* but while gearing up he accidentally grabbed a second life raft—instead of a parachute—and as a result was forced to remain back at the airfield. Further, the camera plane didn't make it to the meeting point on time to join the other two planes on the mission. As a result Levy, the bombardier on *The Great Artiste*, snapped what became one of the most defining images of the explosion. (Levy was originally scheduled to fly on *Bockscar* but his crew switched planes after a last-minute complication—otherwise, one could reason, this image may not exist.)

Levy's image shows a giant plume of smoke and debris erupting from the earth and piercing through the clouds, reaching over eight miles into the sky. It's an unprecedented visualization of this degree of military force. As the mushroom head spouts in a puff from the pillar of smoke, the explosion appears to have taken on a life of its own—a fearsome button that can never be unpressed.

As Levy told the *Free Lance-Star* newspaper at the time, the explosion was "sharp and brighter than double daylight itself inside [the] plane." Afterward, he says: "We saw this big plume climbing up, up into the sky. It was purple, red, white, all colours – something like boiling coffee. It looked alive…we were all plenty scared."

Prior to the explosion, U.S. President Harry S. Truman told Japan that if it did not surrender to U.S. terms, they "may expect a rain of ruin from the air, the like of which has never been seen on this earth." This photograph shows that his threat was no exaggeration.

According to *TIME*, photographs that pictured the bomb's devastation on the ground were censored by U.S. officials, and yet Levy's image of the explosion itself circled the globe. It was the only image to emerge that would show the massive cloud in its entirety; it also showed the explosion as if it occurred in a vacuum, a God-like use of force and modern science that transcended the earth and penetrated the heavens and ultimately, led to the United States' victory and Japanese surrender.

(Though there was a small portion of Japan's supreme war council that wanted to surrender after the first bomb.) It didn't show the over three-mile radius of carnage back on earth, or capture the unbelievable loss of human life.

Instead, in its simplicity—a celestial white shape isolated against a contrasting grey sky—the explosive form Levy captured would emerge as a motif of American power and a symbol of the dawning atomic age. It would be replicated endlessly throughout popular culture—from t-shirts to films to the recent Apple emoji that illustrates a "blown mind" by portraying a brain emitting a mushroom cloud through the crown of a bright yellow head.

It's worth noting that today's nuclear weapons are more powerful than the two atom bombs dropped on Hiroshima and Nagasaki combined, often by thousands of multiples. Levy's indelible image of the mushroom cloud spread through culture as a somewhat superficial emblem of victory and power, as proof that military and science intelligence could accomplish this degree of force and totality—but it obscures the very extreme human toll that resulted from this force.

On the 26,000 tons of radioactive waste under Lake Powell. And more.

By Jonathan P. Thompson

Source: https://thebulletin.org/26000-tons-radioactive-waste-under-lake-powell-and-more11389

Beneath the murky green waters on the north end of Lake Powell, entombed within the tons of silt that have been carried down the Colorado River over the years, lies a 26,000-ton pile of un-remediated uranium mill tailings. It's just one polonium-, bismuth-, thorium-, and radium-tainted reminder of the way the uranium industry, enabled by the federal government, ravaged the West and its people for decades.

In 1949, the Vanadium Corporation of America built a small mill at the confluence of White Canyon and the Colorado River to process uranium ore from the nearby Happy Jack Mine, located upstream in the White Canyon drainage (and just within the Obama-drawn Bears Ears National Monument boundaries). For the next four years, the mill went through about 20 tons of ore per day, crushing and grinding it up, then treating it with sulfuric acid, tributyl phosphate and other nastiness. One ton of ore yielded about five or six pounds of uranium, meaning that each day some 39,900 pounds of tailings were piled up outside the mill on the banks of the river.

In 1953 the mill was closed down, and the tailings left where they sat, uncovered, as was the practice of the day. Ten years later, water began backing up behind the newly built Glen Canyon Dam; federal officials decided just to let the reservoir's waters inundate the tailings. There they remain today.

If you're one of the millions of people downstream from Lake Powell who rely on Colorado River water and this worries you, consider this: Those 26,000 tons of tailings likely make up just a fraction of the radioactive material contained in the silt of Lake Powell and Lake Mead.

During the uranium days of the West, more than a dozen mills—all with processing capacities at least 10 times larger than the one at White Canyon—sat on the banks of the Colorado River and its tributaries, including in Shiprock and Mexican Hat on the San Juan River; in Rifle and Grand Junction and Moab on the Colorado; and in Uravan along the San

Miguel River, just above its confluence with the Dolores. They did not exactly dispose of their tailings in a responsible way.

At the Durango mill the tailings were piled into a hill-sized mound just a stone's throw from the Animas River. They weren't covered or otherwise contained, so when it rained tailings simply washed into the river. Worse, the mill's liquid waste stream poured directly into the river at a rate of some 340 gallons per minute, or half-a-million gallons per day. It was laced not only with highly toxic chemicals used to leach uranium from the ore and iron-aluminum sludge, a milling byproduct, but also radium-tainted ore solids. (Crass self-promotion: For more details on the Durango mill read my book, River of Lost Souls).

Radium is highly radioactive and a "bone-seeker," meaning that when it's ingested it makes its way to the skeleton, where it decays into other radioactive daughter elements, including radon, and bombards the surrounding tissue with alpha, beta, and gamma radiation. According to the Toxic Substances and Diseases Registry, exposure leads to "anemia, cataracts, fractured teeth, cancer (especially bone cancer), and death."

It wasn't any better at any of the other mills. In the early 1950s, researchers from the U.S. Public Health Service sampled Western rivers and found that "the dissolved radium content of river water below uranium mills was increased considerably by waste discharges from the milling operations" and that "radium content of river muds below the uranium mills was 1,000 to 2,000 times natural background concentrations."

That was just from daily operations. In 1960, one of the evaporation ponds at the Shiprock mill broke, sending at least 250,000 gallons of highly acidic raffinate, containing high levels of radium and thorium, into the river. None of the relevant officials were notified and individual users continued to drink the water, put it on their crops, and give it to their sheep and cattle. It wasn't until five days later, after hundreds of dead fish had washed up on the river's shores for sixty miles downstream, that the public was alerted to the disaster.

Of course, what's dumped into the river at Shiprock doesn't stay in Shiprock. It slowly makes its way downstream. In the early 1960s, while Glen Canyon Dam was still being constructed, the Public Health Service folks did extensive sediment sampling in the Colorado River Basin, with a special focus on Lake Mead's growing bed of silt, which had been piling up at a rate of 175 million tons per year (!) since Hoover Dam started impounding water in 1935. The Lake Mead samples had higher-than-background levels of radium-226. The report thus concludes:

"The data have shown, among other things, that Lake Mead has been essentially the final resting place for the radium contaminated sediments of the Basin. With the closure of Glen Canyon Dam upstream, Lake Powell will then become the final resting place for future radium contaminated sediments. The data also show that a small fraction of the contaminated sediment has passed through Lake Mead to be trapped by Lakes Mohave and Havasu."

And so, the billions of tons of silt that has accumulated in Lake Mead and Lake Powell serve as archives of sorts. They hold the sedimental records of an era during which people, health, land, and water were all sacrificed in order to obtain the raw material for weapons that are capable of destroying all of humanity.

***Jonathan P. Thompson** is an award-winning freelance author, journalist and editor. He usually writes about the land, culture, and communities of the American West, with an emphasis on energy development, pollution, land-use politics, and economics. He is the author of River of Lost Souls*: The Science, Politics, and Greed Behind the Gold King Mine Disaster *(Torrey House Press, February 2018) and is a contributing editor at High Country News.*

MBD-2

Source: https://www.mirion.com/

The MBD-2 dosimeter is a real-time, self-indicating device that requires no user intervention for operation. The MBD-2 dosimeter is based upon Mirion Technologies' patented Direct Ion Storage (DIS) technology. Direct Ion Storage technology is a method for detecting ionizing radiation through use of an ion chamber detector combined with a simplified method for computing dose from a voltage value from the detector.

The MBD-2 measures and records dose for gamma, neutron, and beta (shallow). It is ergonomic, and designed to be worn comfortably on the wrist (watch-type), or clipped to a garment (badge-type). The MBD-2 is lightweight, dark grey or black in color and low profile in size. Its edges are rounded to accommodate clothing and gear. The device closely resembles a wristwatch and therefore is natural to observe when reading the display.

Product Features

- Accurate and reliable Direct Ion Storage technology hybrid device (active/passive)
- NFC and/or BLE communication
- Self-reading for effective decision making
- Hands-free operation
- Programmable display
- Configurable operating parameters
- Wrist worn or clipped to lanyard or garment
- Internal histogram
- Pulsed-xray measurements to 65nsec pulses

DIS Dosimetry System

Combining reliable ionization chamber technology with an electronic Direct Ion Storage memory cell, the DIS Series of personal electronic radiation dosimeters offers and repeatedly read on-site, and have the capability to operate in pulsed fields.

The excellent radiological features and the fast and simple reading of the DIS-1 dosimeter with low-cost readers makes the DIS system superior to any Film dosimetry or TLD system. The DIS-1 Dosimetry system, supported by WinELD Software, has found its place among the legal dosimetry and has been accredited in several countries in Europe, Middle East and Asia.

Whether a small in-house system with one dosimeter reader and just a few users or a large facility with thousands of users needing a network of readers - the DIS offers a total solution with highly efficient dosimetry manangement with very little additional staff workload.

ECONOMICAL AND ENVIRONMENTALLY FRIENDLY

- Very low investment costs for a starting system
- Flexible system solutions based on available infrastructure and requirements
- No consumables such as nitrogen gas or packing materials
- Badges can be read locally with only the data being sent forward
- No monthly distribution of dosimeters

PLUG AND PLAY

- Pre-calibrated dosimeters and readers can be used instanly in any system
- Personal dose equivalent measured in a few seconds
- Unlimited dose readouts
- No specialists or additional manual labor required in routine use
- Effortless extension of system for new sites over the internet

MEASURING, COLLECTING, RECORDING AND REPORTING

- Dosimeter can be reset to display doses for either specific time periods (day, week, month) or specific tasks
- Dose information is recorded automatically into a database every time a read-out is performed
- Personnel doses are stored for legal reporting (background radiation is subtracted automatically)
- Ability to measure in pulsed field environments

Compare and Contrast: Christian vs. Christianist on Nukes

Source: http://www.patheos.com/blogs/markshea/2018/01/compare-contrast-christian-vs-christianist-nukes.html

Jan 11 – Here is the Christian position, articulated by Rome, which called the use of weapons of mass destruction a "crime against man and God, meriting firm and unequivocal condemnation" (Gaudium et Spes). Pope Francis sez:

Addressing the international symposium on Nov. 10, Pope Francis did not just condemn the threat of using nuclear weapons. He categorically declared their very possession is immoral.

"They cannot constitute the basis for peaceful coexistence between members of the human family, which must rather be inspired by an ethics of solidarity," Pope Francis said.

Their very possession.

All this is, of course repugnant to Christianists, who think fondling nuclear weapons is awesome and who loved Trump's threat the other week to use them. They are fully on board with the Trump administration's plans to loosen constraints on the use of such weapons, as well as to proliferate more such weapons for their god king to play with in his tiny hands.

Because Christianism is a diabolical cult of death at war with the gospel. That is why it constantly seeks to do the exact opposite of the teaching of the Church–and to call that teaching and this pope "fake Christians" and so forth.

This isn't even hard. This is Moses vs. the Golden Calf stuff. Jesus or Barabbas stuff. And still the Greatest Catholics of All Time consistently make the visible-from-space wrong call and name Trump a stable genius and Francis the "heretic pope".

World War in 2018? Trump and Kim Jong Un Increase Fears Dramatically, New Report Finds

Source: http://www.newsweek.com/nuclear-war-kim-trump-2018-783407

Jan 17 – Fears over wars this year on the Korean Peninsula, the Middle East and around the world have increased dramatically due to President Donald Trump's ongoing nuclear feud with North Korea's Kim Jong Un, as well as threats of extreme weather events, natural disasters and cyber attacks, according to the World Economic Forum.

Seventy-nine percent of the experts tasked saw an increased risk in military conflicts in 2018, while 93 percent expected political and economic rows to ratchet up.

The WEF's annual Global Risks Report was released less than a week before Trump heads to the international organization's global meeting in Davos, Switzerland. Trump is expected to deliver a speech on the final day. The meeting runs from January 23 to 26.

Trump's "Make America Great Again" slogan and brand of politics were cited as reasons for the fear of conflicts involving political and economic power. The risk report mentioned his decision to pull the United States out of the Trans-Pacific Partnership trade deal and the Paris climate accord, as well as threats to yank the Iran nuclear deal put in place by his predecessor.

Trump and Kim have continued to trade insults and barbs across various forms of media. The president has repeatedly nicknamed Kim "little rocket man" while threatening "fire and fury" if the North kept testing intercontinental ballistic missiles and nuclear weapons.

In kind, Kim has called Trump a "dotard" who is actually pushing for war on the peninsula, while he tested missiles and detonated Pyongyang's sixth nuclear test in its history last year.

An example of the widening fears of a U.S. military or nuclear conflict with the North was put on full display over the weekend. Hawaii residents were mistakenly sent a warning of an incoming missile to their phones and televisions, setting off a panic throughout the islands.

The report also indicated economic inequality as an ongoing problem that should be addressed now before "systems breakdown."

"A widening economic recovery presents us with an opportunity that we cannot afford to squander, to tackle the fractures that we have allowed to weaken the world's institutions, societies and environment," WEF founder and executive chairman Klaus Schwab said. "We must take seriously the risk of a global systems breakdown."

The report breaks concerns down into five categories: economic, environmental, geopolitical, societal and technological. And powerful weather events and natural disasters were viewed as the most likely to occur this year, while weapons of mass destruction were ranked highest in terms of potential impact to the globe.

The survey taps the opinions of 1,000 experts from the worlds of businesses, government and non-governmental organizations on 30 global risks over a 10-year period.

What's the Difference Between a Dirty Bomb and a Nuclear Bomb?

By Katherine Scott

Source: https://www.thermofisher.com/blog/identifying-threats/2018/01/16/whats-the-difference-between-a-dirty-bomb-and-a-nuclear-bomb/

Jan 16 – The United States Nuclear Regulatory Commission (USNRC) defines a dirty bomb as one type of a radiological dispersal device (RDD) that combines conventional explosives, such as dynamite, with radioactive material. According to the USNRC, a dirty bomb is in no way similar to a nuclear weapon or nuclear bomb. The fact sheet explains:

> *A nuclear bomb creates an explosion that is millions of times more powerful than that of a dirty*

bomb. The cloud of radiation from a nuclear bomb could spread tens to hundreds of square miles, whereas a dirty bomb's radiation could be dispersed within a few blocks or miles of the explosion. A dirty bomb is not a "Weapon of Mass Destruction" but a "Weapon of Mass Disruption," where contamination and anxiety are the terrorists' major objectives.

Usually, dirty bombs don't release enough radiation to kill people or cause severe illness. That doesn't mean that dirty bombs don't do damage, though. The impact of the explosion itself can do lots of damage to humans and buildings. But the actual 'dirty' part of the bomb is the radioactive particles that are scattered as a result of the explosion.

After a dirty bomb goes off, radiation is spread across a city where it gets into building intakes, drops in people's yards, in parks, on the street, into your car's air intakes, etc. All that needs to be fully cleaned. That means a lot of clean up that could take months/years and substantial sums of money.

Depending on the amount and type of radioactive material used, and which way the wind is blowing, their reach can be extensive. So besides the actual injuries that could be suffered by passersby, and the damage an explosion does to buildings, the radioactive material that spreads can cause, long term health effects from exposure to the radiation.

Ionizing radiation, according to *Popular Science*, "does one main thing to the human body: it weakens and breaks up DNA, either damaging cells enough to kill them or causing them to mutate in ways that may eventually lead to cancer."

I explained in a *PoliceOne.com article* that "Terrorists may use an incident to create public panic. The highly toxic nature of radioactive materials and their threat to life make them frightening. Even if injuries are minimal in the initial explosion, the radioactive material that citizens inhale or ingest can cause a lasting risk to health, increasing the potential of disease. Tests monitoring the impact of small RDDs show the immediate spread of toxic materials may be minimal. If radioactive particles enter an HVAC system, however, and then flow through the air ducts in a building, the risk to human health greatly increases."

Finding radioactive materials before a bomb goes off is the best way to protect the public. Handheld Radiation Isotope Identifiers (RIIDs) or small, belt worn identifiers (SPRDs) are used to search for materials that could make a dirty bomb; it's critical to know the exact isotope of the radioactive material in order to assess the potential threat and quickly initiate a plan of action. Simply knowing you have radiation is not good enough. Nuisance alarms from people with recent nuclear medical treatments, building materials, and even bananas cause users to investigate alarms, taking them away from other, more common, security threats.

The instrument operator can now view the results of an alarm on screen, at the scene, without having to call for a secondary screening tool, allowing immediate implementation of the proper operational step to contain the source or ignore it.

Large detectors that are contained in a vehicle or backpack allow small numbers of officers to quickly see abnormal radiation levels in a large area, or from a distance. Small, personal radiation detectors, worn covertly by all personnel, provide radiation detection in the immediate area around the wearer, are inexpensive, and provide a "network" of sensors to detect hidden sources. They can quickly pinpoint the location of radioactive sources easily, allowing officers to respond to the exact location of a threat.

What Makes A Dirty Bomb Dirty?

Source: https://www.thermofisher.com/blog/identifying-threats/2017/12/21/what-makes-a-dirty-bomb-dirty/

December 2017 – The actual 'dirty' part of a dirty bomb is the radioactive particles that are scattered as a result of the explosion. The United States Nuclear Regulatory Commission (USNRC) defines a dirty bomb as one type of a radiological dispersal device (RDD) that combines conventional explosives, such as dynamite, with radioactive material.

In a dirty bomb, the ionizing radiation would come from radioactive isotopes (also called radioisotopes). The website "How Stuff Works" explains that "Radioactive isotopes are simply atoms that decay over time. In other words, the arrangement of protons, neutrons and electrons that make up the atom gradually changes, forming different atoms. This radioactive decay releases a lot of energy in the form of ionizing radiation…. A dirty bomb would boost the radiation level above normal levels, increasing the risk of cancer and radiation sickness to some degree. Most likely, it wouldn't kill many people right away, but it could possibly kill people years down the road. "

Where does someone obtain radioactive material to add into an explosive? Nuclear plants, both in the US and abroad, are of course a possibility.

However, radioactive materials are used extensively in the medical field. There are diagnostic and therapeutic procedures that utilize nuclear medicine. The Centers for Disease Control and Prevention reports that diseases treated with nuclear medicine procedures are hyperthyroidism, thyroid cancer, lymphomas, and bone pain from some types of cancer. So hospitals, doctor's offices, and cancer treatment centers could be a source – as well as manufacturing plants that build the equipment used by the medical industry and pharmaceutical companies that make the medicine.

In addition, food, water, and other beverages are irradiated by processing plants to ensure products are safe for consumption. Construction crews utilize portable density gauges and non-invasive inspection tools daily with strong radioactive sources to verify structural integrity of buildings, roads, and bridges, with several documented cases of gauges being lost or stolen. Scrap yards and metal recycling facilities may inadvertently have large, orphaned radiation sources in its pile of scrap metal, typically from long ago closed factories and warehouses.

This YouTube video shows a map of the United States and the industries and locations where radiation threats can originate.

Fortunately, there is radiation detection and measurement technology for routine monitoring and surveillance to help mitigate the threat and keep you safe. Radiation detection solutions provide comprehensive, real-time monitoring, early warning, and complete information so you can identify and protect against radiation threats. Handheld Radiation Isotope Identifiers (RIIDs) are often used in searching for materials that could make a dirty bomb.

However, those devices are relatively large and require dedicated personnel to deploy and monitor. Now there are compact, pager-sized portable radiation detection and identification instruments to detect, locate, and identify radioactive nuclides such as nuclear weapons, dirty bombs, and orphaned or purposely masked sources, that are as small as your mobile phone, and can passively monitor from your belt, pocket or vest allowing you to monitor for radiation while still focusing on your primary, overarching, security mission. In addition, these small devices cost fractions of what a RIID costs, allowing large deployments to find that "needle in the haystack" more effectively.

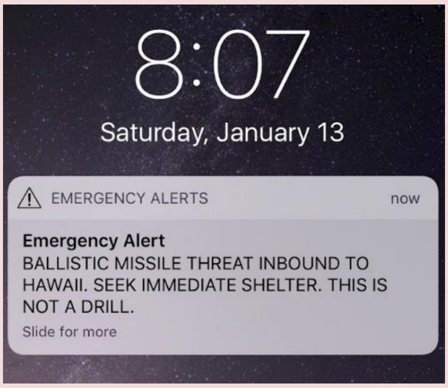
The hope is finding a dirty bomb before you have to clean up after it.

Responding to the Nuclear Threat – Then & Now

By *Keith Grossman* Wed, January 17, 2018

Jan 17 – In the civil defense era of emergency management, the federal, state, and local civil defense authorities were presented with the mission to protect the civilian population from an attack on the U.S. mainland. Shelter programs, coordinated public warning systems, emergency assistance provisions, and other protective measures were developed. Today, these measures need to be revisited and adapted in accord with current threats, timing, and resources.

The Office of Civil Defense and Mobilization was created by President John F. Kennedy via Executive Order 10952 in September 1961. This executive order established the creation of the Community Fallout Shelter Program, developed a coordinated public warning system, employed the provision of emergency assistance to state and local governments, and empowered the Secretary of Defense to plan for the continuity of government. It is important to put this in the context in which this executive order was enacted. These programs and initiatives occurred during the Cold War, in the atomic age, with a growing nuclear threat from Russia, and growing concerns from U.S. citizens over the effects of a first strike.



Emergency Alert
BALLISTIC MISSILE THREAT INBOUND TO HAWAII. SEEK IMMEDIATE SHELTER. THIS IS NOT A DRILL.

The United States is now faced with a renewed conversation about a nuclear threat, causing Hawaii to activate and perform a monthly test of their State Attack Warning Tone for the first time since the Cold War. The most recent routine test of the system created a widely publicized false alarm that occurred at 8:07 am on 13 January 2018 (see Fig. 1). This false alarm highlighted a flaw in Hawaii's warning system in which a singular person could initiate activation. Hawaii is now moving to a two-person activation method in the aftermath of this event. Given the time lapse since the Community Fallout Shelter Program was established in 1961, many fallout shelters have since been closed, this poses the question of what would happen should this alarm have been real.

Historical Review

In order to fully understand the current situation, it is important to understand the origins of civil defense. President Franklin Delano Roosevelt established the Office of Civilian Defense (OCD) in 1941 to plan for a community-based response to protect civilians in the event of a military attack on U.S. soil. The OCD was an independent agency that coordinated with the Chemical Corps of the U.S. Army and the U.S. Public Health Service. When it was created, this office looked at the many hazards with which a community would be presented after a land attack.

At the end of World War II, the office was disbanded due to the decreased threat. This changed over the course of the next decade as the world entered the atomic age following the bombing of Hiroshima and Nagasaki in Japan and Russia detonating its first atomic weapon. As atomic threat became reality, the OCD went through several iterations throughout the years, most notably as the Federal Civil Defense Administration under President Harry S. Truman in 1951 and the Office of Civil Defense and Mobilization beginning in September 1961.

With the creation of the Community Fallout Shelter Program, thousands of shelters were built across the United States, especially in urban centers. The program focused on creating infrastructure and capacity along with a stringent training and exercise program. For many, the memory of a fallout shelter and "Duck and Cover" drills during elementary school remain. Throughout the decade-long tenure of this program, countless home and public shelters were built throughout the country, creating a sense of security and a belief that people could easily survive nuclear fallout in their geographic areas.

A significant amount of research was also performed on the human condition during an extended stay in a shelter with only Department of Defense rations, chemical communal toilet canisters, poor ventilation, and overcrowding. It was found that a lack of sleep, the chemical commode, and a lack of bathing facilities caused major discomfort, as well as headaches and nausea. Additional psychological issues included the ability to adjust to hygiene and decontamination rituals, to adapt to the change in living conditions, and to adapt to the uncertainty that lay outside. The response to these issues was training and the creation of motivational in-shelter programs that would enable people to emerge from the shelter in an emotionally stable condition. To a great degree, the activities may not have been realistic but designed to stabilize and support the anxiety and concerns exhibited by the populace.

For example, the OCD created a guidance document, entitled Fallout Protection. This training aid was used to guide families and communities in their preparedness and planning for a nuclear attack. It instructed families to stay in their fallout shelters for at least 14 days, and come out in increasing intervals beginning at no more than four hours per day. The Fallout Protection guide not only gave information regarding the effects of a nuclear blast and the subsequent fallout, but also gave instruction on supplies needed for survival. Additionally, this era led to the build out of multiple sites for continuity of government including: Orange One, which is the president's bunker at Camp David; and Site R (Raven Rock Mountain Complex), which is the emergency operations center for the U.S. military.

In 1969, Congress began defunding the Community Fallout Shelter Program and, by 1972, merged the Office of Civil Defense and Mobilization into the Defense Civil Preparedness Agency. Since many of the public shelters were reliant on federal funding to maintain their functionality, the lack of funds diminished the feasibility of the shelters. In 1979, President James "Jimmy" Carter issued Executive Order 12148, which dismantled the Defense Civil Preparedness Agency and transferred all of its responsibilities to the Federal Emergency Management Agency. Since that time, the national response has moved away from a nuclear focus, and toward the all hazards approach currently used as the industry standard.

Changes & Current Standards

The primary change has been related to timing. In the 1960s, a nuclear device was delivered by plane, with an advanced warning potentially of up to 40 hours. In the age of the intercontinental ballistic missile (ICBM), notice is significantly shorter, usually less than one hour of lead-time. This is not enough time to report to an assigned community fallout shelter. As such, the focus has shifted to surviving the blast and staying indoors in the most central part of the nearest building when the blast occurs.

In addition to the launch of an ICBM, threat of a dirty bomb release exists and can happen with virtually no warning. In the case of a dirty bomb, the actual blast would likely not be the most deadly part of the attack. The fallout created by the release could create long-lasting health and safety issues in the region where the attack occurred.

Although there is a marked change in the timing of a release, the fallout risk remains the same in the aftermath of the event. In present day Hawaii, emergency planners have re-tooled some of the Civil Defense Era planning and response methods. As previously mentioned, the state of Hawaii has resumed testing of the state attack warning tone. It has also reissued a Guidance Summary for Coordinated Public Messaging on Response to a Nuclear Detonation. This document gives similar advice as its predecessor, the Fallout Protection pamphlet issued in 1961. It advises people to get inside immediately, stay away from windows, stay low to the ground, stay inside for up to 14 days, and venture outside only to find essential supplies. The major difference between these two guiding documents is simply the lack of need for or use of fallout shelters.

As New York City continues the process of taking down the iconic fallout shelter signs from the New York City Public Schools, some may walk by these signs daily without even knowing they are there. Others may be conscious of their presence given their connection to a time gone by. New York City has adopted the response planning guidance set by Lawrence Livermore National Laboratory in 2009 for the aftermath of nuclear terrorism. Any concerned or informed citizen can go to the Plan Now NYC website and find guidance on what to do after a radiological attack. Much like Hawaii, New York City will provide emergency messaging primarily advising the public to cover their noses and mouths to avoid inhalation injury and find shelter inside the house.

What This Means Today

For present-day emergency managers, much can be learned from the principles of the Civil Defense era. The Civil Defense Program taught that it is the responsibility of all levels of government to plan and prepare citizens to respond to an emergency. This program established the precedent that the federal government should and will support a locality after an emergency declaration similar to the Robert T. Stafford Disaster Relief and Assistance Act. It taught that, "An acceptable program, must be one that is understood by those directly involved in it," and that hazards must be mitigated to the extent possible to moderate the potential for a massive recovery effort.

In its final days, the Civil Defense Program demonstrated that developing planning efforts and training for specific hazards is highly effective and should be applied to all hazards, paving the way for current planning practices. It is vital that emergency managers continue to plan for all hazards. However, with old threats returning anew, it is important to prepare for a perceived and or imminent threat and focus training to reduce it. The Civil Defense Program highlighted that "the best defense is often a good offense," as seen in the current Hawaiian education campaign.

Although the most recent false alarm created genuine concerns and issues, the importance of these tests cannot be overstated. Despite the false alarm in Hawaii, the need for and value in regulated and recognized monthly testing should not be ignored. These tests familiarize the citizens of Hawaii with the sound of air raid sirens, making the sound recognizable and providing citizens opportunities to practice recommended actions. The tests familiarize the Hawaii Emergency Management Agency with the notification procedures and highlight areas for improvement. Most importantly, practicing these scenarios will reduce panic, to some degree, at the time of an actual event.

The response to a nuclear event has not changed much over the past 70 years. However, when seeking shelter, one cannot go back to the fallout shelters of yesterday. Instead, they must seek shelter, as quickly as possible, in the closest possible building, or even in the confines of their own homes.

Keith Grossman, *MPA, is the director of emergency management for the New York City Department of Education (DOE). In this role, he is responsible for the system-wide emergency planning for the largest school system in the United States consisting of over 1,800 schools in over 1,300 locations. His team is responsible for shaping the role of the DOE in the city-wide response framework, serving as the 24/7point of contact for the NYC's emergency services, serving as the logistics chief for the Emergency Sheltering System, and conformity of emergency programs with the American's with Disabilities Act. Prior to working at the DOE, Keith served as the Director of Emergency Management Safety at Brookdale Hospital in Brooklyn, the Planning Section Chief at Brookhaven National Laboratory and the Emergency Management Coordinator at Nassau University Medical Center. Keith holds a Bachelor of Arts from Binghamton University, a Graduate Certification in Emergency Management from Adelphi University and a Master of Public Administration from Alfred University.*

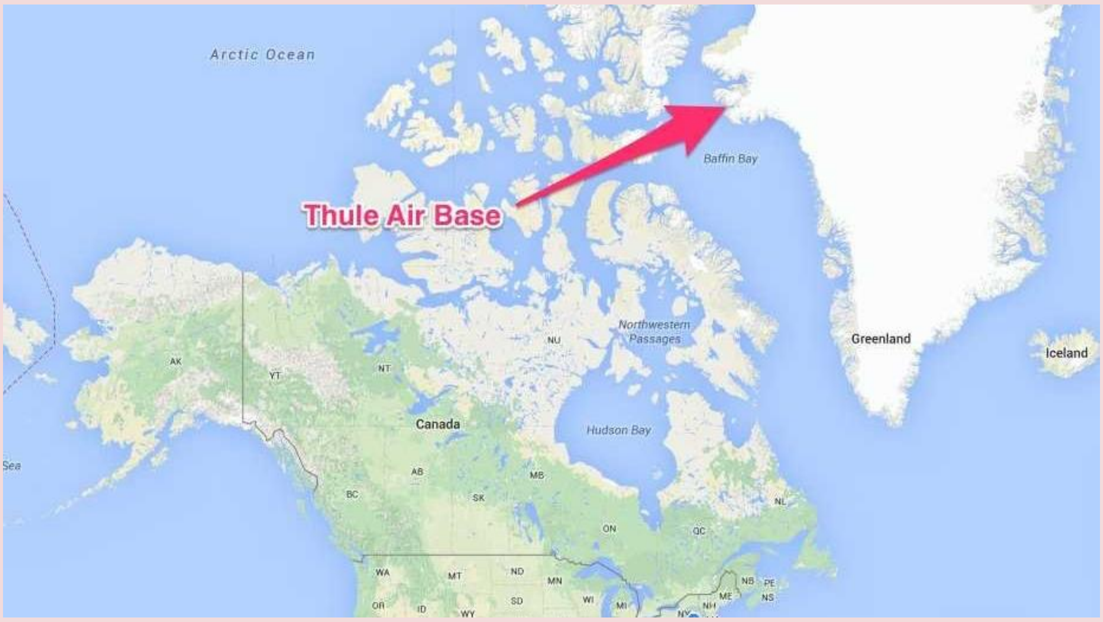
50 Years Ago, a US Military Jet Crashed in Greenland—with 4 Nuclear Bombs on Board

By Timothy J. Jorgensen

Source: https://www.scientificamerican.com/article/50-years-ago-a-us-military-jet-crashed-in-greenland-mdash-with-4-nuclear-bombs-on-board/

The gunner (center), SSgt Calvin Snapp, is rescued after ejecting onto the ice. *Credit: Project Crested Ice Wikimedia*

The following essay is reprinted with permission from The Conversation, an online publication covering the latest research.



Jan 20 – Fifty years ago, on Jan. 21, 1968, the Cold War grew significantly colder. It was on this day that an American B-52G Stratofortress bomber, carrying four nuclear bombs, crashed onto the sea ice of Wolstenholme Fjord in the northwest corner of Greenland, one of the coldest places on Earth. Greenland is part of the Kingdom of Denmark, and the Danes were not pleased.

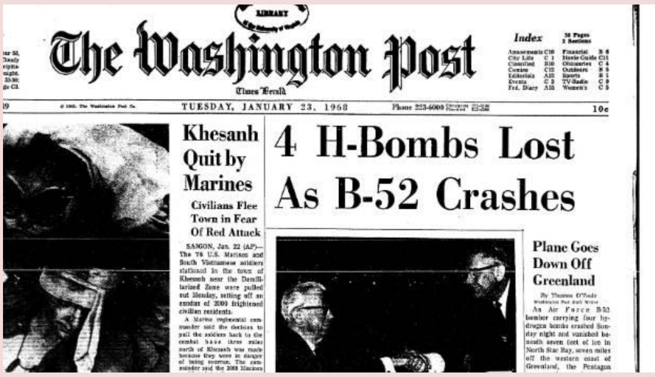
The bomber—call sign HOBO 28—had crashed due to human error. One of the crew members had stuffed some seat cushions in front of a heating vent, and they subsequently caught fire. The smoke quickly became so thick that the crew needed to eject. Six of the 7 crew members parachuted out safely before the plane crashed onto the frozen fjord 7 miles west of Thule Air Base—America's most northern military base, 700 miles north of the Arctic Circle.

The island of Greenland, situated about halfway between Washington D.C. and Moscow, has strategic importance to the American military—so much so that the United States had, in 1946, made an unsuccessful bid to buy it from Denmark. Nevertheless, Denmark, a strong ally of the United States, did allow the American military to operate an air base at Thule.

The crash severely strained the United States' relationship with Denmark, since Denmark's 1957 nuclear-free zone policy had prohibited the presence of any nuclear weapons in Denmark or its territories. The Thule crash revealed that the United States had actually been routinely flying planes carrying nuclear bombs over Greenland, and one of those illicit flights had now resulted in the radioactive contamination of a fjord.

The radioactivity was released because the nuclear warheads had been compromised. The impact from the crash and the subsequent fire had broken open the weapons and released their radioactive contents, but luckily, there was no nuclear detonation.

To be specific, HOBO 28's nuclear weapons were actually hydrogen bombs. As I explain in my book, "Strange Glow: The Story of Radiation," a hydrogen bomb (or H-bomb) is a second-generation type of nuclear weapon that is much more powerful than the two atomic bombs dropped on Hiroshima and Nagasaki. Those two bombs were "fission" bombs—bombs that get their energy from the splitting (fission) of very large atoms (such as uranium and plutonium) into smaller atoms.



The Washington Post
Times Herald

Index — 36 Pages, 3 Sections

Amusements	C10	Financial	B6
City Life	C1	Movie Guide	C11
Classified	B10	Obituaries	C4
Comics	C12	Outdoors	B5
Editorials	A12	Sports	B1
Events	C3	TV-Radio	C9
Fed. Diary	A13	Women's	C5

TUESDAY, JANUARY 23, 1968 — 10c

Khesanh Quit by Marines

Civilians Flee Town in Fear Of Red Attack

SAIGON, Jan. 22 (AP)—The 75 U.S. Marines and South Vietnamese soldiers stationed in the town of Khesanh near the Demilitarized Zone were pulled out Monday, setting off an exodus of 2000 frightened civilian residents.

A Marine regimental commander said the decision to pull the soldiers back to the combat base three miles north of Khesanh was made because they were in danger of being overrun. The commander said the 2000 Marines

4 H-Bombs Lost As B-52 Crashes

Plane Goes Down Off Greenland

By Thomas O'Toole
Washington Post Staff Writer

An Air Force B-52 bomber carrying four hydrogen bombs crashed Sunday night and vanished beneath seven feet of ice in North Star Bay, seven miles off the western coast of Greenland, the Pentagon

In contrast, HOBO 28's bombs were fusion bombs—bombs that get their energy from the union (fusion) of the very small nuclei of hydrogen atoms. Each of the four Mark 28 F1 hydrogen bombs that HOBO 28 carried were nearly 100 times more powerful than the bomb dropped on Hiroshima (1,400 kilotons versus 15 kilotons).

Fusion bombs release so much more energy than fission bombs that it's hard to comprehend. For example, if a fission bomb like Hiroshima's were dropped on the Capitol building in Washington, D.C., it's likely that the White House (about 1.5 miles away) would suffer little direct damage. In contrast, if just one of the Mark 28 F1 hydrogen bombs were dropped on the Capitol building, it would destroy the White House as well as everything else in Washington, D.C. (a destructive radius of about 7.5 miles). It is for this reason that North Korea's recent claim of achieving hydrogen bomb capabilities is so very worrisome.

After the crash, the United States and Denmark had very different ideas about how to deal with HOBO 28's wreckage and radioactivity. The U.S. wanted to just let the bomber wreckage sink into the fjord and remain there, but Denmark wouldn't allow that. Denmark wanted all the wreckage gathered up immediately and moved, along with all of the radioactively contaminated ice, to the United States. Since the fate of the Thule Air Base hung in the balance, the U.S. agreed to Denmark's demands.

The clock was ticking on the cleanup, code named operation "Crested Ice," because, as winter turned into spring, the fjord would begin to melt and any remaining debris would sink 800 feet to the seafloor. Initial weather conditions were horrible, with temperatures as low as minus 75 degrees Fahrenheit, and wind speeds as high as 80 miles per hour. In addition, there was little sunlight, because the sun was not due to rise again over the Arctic horizon until mid-February.

Groups of American airmen, walking 50 abreast, swept the frozen fjord looking for all the pieces of wreckage—some as large as plane wings and some as small as flashlight batteries. Patches of ice with radioactive contamination were identified with Geiger counters and other types of radiation survey meters. All wreckage pieces were picked up, and ice showing any contamination was loaded into sealed tanks. Most every piece of the plane was accounted for except, most notably, a secondary stage cylinder of uranium and lithium deuteride – the nuclear fuel components of one of the bombs. It was not found on the ice and a sweep of the seafloor with a minisub also found nothing. Its current location remains a mystery.

Although the loss of the fuel cylinder was perplexing and disturbing, it is a relatively small item (about the size and shape of a beer keg) and it emits very little radioactivity detectable by radiation survey meters, making it very hard to find at the bottom of a fjord. Fortunately, it is not possible for this secondary "fusion" unit to detonate on its own without first being induced through detonation of the primary "fission" unit (plutonium). So there is no chance of a spontaneous nuclear explosion occurring in the fjord in the future, no matter how long it remains there.

The successful cleanup helped to heal United States-Denmark relations. But nearly 30 years later, the Thule incident spawned a new political controversy in Denmark. In 1995, a Danish review of internal government documents revealed that Danish Prime Minister H.C. Hansen had actually given the United States tacit approval to fly nuclear weapons into Thule. Thus, the Danish government had to share some complicity in the Thule incident.

As recently as 2003, environmental scientists from Denmark revisited the fjord to see if they could detect any residual radioactivity from the crash. Was bottom sediment, seawater or seaweed radioactive, after nearly 40 years? Yes, but the levels were extremely low.

Thule Air Base survived all of the controversies over the decades but became increasingly neglected as nuclear weaponry moved away from bomber-based weapon delivery and more toward land-based and submarine-based intercontinental ballistic missiles. Nevertheless, as Thule’s bomber role waned, its importance for radar detection of incoming ICBMs grew, since a trans-Artic trajectory is a direct route for Russian nuclear missiles targeted at the United States.

In 2017, Thule got a US$40,000,000 upgrade for its radar systems due, in part, to increased concern about Russia as a nuclear threat, and also because of worries about recent Russian military forays into the Arctic. Thule Air Base thus remains indispensable to American defense, and the United States remains very interested in Greenland—and committed to maintaining good relations with Denmark.

***Timothy J. Jorgensen** is Director of the Health Physics and Radiation Protection Graduate Program and Associate Professor of Radiation Medicine, Georgetown University.*

Hawaii’s missile alert gaffe: why good human-machine design is critical

By Siraj Ahmed Shaikh

Source: http://www.homelandsecuritynewswire.com/dr20180119-hawaii-s-missile-alert-gaffe-why-good-humanmachine-design-is-critical

Jan 19 – A ballistic missile warning alarm that was wrongly triggered in Hawaii recently rams home the importance of the way interfaces are designed to prevent such major bloopers from happening in the first place.

It’s an unfortunate reality that we need to prepare for national emergencies due to war or natural disasters. Civil defense organizations, set up to coordinate and respond to such emergencies, are an important part of any modern state. Such entities – often a mix of state apparatus and voluntary organizations – play a critical role in terms of triggering alerts, coordinating response across law enforcement and emergency services, disseminating information and aiding response efforts to minimize impact and restore order.

Clearly, they are important systems for alerting nations to risks when disaster strikes. But such systems can go wrong.

In Hawaii on 13 January an employee of the U.S. state’s Emergency Management Agency set off a false alarm that seemed only too real to anyone seeing the stark warning of a “Ballistic Missile Threat Inbound to Hawaii.” It was sent to social media channels and mobile phones, followed by the chilling message: “Seek Immediate Shelter. This is not a drill.” The false alarm continued for 38 minutes and caused widespread panic.

Human error was reportedly behind the false alarm, after an employee chose the incorrect option from a drop-down menu. The options of an actual alarm and a drill were provided in the same menu. One offered to trigger a “DRILL – PACOM (CDW) STATE ONLY,” while the other very similar sounding option was described as “PACOM (CDW) STATE ONLY.”

Triggering the alarm also brought up a confirmation dialogue box – the only prompt that could have prevented the errant message from being sent. The operator clicked on it to confirm that he did want to send out the alert and, in the panic that ensued, Hawaiians thought they only had minutes to live before a ballistic missile attack.

Design for error

Poor interface design clearly fails to address human errors. Human-Computer Interaction (HCI) systems, examples of which are found ranging from aircraft cockpit design to interactive medical devices, have been studied extensively.

The underlying science tries to address optimal interaction between human and machine, in an effort to minimize gaffes such as the Hawaiian incident. A couple of design principles serve as pertinent reminders on this occasion.

Human error is to be expected – it's not the case of if but when. Every step of the way mechanisms should be built in to prevent mistakes. Strong audiovisual cues could be used to make a notable distinction between genuine alerts and drills. Different menu styles could also be provided where alerting sequences could be different to drill sequences. Simplicity of design should, however, trump all design elements to avoid complexity which in turn can also be problematic for the person behind the controls.

Two-person rule

Beyond the interface design, operational protocols could also be devised requiring two people to issue an alert. This prevents one person making a false choice, inadvertently or deliberately, and ensures that the probability of an error is significantly reduced. However, this may introduce an unnecessary delay or an added cost burden in case of genuine alerts where both operators need to be present at all times.

While years of research into HCI and safety-critical systems have served us well, be it aviation safety or healthcare and patient safety, the possibility of human error remains. The unfortunate mistake that led to the Air France AF447 accident in 2009, in which the pilot doggedly pulled on the control stick in a fatal climb even though the aircraft was repeatedly warning it had stalled, is a reminder that accidents do still happen despite advances in design. A cockpit scenario albeit has a radically different context to an early warning alert system.

Our interaction with technology is becoming more and more complex. Early warning systems are very welcome but the Hawaii mishap serves as an opportunity for a radical redesign, with a better understanding of their impact on the population: how do people respond to mass panic? How do we communicate alerts to reduce panic and promote orderly movement? It is also an opportunity for scientists to reexamine the social dynamics in an emergency situation.

At a time when the world is increasingly uncertain and our dependence on technology is so high, a redesign of poor warning systems is critical.

__Siraj Ahmed Shaikh__ is Professor of Systems Security, Coventry University.

Explosive News

A Brave Bomb-Disposal Robot You Control in Virtual Reality

Source: https://www.wired.com/story/a-brave-bomb-disposal-robot-you-control-in-virtual-reality/

Sept 2017 – A robot probably isn't coming for your job. But there are plenty of dull, dirty, and dangerous gigs out there that humanity wouldn't mind turning over to the machines. Indeed, **a robot called Taurus** from SRI International has already begun its takeover of one of the most dangerous jobs on Earth: bomb disposal.

Sure, bomb disposal robots have been rolling the earth for some time. But now SRI has taken its already brilliant bot and made it ... brillianter, by outfitting Taurus with virtual reality. Before, Taurus' operators watched a 3-D monitor to see the world through the robot's eyes, then manipulated controls that translated their movements into the movement of the robot's hands and graspers. Now by strapping on a VR headset, the user can use Oculus Touch controllers as manipulators.

It's about as close as you can get to assuming the body of a machine. And adding to the immersion is the haptic feedback SRI can also load into the robot. "If you need to actually feel either the static forces that it's pushing on, on a wall or the world, we can do that," says Mark Baybutt, associate R&D director in the SRI Robotics Group. Especially useful for feeling around a suspicious device without blowing up your robotic proxy.

Now, look through the headset and you won't just see the world through Taurus' eyes. You'll see a heads-up display of sorts, with virtual buttons you can tap with the Oculus Touch motion controls to lock the robot's arms, for instance. "Not only does it make you feel more immersed and connected with the remote world that you're operating," says Baybutt, "but it also offers very unique and interesting human machine interfaces that we can actually create with different buttons or information presented to the user."

Get ready for more of this sort of thing. As ever more sophisticated robots creep into our lives, we'll need ever more sophisticated ways of interfacing with them. You're already used to an operating system on your phone or PC, sure, but humans will have to develop interfaces for the virtual world that will connect us to machines like Taurus.

Not that you personally will be disposing of bombs anytime soon. And not that Taurus is only good for disposing bombs—send it into a mine if you don't want to go yourself. If it's dangerous and it needs doing, chances are that in the near future a robot will be putting its life on the line for a human with a machine strapped to their face.

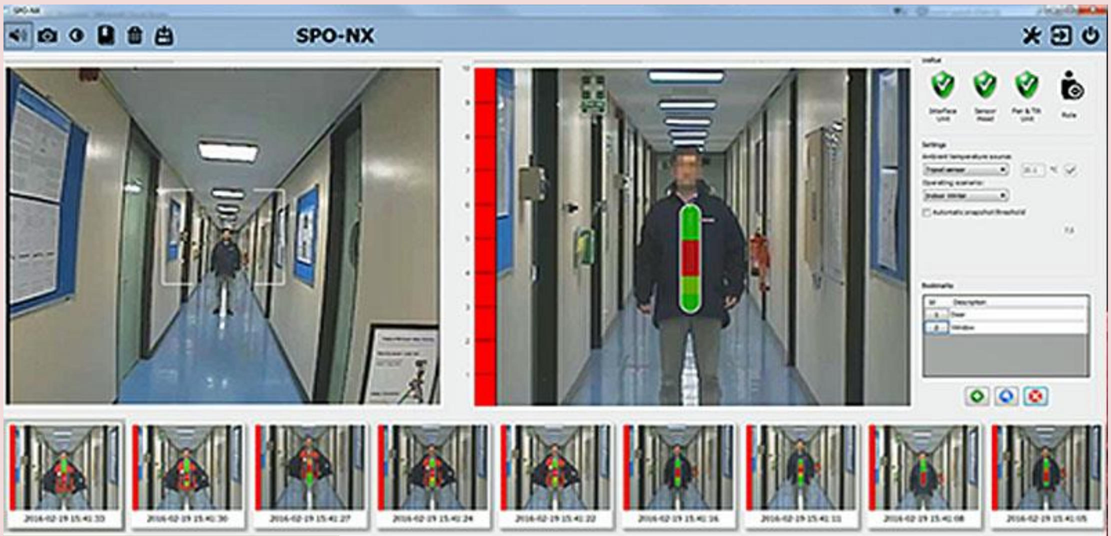
▶▶ **Watch the video at source's URL.**

New Tech to Detect Terrorist Suiciders in Metro Stations

Source (+video): https://i-hls.com/archives/80358

Dec 20 – A new security screening technique currently being tested in the US is designed to scan large crowds and spot hidden explosives and suicide vests. The TSA hopes that the new technology would lead to better detection be it at a train station or an airport.

The technology uses cameras to scan people entering the transit system for dense items concealed under their clothing, according to cbsnews.com. The scanners are designed to operate in the background, passively scanning people walking by in real time without using radiation.



"We're really looking for those alarm indicators. And so as that bar turns from green to red, we know we've identified an individual that may need a little closer scrutiny," said Alex Wiggins, head of security for Los Angeles' transit authority. "If we can encounter that person as they enter the station in the mezzanine, we can very, very quickly isolate them and move to an area where if there is a threat we can contain that much better."

The **SPO-NX equipment** can sense certain emissions made by the human body — and tell when those emissions are blocked by something such as a bomb vest or other contraband worn around the body under the clothes, according to manufacturer QinetiQ. The system can scan large crowds and flag potential risks so security workers can then screen them individually.

The TSA technology is currently being tested at Los Angeles' busy 7th Street metro station where four of the region's commuter lines connect. More than 86,000 people pass through there each weekday. One scanner is currently being tested at a TSA facility outside Washington, D.C. TSA said more testing will be needed.

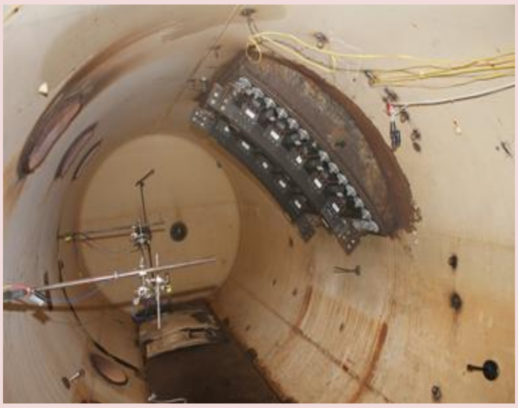
The hope is eventually it can scan people as they pass by without them noticing they are being screened.

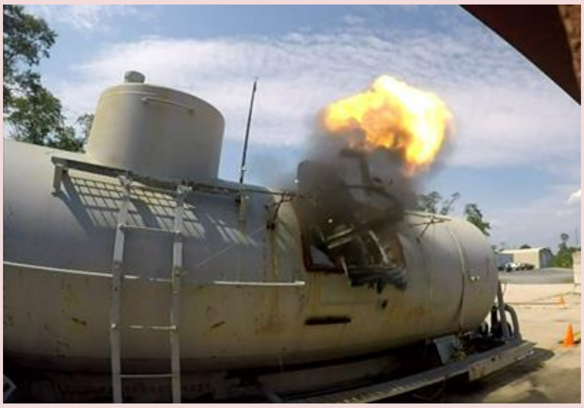
New simulator tool allows testing the explosive vulnerabilities of aircraft

Source: http://www.homelandsecuritynewswire.com/dr20171222-new-simulator-tool-allows-testing-the-explosive-vulnerabilities-of-aircraft

Dec 22 – Each day, more than twenty-six thousand commercial flights transport passengers and cargo to destinations around the world. Several U.S. government agencies work together to secure these flights, including the Department of Homeland Security (DHS) Science and Technology Directorate (S&T). S&T's Commercial Aircraft Vulnerability and Mitigation (CAVM) program, part of the Homeland Security Advanced Research Projects Agency Explosives Division, supports testing and evaluation efforts to assess potential vulnerabilities and evaluate countermeasures that can mitigate the impact of explosives on commercial aircraft. Recently, CAVM partnered with the Federal Aviation Administration (FAA) and U.S. Army Aberdeen Test Center (ATC) to develop a reusable Aircraft Explosive Testing Simulator that facilitates the explosive testing of new generation commercial aircraft.

S&T notesthat the majority of current commercial aircraft have aluminum fuselages, and CAVM has conducted a significant amount of explosive vulnerability testing on a wide range of those aircraft types. However, newer generations of commercial aircraft fuselages are being made with composite materials, such as carbon fiber reinforced plastic. Understanding the potential vulnerability of composite aircraft to explosives requires testing, but the new generation composite aircraft fuselages are less available and more expensive than legacy aluminum fuselage structures. This made it essential to develop a sustainable and representative testing solution so evaluations of new composite aircraft structures to explosive-based threats could continue as needed.





"The lack of availability of new generation composite commercial aircraft structures for use in destructive explosive testing necessitated development of alternate test methods and tools," said Nelson Carey, CAVM Program Manager. "Doing so is essential to provide S&T and its U.S. government customers with accurate and efficient methods for conducting commercial aircraft explosive vulnerability assessments."

Based on this need, ATC developed the Aircraft Explosive Testing Simulator that could be used for repeated explosive testing. The simulator consists of a steel cylinder that can be pressurized to simulate conditions of an in-flight aircraft. The cylinder has an opening where composite test panels are installed and subjected to testing for a variety of explosive threat scenarios. The composite aircraft test panels are provided through an interagency agreement with the FAA and the National Institute for Aviation Research, an FAA Center of Excellence.

"Interagency cooperation in support of CAVM efforts is essential for extending limited resources and insuring a maximum rate of return on research and development investment," Carey said.

During a test, evaluators place an explosive threat inside the simulator, which is then pressurized to simulate airline operational flight profiles. Once the explosive is detonated, instrumentation gathers data on internal and external pressure resulting from the blast, and high speed video instruments gather information on the panel's physical condition, looking for any deformation, breach, or crack growth. Aircraft vulnerability experts from S&T's Transportation Security Laboratorythen conduct a post-blast inspection and analysis to determine the structural response of the composite test panel to the specific explosive threat condition. Finally, evaluators remove the panel from the simulator and install a new one in its place, allowing for multiple tests to be conducted within a short time period.

"The Aircraft Explosive Testing Simulator provides a rapid, reconfigurable and cost effective tool for acquiring test data on composite aircraft structural response to internal explosive threats," Carey explains, highlighting the impact the tool has on testing efforts.

Not only does the Aircraft Explosive Testing Simulator help S&T develop a better understanding of how explosives affect composite commercial aircraft, it also allows experts to compare results with previous tests on aluminum structures. CAVM researchers will use the data to learn about composite-based commercial aircraft structure vulnerability to terrorist-based internal explosive threats. This research supports the Transportation Security Administration's sponsor requirements to investigate the vulnerability of new generation composite construction commercial aircraft to internal explosive threats.

S&T is already sharing its findings from the simulator with other government partners. The Department of Defense's (DoD) U.S. Army Research Laboratoryis using the data to develop numerical analysis models and tools to help simulate composite structure response for different and more complex threat scenarios. Additionally, CAVM recently hosted a round of tests with TSA, FAA, DoD, TSL, and the French government's Alternative Energies and Atomic Energy Commission (CEA). The event was part of an international effort to strengthen aviation security by bringing together officials from around to globe to share findings and discuss shared goals.

S&T says that the Aircraft Explosive Testing Simulator is the latest S&T-funded technology that will help enhance the nation's aviation security. As threats continue to evolve, it is crucial to have tools that can efficiently gather accurate data on potential vulnerabilities and the countermeasures employed to overcome them.

Explosion at major oil pipeline in Libya

Source: https://www.rt.com/news/414265-libya-oil-pipeline-explosion/

Dec 22 – An explosion has rocked a crude oil pipeline that feeds the Es Sider sea terminal in Libya, an oil source in the country said.

The Mediterranean port of Es Sider, also spelled as Sidr and Sidra, features the largest oil depot in Libya. The blast occurred near Marada, on the pipeline belonging to the Waha oil company, the source told Reuters.

Unverified photos of what is said to be a plume of black smoke coming from the site of the pipeline explosion are being shared on social media.

A military source told RIA Novosti that the *"large"* explosion at the pipeline was the result of a terrorist attack, carried out with the use of *"an improvised explosive device."* The Libyan armed forces heard the blast from a distance of 20 kilometers and headed in that direction, while the militants retreated, the source added. *"The fighters belonged to either (al-Qaeda-affiliated) Benghazi Defense Brigades or Islamic*

State (IS, formerly ISIS/ISIL) as they are terrorists who carry out diversions to cripple oil production facilities."

The news of the Libyan blast saw oil prices spike to above $65 a barrel on Tuesday, trading close to its highest mark since mid-2015. Another factor contributing to the increase in price are the voluntary supply cuts by OPEC. Brent crude, the international benchmark for oil prices, went up 10 cents to $65.35 a barrel, while US crude added 12 cents at $58.59, Reuters reported.

The port of Es Sider changed hands on several occasions during the Libyan civil war, which started in 2011. It was severely damaged by the fighting, and remained closed between 2014 and 2016. This March Es Sider, which was shipping around 447,000 barrels per day when the conflict started, was recaptured by forces loyal to Libya's eastern-based military commander, Khalifa Haftar, and resumed operations.

When a North Korean Missile Accidentally Hit a North Korean City

By Ankit Panda and Dave Schmerler

Source: https://thediplomat.com/2018/01/when-a-north-korean-missile-accidentally-hit-a-north-korean-city/

Jan 03 – What happens when a North Korean ballistic missile test fails in flight and explodes in a populated area? On April 28, 2017, North Korea launched a single Hwasong-12/KN17 intermediate-range ballistic missile (IRBM) from Pukchang Airfield in South Pyongan Province (the Korean People's Army's Air and Anti-Air Force Unit 447 in Ryongak-dong, Sunchon City, to be more precise). That missile failed shortly after launch and crashed in the Chongsin-dong, in North Korean city of Tokchon, causing considerable damage to a complex of industrial or agricultural buildings.

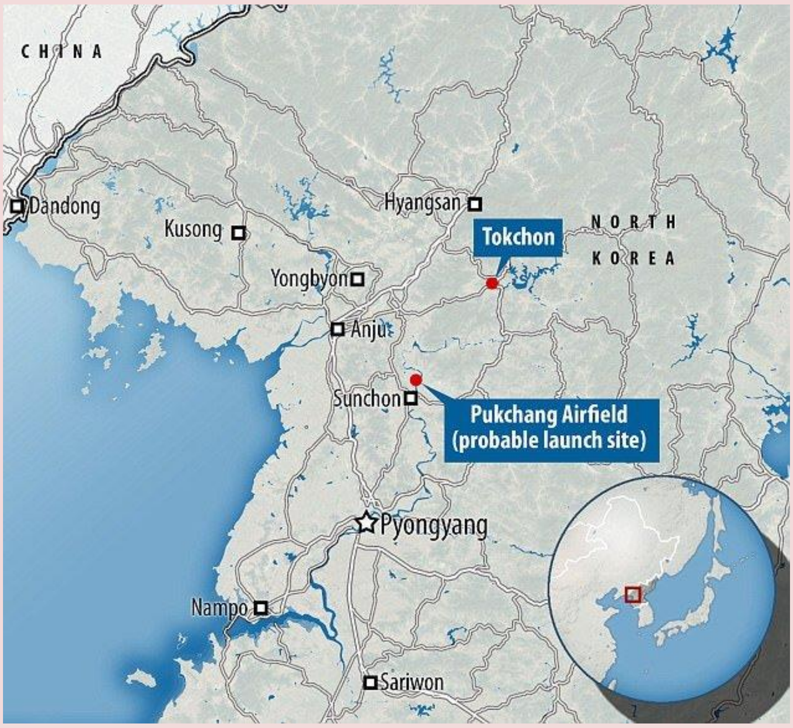
According to a U.S. government source with knowledge of North Korea's weapons programs who spoke to *The Diplomat*, the missile's first stage engines failed after approximately one minute of powered flight, resulting in catastrophic failure. The missile never flew higher than approximately 70 kilometers. The location of the missile's eventual impact was revealed exclusively to *The Diplomat* and evidence of the incident can be independently corroborated in commercially available satellite imagery from April and May 2017.

The April 28 failure merits close analysis, especially as North Korea continues to carry out flight-testing of its various ballistic missile platforms from a range of new test sites. In 2017, North Korea has introduced new sites for missile testing, arguably to demonstrate the flexibility of its Strategic Rocket Force. It has even carried out ballistic missile launches from a restricted area at Pyongyang's Sunan Airport, which also serves as the country's primary civil aviation facility and the entrypoint for most non-Chinese foreign visitors to North Korea. The potential for similar accidents occurring over Pyongyang, the country's capital, or other populated regions remains high, especially with untested systems.

These risks may even serve to explain why North Korea chose to use the seaside town of Sinpo as its initial test site for the first two failed Hwasong-12 launches in April. An early in-flight failure over the sea would have a lower chance of striking any human infrastructure — certainly populated urban areas. However, since April, North Korea has not carried out any further ballistic missile testing from Sinpo (with the exception of four submarine-launched ballistic missile ejection tests).

Anatomy of a Failed Hwasong-12 Launch

In April, most reports of the circumstances of this launch were sparse, noting only that North Korea launched a single missile that failed in flight. U.S. Pacific Command stated that the missile was launched from “near” Pukchang Airfield, a previously unused launch site for North Korean ballistic missile testing. As *The Diplomat* first reported in June, contrary to other reports at the time, the three missiles tested in April were not anti-ship ballistic missiles, but a new type of intermediate-range ballistic missile.



The April 28 test, in fact, was the third attempted flight-test of this new missile. The Hwasong-12, it would later emerge, was the fundamental building block for the Hwasong-14/KN20 intercontinental-range ballistic missile (ICBM) revealed later in the year. Despite the three failures in April, the Hwasong-12 would see its first successful flight-test just weeks later on May 14. (The Hwasong-12 and -14 family of missiles emerged from the so-called “March 18 revolution” engine, which was first tested on that day in 2017; the single thrust-chamber engine is used to power the first stage of both missiles.)

Later in the year, the North Korean regime provided more evidence regarding these April launches. At a concert held in July to celebrate the country’s first-ever successful test launch of the Hwasong-14 ICBM, North Korea showed an extensive slideshow detailing a history of the country’s ballistic missile program, with imagery dating back to Kim Il-sung — current North Korean Supreme Leader Kim Jong-un’s grandfather and the founder of North Korea — inspecting early Scud short-range ballistic missiles (SRBMs). (Those images have been cropped from the concert video and archived here.)

Toward the end of the slideshow, which was mostly shown in chronological order, the North Koreans helpfully included photographic evidence of Kim Jong-un inspecting all three of the failed April Hwasong-12 launches, including the April 28 launch out of Pukchang Airfield. These photographs are composed in a manner similar to the images North Korea publicly releases through its state media after successful launches; had the launches succeeded, it is likely that we would have seen these images in *Rodong Sinmun* immediately afterward.

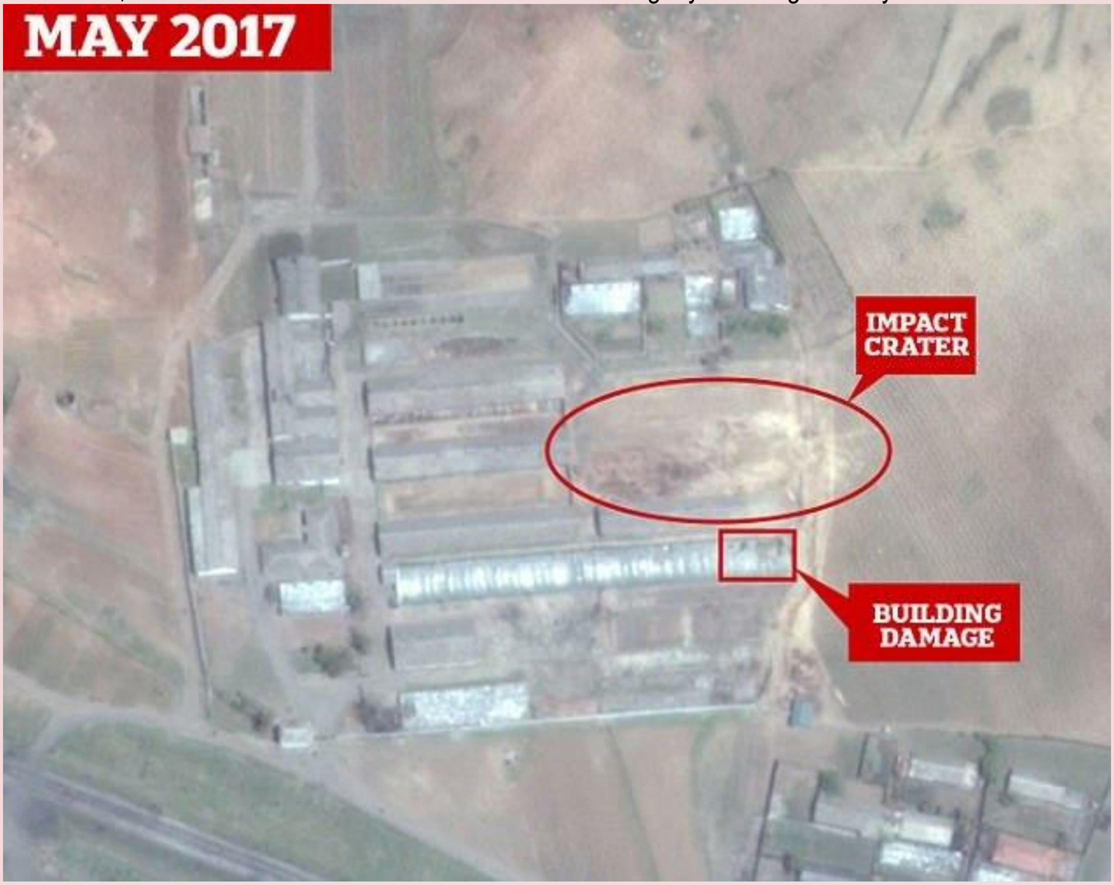
From an area near the Pukchang Airfield, the missile flew approximately 39 km to the northeast where it struck a complex in the small city of Tokchon seen below. Had it completed its flight successfully, the missile may have been designed to land in the northern reaches of the Sea of Japan, near the Russian coast. North Korea used a similar splashdown location for its first successful Hwasong-12 flight-test in May 2017. (The launch, however, took place from Kusong, not Pukchang.)

An image from Google earth of the complex show ground disturbances in an area that previously contained a building with fencing, also showing that a portion of the seasonal greenhouse had been damaged near the side of the complex where the debris fell. Using Planet Labs’ high frequency satellite images of this site, we can narrow down the date which this change occurred, which was sometime between the 26th and the 29th, or the two day window in which the test is known to have occurred.

Liquid-fuel missiles like the Hwasong-12, which use a highly volatile combination of hypergolic propellant and oxidizer (meaning that the two agents ignite spontaneously on contact), can produce massive explosions depending on how they fail. In this case, with the missile having survived its descent following an engine failure, it is likely that this facility at Tokchon experienced a large explosion upon impact. It’s impossible to verify if the incident caused any loss of life and, given the time of day the test occurred and the location of the impact, it may be likely that few, if any, casualties resulted from the incident.

However, as the Google Earth imagery of the incident demonstrates, the Tokchon facility is located adjacent to what appear to be residential and commercial buildings. A slight difference in trajectory may could have resulted in an even more catastrophic accident over a populated region.

To be sure, this North Korean incident is far from the first tragedy involving rocketry near a civilian area.



In February 1996, a Chinese Long March CZ-3B satellite launch vehicle failed shortly after launch from the Xichang Satellite Launch Center in Sichuan. Raw video footage of the incident conveys the immense damage resulting from the explosion, which took place near a populated area. The Chinese government never released a full accounting of the loss of life resulting from the accident and public estimates vary.

Even beyond the human and economic damage potentially caused by such a failed launch, North Korea, since August 2017, has started launching ballistic missiles over Japanese territory. It has done so twice with the Hwasong-12, succeeding both times, with the reentry vehicles splashing down in the northern Pacific Ocean, clear of Japanese territory. But future successes are not guaranteed and should a future North Korean missile overflying fail at the wrong moment during its powered flight phases, its trajectory may come to resemble an attack on Japan. Even with a dummy payload, an incident like that could spark a serious crisis in Northeast Asia. North Korea's missile tests, which violate its obligations under United Nations Security Council resolutions, come with no formal warning or notices to airmen, leaving regional states and the United States to their own devices in interpreting Pyongyang's intentions once the engines are ignited.

Implications for the United States and Allies

Aside from the safety implications of North Korean launch practices, the few images associated with this test offer insight into the country's pre-launch storage practices, with implications for U.S. and allied attempts at potential preemption and prevention. As seen in image 1, had the launch succeeded, *Rodong Sinmun* would likely have printed an image of Kim Jong-un standing in front of the transporter-erector-mounted IRBM in a hardened tunnel.

That would have (and now does) send a dire message to U.S. and allied military planners: North Korea's missiles won't be sitting ducks at known "launch pads," contrary to much mainstream analysis. What's more, the proliferation of newly constructed hangers, tunnels, and storage sites cannot be assumed to stop at the Pukchang Airfield. Similar facilities likely exist across the country. In 2017, not only has North Korea tested a massive variety of strategic weaponry, but it has done so from a more diverse list of launch sites — what the U.S. intelligence community calls "ballistic missile operating areas" — than ever before. Gone are the days of Kim Jong-un supervising and observing launches at a limited list of sites that'd include Sinpo, Sohae, Wonsan, and Kittaeryong.

It is true that missiles like the Hwasong-12, Hwasong-14, and even the new behemoth, the Hwasong-15, all use liquid fuels and must be fueled prior to launch. (North Korea's Pukguksong-2 medium-range ballistic missile uses solid propellants and does not have this limitation.) Even with this fueling requirement, U.S. and allied intelligence would have at best a couple hours to detect launch preparations. Finally, though riskier, North Korea could fuel these missiles in a horizontal configuration within their hardened storage sites and use its road-mobile transporter-erector-launchers to launch them with fewer pre-launch signatures.

As North Korea's production of now-proven IRBMs and ICBMs continues, it will have a large and diversified nuclear force spread across multiple hardened sites, leaving the preventive warfighter's task close to impossible if the objective is a comprehensive, disarming first strike leaving Pyongyang without retaliatory options. The time is long gone to turn the clock back on North Korea's ballistic missile program and its pre-launch basing options.

Ankit Panda *is a senior editor at* The Diplomat.
Dave Schmerler *is a research associate at the James Martin Center for Nonproliferation Studies at the Middlebury Institute of International Studies at Monterey*.
The authors are grateful to ***Jeffrey Lewis*** *for imagery assistance and* ***Curtis Melvin*** *for geographical assistance and facility identification.*

Teenage Suicide Bomber Kills Father in Mosque Attack

Source: https://clarionproject.org/teenage-suicide-bomber-kills-father-in-mosque-attack/

Jan 04 – **A teenage suicide bomber in Nigeria blew himself up in a mosque, killing his father among others who were praying at the time.**

Reports of the death toll varied between five and 11 people in the explosion which the bomber set off during the 5 am service.

The attack occurred in Gamboru, a town in the Borno state in northeastern Nigeria located on the border with Cameroon.

It was not immediately known to which group the teenage attacker identified, but the attack had all the markings of the terror group Boko Haram, which is known for targeting crowded mosques and market places and using children to carry out their deeds.

Boko Haram (which literally means "secular education is forbidden") opposes all groups – including Muslims – that do not adhere to their extreme beliefs.

Boko Haram is also believed to be behind the recent disappearance of 30 loggers in the same area. Local sources feared the loggers – mostly men in their 20s –had been kidnapped after they left Gamboru early Tuesday morning, January 2, to gather firewood and failed to return.

Last month, 30 soldiers disappeared after a raid on a military base in the same region, known to be a Boko Haram stronghold.

EOD Airman receives Purple Heart

Source: https://www.dvidshub.net/news/261432/eod-airman-receives-purple-heart

Jan 05 – After 10 years, Tech. Sgt. Douglas Smits, 90th Civil Engineer Squadron explosive ordnance disposal team leader, received a Purple Heart medal at F.E. Warren Air Force Base, Wyo., Jan. 5, 2018.

The Purple Heart medal is one of the military's oldest medals dating back to 1782. It recognizes military members who were wounded or killed in combat.

In 2007, then Senior Airman Smits went on a six-month deployment to Afghanistan in support of Operation Achilles, one of NATO's largest ground operations at the time.

“I was deployed out of Kandahar, and we were going into the Ghorak Valley to root out the Taliban, but as we were driving to one of our rally points, we hit an improvised explosive device,” Smits said.

Upon hitting the anti-tank mine, which contained more than 30 pounds of explosives, the 51,00-pound vehicle was blown up, and resulted in Smits suffering a traumatic brain injury.

“It was like riding lightning, and it sent a shockwave through my body,” Smits said. “My ears were ringing, and I remember looking up and seeing pieces flying off of the vehicle and black smoke covering the crater. Although I was in significant pain, I did not request medical evacuation as I felt I could still function to contribute to our mission and continue with field treatments of injuries to other members of the team.”

Senior Master Sgt. Alejandro Rodriguez, 509th Civil Engineer Squadron EOD flight chief, who was the team leader at the time; said they had to be tough and resourceful. The team was isolated for five days until recovery assets were sent.

“We strapped our equipment onto a stretcher and carried it throughout the battlefield from scene to scene clearing other detonation sites,” Rodriguez said. “We never quit, and we never hesitated. We were facing bitter cold conditions; I'm talking about bone-chilling, teeth-rattling cold. It was just one more obstacle that was working against us and testing our resolve.”

Smits reflected on the challenges of adjusting back to normal life after the deployment.

“The hardest part for me was coming back from an experience where you almost get addicted to the adrenaline, and then you don’t have that anymore when you come back to your home base,” Smits said. “The experience of almost getting blown up, or helping people who have, just becomes the norm while deployed.”

Smits is still making strides to overcome some of the mental obstacles associated with the explosion.

“I initially felt like it was a weakness to admit having post-traumatic stress disorder, but now I wish I would’ve gotten help sooner in my career,” Smits said. “There’s nothing wrong with seeking help after a deployment, and when a person close to you notices that you’re not being yourself, never be ashamed to go talk to someone.”

Smits continues to serve in the EOD career field, and his efforts from 2007 are not forgotten.

“The team proudly represented the best of what this country and the Air Force has to offer,” said Rodriguez. “I would describe Doug as a battle-proven man of grit, and I am extremely proud to have served with him.”

During the ceremony, Col. Stacy Jo Huser, 90th Missile Wing commander, acknowledged Smits’ composure and courage under fire.

“I want to personally thank you for your extensive preparation and your willingness to go beyond the call of duty,” Huser said. “Your example inspires the rest of us to serve with distinction and go the extra mile, not only in combat, but in our training and day-to-day duties as well.”

Enlisting drones to detect unexploded landmines through changes in plant health

Source: http://www.homelandsecuritynewswire.com/dr20180111-enlisting-drones-to-detect-unexploded-landmines-through-changes-in-plant-health

Jan 11 – From U.S. Navy laboratories to battlefields in Afghanistan, researchers are lining up to explore the use of unmanned aerial vehicles to detect unexploded landmines. At Missouri University of Science and Technology, civil engineeringdoctoral student Paul Manley is enlisting a third variable —plant health — to see whether drones can be used to more safely locate such weapons of destruction.

MST says that Manley's Ph.D. research leverages his master's thesis work in biology atVirginia Commonwealth Universitywith the resources of Missouri S&T. In his case, that notably includes the MinerFlysupport team, which helps researchers such as Manley and thesis adviser Dr. Joel Burken with UAV construction, flight tests and navigating Federal Aviation Administration regulations.

"At VCU, Paul's experiments on plant responses to explosives were at the leaf level and in the lab," says Burken, Curators' Distinguished Professor and chair of civil, architectural and environmental engineering. "Now his research can be applied at the field level with the use of UAVs."

The hyperspectral camera Manley favors is no ordinary point-and-shoot. Rather, the device's higher spectral resolution allows for image collection across hundreds of bands that can detect subtle changes in how plants such as corn and sorghum gain or lose water and nutrients, or how they biochemically respond to stress.

"As drought increases, so does the relative temperature around that area," says Manley. "So we can use thermal imaging to see how plants are responding to drought stress. When you add in those hundreds of bands, you can really 'see' how the plants are responding."

The research is funded in part through Missouri S&T's share of a five-year, $20 million National Science Foundation grant to nine institutions across the state that are teaming up to better understand climate variability and its potential agricultural, ecological and social impacts.

The consortium enables Manley to conduct test flights at locations such as the University of Missouri-Columbia's Bradford Research Center as well as the Southwest Research Centernear Mount Vernon, Missouri. Soil, terrain and crop types vary by location.

The project, "Missouri Transect: Climate, Plants and Community"received federal funding from the Experimental Program to Stimulate Cooperate Research (EPSCoR), with a goal of building research teams and expanding research capacity across the state.

Those same sensors are now being pointed toward the topic of detecting landmines and explosives. Existing landmine detection methods are far from ideal, Manley explains.

"Currently, you have people walking around the minefields, leading animals on leashes, tilling up the surface to just detonate the mines and get it over with, or they are using ground-penetrating radar to detect these in the subsurface," Manley says. Another innovative device —constructed from plastic, iron and bamboo, and powered by wind — would need to be replaced each time it detected any of the more than 100 million unexploded landmines across the world.

"These detection methods are really slow, and they're expensive, and they all involve people out in the minefields doing this work, so it's dangerous," he says.

Observing changes in plant health to determine the presence of unexploded landmines is not dissimilar from Manley's earlier work. Over time, he explains, the mine casings can degrade, causing changes in soil properties as compounds then leach into the subsurface.

Explosive ingredients such as TNT and RDX, also known as T4, are "taken up by plants readily," he says.

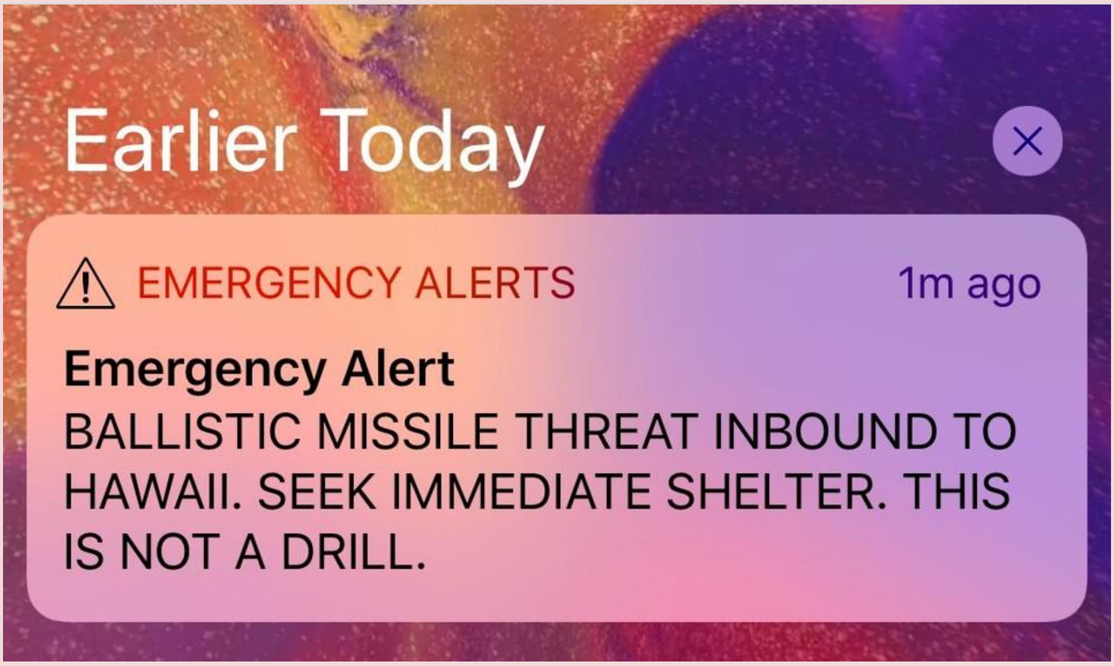
"RDX gets into groundwater, while TNT tends to stay in the roots. And RDX is readily taken into the leaves."

"By combing the knowledge of how plants and chemicals interact and the new technical capabilities to 'see' how plants behave from the sky, Manley aims to have a new approach to help disarm minefields around the globe — and change the world for the better," MST says.

Hawaii and the Horror of Human Error

Source: https://www.theatlantic.com/international/archive/2018/01/hawaii-alert-north-korea-icbm/550538/

Jan 15 – The Cold War came to an end, somehow, without any of the world's tens of thousands of nuclear warheads being fired. But there were decades-worth of close calls, high alerts, and simple mistakes that inched world leaders shockingly close to catastrophe.



Earlier Today

EMERGENCY ALERTS 1m ago

Emergency Alert
BALLISTIC MISSILE THREAT INBOUND TO HAWAII. SEEK IMMEDIATE SHELTER. THIS IS NOT A DRILL.

Saturday's terrifying, 38-minute episode in Hawaii will not go down as one of those close calls: Residents of the state waited for the bombs to fall after receiving text messages that a ballistic missile was on its way. FCC Chairman Ajit Pai on Sunday said "the government of Hawaii did not have reasonable safeguards or process controls in place to prevent the transmission of a false alert"—a case of human error, in other words.

It took 38 minutes for officials to correct a false alert that said a missile was heading for Hawaii. Instagram/@sighpoutshrug/via REUTERS

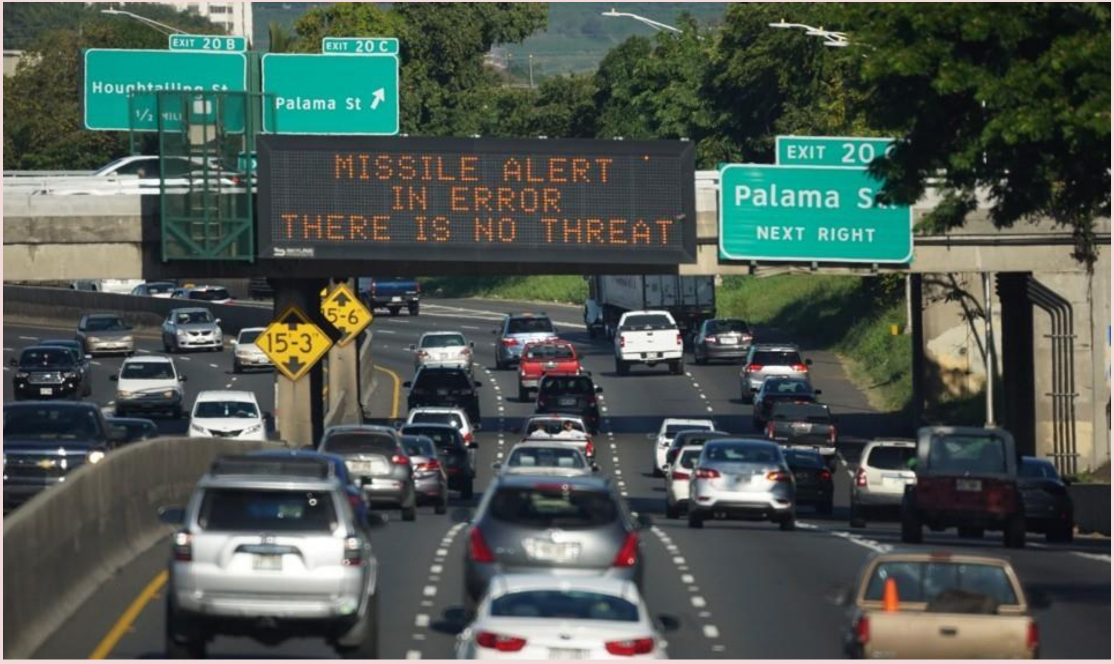
But the episode did reveal the glaring deficiencies of an early-warning system that can easily misfire, along with some frightening truths about the speed at which policymakers and presidents must make decisions in the event that missiles really do fly. "Mistakes have happened and they will continue to happen," the Arms Control Association's Daryl Kimball told me. "But there is no fail safe against errors in judgment by human beings or the systems that provide early warning."
As such, worries about miscalculation remain vivid. Vipin Narang, a political science professor at MIT focused on nuclear issues, tweeted one scenario on Saturday. "POTUS

sees alert on his phone about an incoming toward Hawaii, pulls out the biscuit, turns to his military aide with the football and issues a valid and authentic order to launch nuclear weapons at North Korea. Think it can't happen?"

The United States operates a series of radar and missile-defense systems across the Pacific. It includes satellites monitoring the Korean peninsula and fleets of American and Japanese warships equipped with the Aegis system, a powerful computing network that detects and tracks missile launches and aircraft. Those systems are tied to the U.S. Strategic Command's Global Operations Center, buried deep underground in Nebraska, which monitors events around the world in real time and pumps that information to the Pentagon and the White House.

In the Hawaii incident, there was little danger of the United States firing off a nuclear response. Military officials knew within minutes of receiving the alert that there was no threat to U.S. territory; none of the Pentagon and U.S. spy satellites or the ground and sea-based radars detected any sign of missile launches from North Korea, government officials told me.

But with a president obsessed with cable news and Twitter, the erroneous alert could have easily triggered an angry or provocative tweet, which could have been interpreted by the North Koreans or Russians as an imminent threat. According to pool reports, Trump was briefed on the false alarm while at his private golf course in Florida. Hours later, he tweeted about Hillary Clinton's "missing" emails and the performance of the stock market. He has yet to comment on the incident despite knowing within minutes that all was safe, even as horrified Hawaiians continued to expect the worst.



"There are fail safes built into the system, but there aren't enough fail safes," Kingston Reif, director of threat reduction policy at the Arms Control Association, said. "If the president wants to respond—and there's very little time to respond—the president and only the president has the sole authority or authorize the use of nuclear weapons," he added.

President Trump's apparent attempts to dictate national policy via tweet and his bombastic rhetoric about North Korean leader Kim Jung Un have seemingly raised the odds of a coming conflict. In August, Trump tweeted that "military solutions are now fully in place, locked and loaded, should North Korea act unwisely." His advisors consistently warn that time is running out to stop the North Korean nuclear and ballistic missile programs

While the United States has a series of sophisticated early warning systems, potential adversaries do not, making initial statements from American officials critical in tense situations. “We have to be concerned about our adversaries early warning systems and their interpretation of these signals and messages,” Kimball said.

Entering this complex array of political signaling, high-tech surveillance, and careless tweeting, is the Pentagon’s new Nuclear Posture Review, the first since 2010. Originally slated for release next month, a draft of the document leaked this past week shows the Trump administration is lowering the bar for what would trigger an American nuclear response. It includes an entire section about non-nuclear strategic attacks that could spur an American nuclear response: cyber warfare, massive blows to critical infrastructure, and certain catastrophic attacks on civilians.

That is a “major expansion over Clinton, Bush and Obama,” all of whom attempted to reduce the role of nuclear weapons, Jon Wolfsthal, a former Obama official who worked on nuclear issues, told me. The new strategy views nuclear weapons as “a swiss army knife that can be pulled out to solve a range is issues,” he added. Among several new weapons the document proposes are so-called “low-yield nukes,” which could be placed on existing Trident ballistic missiles launched from submarines, lowering the threshold for use by causing less fallout, limiting the impact zone, and causing fewer civilian casualties.

As one defense official involved in nuclear issues put it: “We are self-deterred because our nuclear weapons are too big, and would cause too much damage if used.” The new strategy paper, then, expands the types of scenarios under which the United States would choose the nuclear option, which in turn “could lead to a new round of testing of nuclear weapons,” the official said.

Another concern is the lack of nuclear expertise currently at the White House and at the Pentagon. Key positions in the Pentagon’s policy-making offices remain unfilled or are only now seeing officials take their desks after a year of vacancies. At the National Security Council, for example, Andrea Hall is currently serving as both director for Weapons of Mass Destruction on the National Security Council, and director for WMD, Terrorism and Threat Reduction, which were separate roles under previous administrations.

The new nuclear strategy, Wolfsthal said, indicates that under the Trump administration “there’s no downside to threatening the use of nuclear weapons.” Simply making the threat more explicit, and more likely to be acted upon, is seen as enough of a deterrent to sway potential adversaries. What the North Korean and Russian leadership think of these threats is something Washington will discover over time.

Japan government tells public broadcaster not to repeat false missile alert

Source: https://www.reuters.com/article/us-northkorea-missiles-japan/japan-government-tells-public-broadcaster-not-to-repeat-false-missile-alert-idUSKBN1F60FV

速報 01月16日 18時55分
北朝鮮ミサイル発射の模様　Jアラート　政府"建物の中や地下に避難を"(18:55)

Jan 17 – The Japanese government called on public broadcaster NHK on Wednesday to make sure a false alarm warning of a North Korean missile launch will not be repeated, with tensions still high because of the North’s missile and nuclear programs.

Japan's public broadcaster NHK's false alarm about a North Korean missile launch which was received on a smart phone is pictured in Tokyo, Japan January 16, 2018. REUTERS/Kim Kyung-Hoon

NHK issued an erroneous alarm on its website on Tuesday evening, saying North Korea appeared to have launched a missile and urging people to take shelter. A similar gaffe caused panic in the U.S. island state of Hawaii at the weekend.

Japan's public broadcaster put out another message on its website within five minutes correcting itself and said no government warning, known as a "J-alert", had been issued.

"The J-alert system is information of extreme importance in maintaining the security and safety of the people, so we've asked that they ensure this does not happen again," Chief Cabinet Secretary Yoshihide Suga told a regular news conference.

There have been no reports of panic or other disruptions following the NHK report.

NHK said the false alert was sent by mistake when it was trying to issue another news flash.

The broadcaster declined to say what the other news flash was about, but some domestic news outlets issued bulletins at around the same time about the latest recipients of a Japanese literary award.

NHK is looking into measures to prevent a recurrence but could not comment on specific details because the plan had not been firmed up yet, an NHK spokeswoman said.

The false alert was also sent to mobile phone users of NHK's online news distribution service. It was not clear how many of its 300,000 users have a function to let news alerts pop up on the cellphone screen when activated, NHK said.

Seizure of 'swimming bomb' highlights Greece's growing role in the fight against smuggling

Source: https://www.washingtonpost.com/news/worldviews/wp/2018/01/11/seizure-of-swimming-bomb-highlights-greeces-growing-role-in-the-fight-against-smuggling/

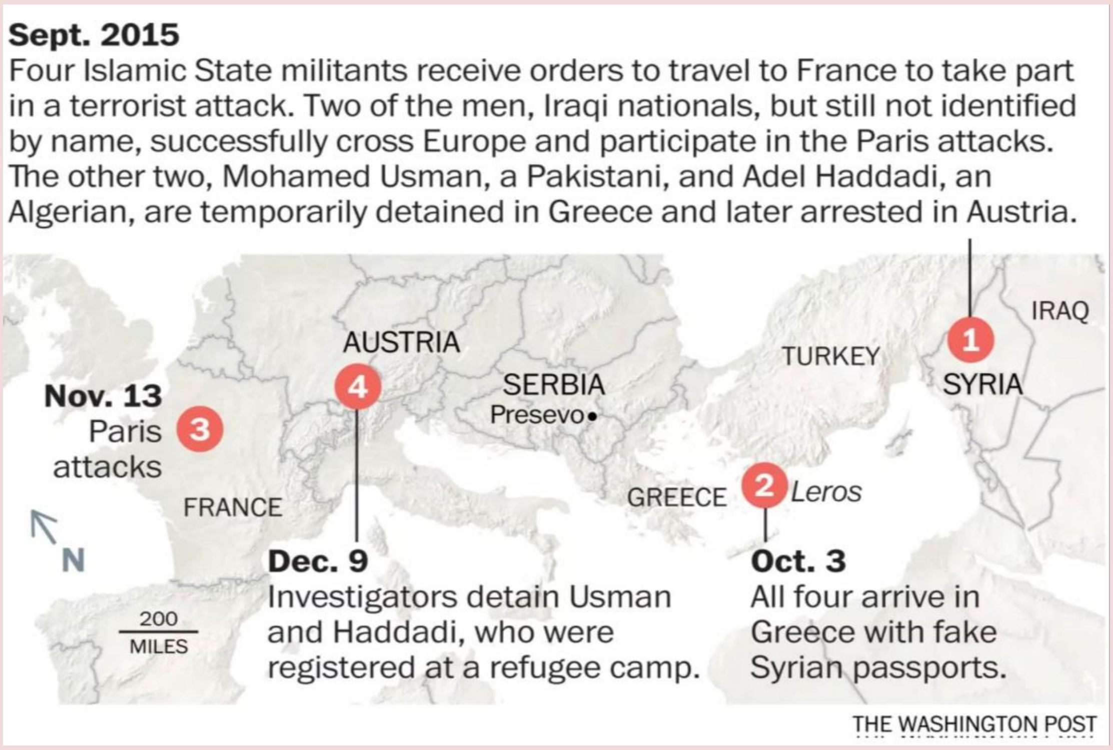
On Jan. 9, Greece officials intercepted a cargo ship en route to Libya that was found to be carrying 29 shipping containers of explosives and detonators. (Hellenic Coast Guard)

When Greek authorities boarded a ship on Jan. 6, they quickly noticed that something was wrong. The vessel, supposedly bound for the Arabian Peninsula, did not have any nautical maps of the destination area.

Then they took a closer look at the cargo and found 29 containers with over 400 tons of materials used to make explosives, as well as detonators and other equipment for blowing things up, authorities announced on Wednesday evening. A representative for the Greek Coast Guard, Giannis Sotiriou, described the discovery as a "swimming bomb" that appeared to be on its way to civil war-torn Libya.

"If something had gone wrong, the explosives would probably have destroyed the entire port," a senior Greek coast guard official said on Thursday. He spoke on the condition of anonymity because he was not authorized to publicly discuss the operation.

Two officials said that last week's operation and previous incidents highlight Greece's raised profile in policing the Mediterranean in recent months, as the country's coast guard has gradually moved from operating as an emergency task force rescuing refugees on their way to Europe to now playing an increasingly significant role in international security. Greece is spread over about 6,000 islands at a crucial naval intersection that connects the Middle East with Europe and North Africa — and has long been a major hub for drugs, arms and human trafficking. In the past, officials complained, the significance of the area to international security has too often been ignored.



Sept. 2015
Four Islamic State militants receive orders to travel to France to take part in a terrorist attack. Two of the men, Iraqi nationals, but still not identified by name, successfully cross Europe and participate in the Paris attacks. The other two, Mohamed Usman, a Pakistani, and Adel Haddadi, an Algerian, are temporarily detained in Greece and later arrested in Austria.

Oct. 3
All four arrive in Greece with fake Syrian passports.

Nov. 13
Paris attacks

Dec. 9
Investigators detain Usman and Haddadi, who were registered at a refugee camp.

THE WASHINGTON POST

"We are surrounded by a triangle of crisis and destabilization," said Greek Foreign Minister Nikos Kotzias in a 2015 Washington Post interview, referring to the conflicts in Ukraine, Syria, Iraq and Libya. Greece was also the first country many Syrians reached on their flight from Turkey to Europe during the mass refugee influx, which picked up momentum in 2015.

For months, Greek authorities — already stretched by years of austerity due to the country's ongoing debt crisis — were largely overwhelmed by the sudden influx of refugees. Initially, few of the hundreds of thousands newcomers underwent comprehensive identity checks; and two of them later went on to commit the devastating November 2015 terrorist attacks in Paris.

The incident also marked a turning point for Greek authorities.

At the time, a senior European intelligence official who spoke on the condition of anonymity to discuss classified information, told my colleagues Anthony Faiola and Souad Mekhennet: "The Greeks failed in protecting the borders into the E.U."

"And we all failed by not pushing hard enough to establish that security," he added.

Greek officials defended themselves, saying that they had pleaded for more European Union help but had their requests denied.

"Everyone knew we were facing huge financial problems. So for months we had to make do with what we had, hoping help would arrive," Zacharoula Tsirigoti, lieutenant general of the Greek police, told my colleagues in April 2016.

But in the months since, the United States and the European Union have stepped up their cooperation with Greece, potentially bolstering the country's critical security infrastructure, even though there may not be a direct link with the recent string of attacks in Europe.

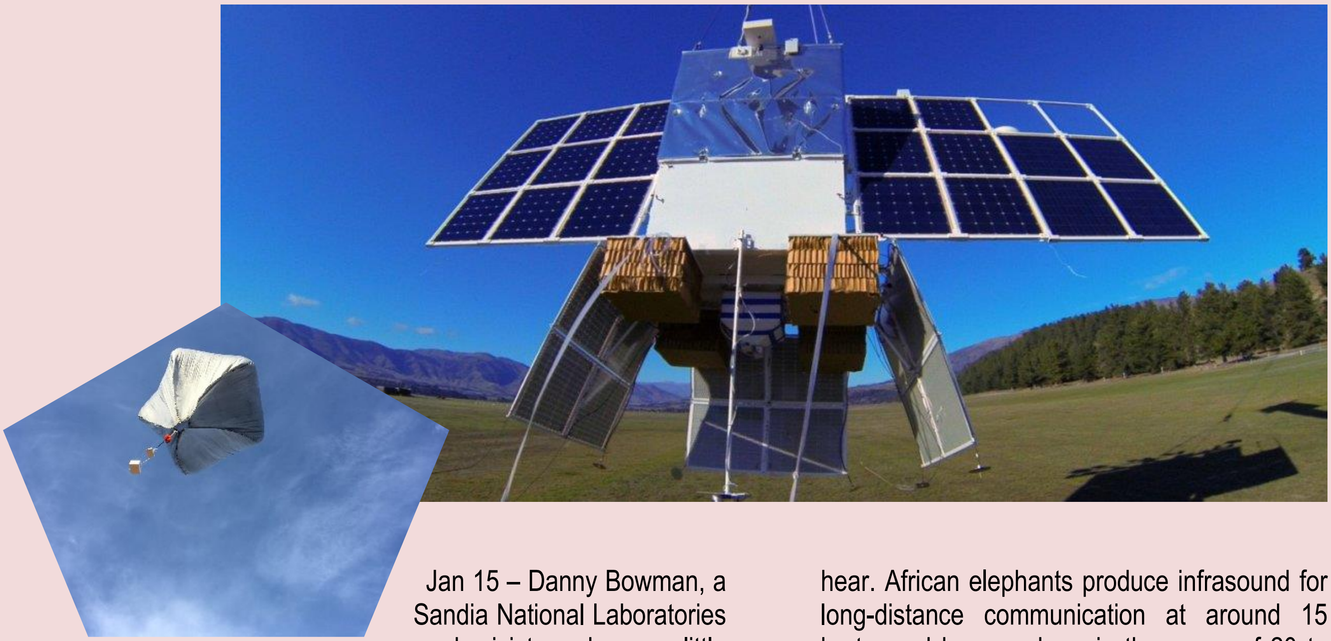
The United States, for instance, has expanded its training missions in the country, a Greek coast guard official said. The deepening of Greek-American security cooperation was first publicly discussed last summer and appears to have affected recent Greek operations, including several large-scale seizures of illicit drugs, and recent operations targeting arms and human trafficking, the official said.

He added that U.S. and European officials have also stepped up intelligence sharing with their Greek counterparts and the country's MYA counterterrorism unit in recent months. Illicitly trafficked goods were intercepted several times last year after European partners provided crucial hints. The official did not specify to what extent U.S. information had so far contributed to Greece's anti-smuggling and anti-terrorism efforts. Cooperation between Greece and the U.S. military has also boosted the Greek coast guard's capacity to respond to certain situations such as high-speed manhunts at nighttime, he said.

Greece's experience appears to match a broader cross-European trend. The European Union's police agency, Europol, announced last year that counterterrorism intelligence sharing within the European Union "had reached an all-time high."

New Hot-Air Balloon to Detect Explosion's Infrasound

Source: https://i-hls.com/archives/80810



Jan 15 – Danny Bowman, a Sandia National Laboratories geophysicist needs a very little number of everyday products in order to build a solar-powered hot air balloon for detecting infrasound.

Infrasound is sound of very low frequencies, below 20 hertz, which is lower than humans can hear. African elephants produce infrasound for long-distance communication at around 15 hertz, and humans hear in the range of 20 to 20,000 hertz.

On July 2017, a fleet of five solar-powered balloons reached a height of 21 to 24 kilometers, twice as high as commercial jets, and detected the infrasound from a test explosion.

Infrasound is important because it's one of the verification technologies the U.S. and the i nternational community use to monitor explosions, including those caused by nuclear tests. Traditionally, infrasound is detected by ground-based sensor arrays, which don't cover the open ocean and can be muddled by other noises, such as the wind. Bowman said air conditioners are also a common source of infrasound noise.

© Shutterstock / Mette Fairgrieve

"The stratosphere is much less noisy so you can detect events of interest to science and national security from greater distances," said Bowman. The stratosphere is the atmospheric layer from about 8 kilometers to 50 kilometers above the ground.

A solar-powered hot air balloon takes three hours for Bowman and fellow geophysicist Sarah Albert to make, and uses about $50 worth of materials, not including the reusable infrasound sensor or GPS tracker. The charcoal dust helps heat up the air inside the balloon, providing lift, without requiring helium gas, a nonrenewable resource.

The balloons can even be launched on partly cloudy days, said Albert. They stay up in the stratosphere all day and come down after the sun sets. This "guaranteed termination mechanism" is both a pro and con, said Bowman.

It's a fool-proof way to bring down the balloons, the sensors and the data they have collected. On the other hand, longer flights would be useful. During the Arctic summer, the balloons could fly for weeks, but the team also is working on balloons that can stay aloft at night.

For future experiments, Bowman is interested in a balloon design with an insulator on the top surface of the balloon and absorber on the bottom, so it absorbs heat from the Earth to allow it to keep flying at night.

The most important aspect of this experiment is that the five balloons formed a 3-D array of sensors, said Albert. One sensor can hear a sound, but cannot provide any location information. Albert said, "My mom is deaf in one ear so it's hard for her to tell where a sound is coming from." Having two ears allows animals to determine the source of a sound.

Five microphones in an array, as in this experiment or ground-based sensor arrays, provide the same information — the direction from which the sound wave comes. Researchers coordinate the information from multiple arrays to triangulate the source of the sound.

According to share-ng.sandia.gov, calculating where the sound wave is coming from can be a challenge when each sensor in the array is moving relative to each other and the source, said Bowman. A lot of computational algorithms assume stationary sensors, so the team needed to adapt them to include GPS information.

Bowman has proposed flying balloon-borne infrasound sensors as a part of the next series of the National Nuclear Security Administration's Source Physics Experiment project. This project develops new and improved, physics-based approaches for monitoring underground nuclear explosions.

In addition to potential treaty monitoring and national security uses, Bowman and Albert hope to fly hot air balloons in non-terrestrial experiments.

Bowman is assisting a NASA Jet Propulsion Laboratory project to explore the possibility of using balloon-borne infrasound sensors on Venus to listen for Venus-quakes. Venus is similar to Earth in mass, but is geologically very different with no apparent plate tectonics.

Another possibility the team is exploring is flying infrasound sensors on Jupiter. Jupiter is a gas giant with open scientific questions about its internal structure and geology that infrasound could help answer. "We're still decades out from an actual mission," said Bowman. "But I'm excited to see how far it will go."

The results from Bowman's prior research test flying individual infrasound sensors on balloons were published in Geophysical Research Letters and more recently in Journal of Geophysical Research: Atmospheres.

Bowman said, "This is a really exciting new area of research. Balloon-borne infrasound sensors will never replace ground-based acoustic arrays, but I think it can augment them. And the most exciting thing is flying in the atmospheres of other planets and what we can learn from them."

U.K. gov. launches £3M competition for innovative airport bomb-detection tech

Source: http://www.homelandsecuritynewswire.com/dr20180116-u-k-gov-launches-3m-competition-for-innovative-airport-bombdetection-tech

Jan 16 – Two U.K. government ministries — the Home Office and Department for Transport—have launched a Dragons' Den-style investment prize, hoping to find innovative ways to detect bombs in laptops, phones, and cameras carried by passengers on board.

The government has announced a £3 million SOS in an effort to attract scientists and inventors to help the security services and the airline industry keep up with the nefarious ingenuity of terrorists.

The competition will be open until 15 February.

The Home Office's website says: "The competition is looking for proposals for technologies to improve our ability to prevent explosives hidden within electrical items in hand luggage from being taken on board an aircraft."

The *Sun* reports that the competition follows the March 2017 ban the U.K. government imposed on carrying large electronic devices in the cabin of U.K.-bound planes from several Middle Eastern and African countries.

The ban was imposed after revelations that U.K. security services had thwarted thirteen terrorist plots in less than four years.

The restrictions on large phones, laptops, and tablets were lifted on flights from some of the airports in Turkey, Egypt, and Tunisia – but they remain in place on flights from other airports in Saudi Arabia, Jordan, Lebanon, as well as some airports in Turkey and Egypt.

The government says it hope that the technology would help produce a technology which would rule out "invasive and time-consuming" airport searches and reduce the need for extra security.

A government spokesperson added: "We're confident in the ability of current processes used to detect threats, but are aware that we need to stay ahead of changes to the threat.

"We're not just looking for solutions to detect concealed explosive devices/components. We'd also be interested in solutions to identify electrical items that may have been tampered with, or which appear to be out of the ordinary.

"This could allow us to focus the more resource intensive detection techniques on a smaller number of items."

The competition calls for technology which would be deployed at airports' central search areas and at the final departure screening point.

Following the ban, restrictions on

Philip Baum, an aviation safety expert and editor of *Aviation Security International*, told the *Sun* that the sheer variety of explosives means bomb-detecting technology is difficult to get right.

"Every bomb is different. Different component parts, different materials.

"Not all explosives are the same. There are thousands of different types. Powder, gels, cord, liquid.

"We have to think about how the broad range of explosives are going to be concealed."

He added: "For me, the biggest problem is, could it ID all types of IED, is it going to id chemical or biological bombs. No, because that would be different.

"Government is desperate to find a technological solution to resolve the problem and there is a huge reluctance to use the best technology of all - and that is the human brain. Using some common sense.

"Behavioral analysis is one thing. Non-racial profiling techniques.

"We have been installing X-ray machines since the 1960s, but we are assuming people are going to go through the machine and not go round the side or an attack on the check-in, like in Brussels.
"We must think and look at the behavior pattern and assess people. Looking for people with criminal activity or mental problems.
"That [a new bomb-detecting device] assumes nobody will have something in their body."

— Read more in Competition document: finding explosives hidden in electrical items (U.K. Department of Transport, U.K. Home Office, 12 January 2018).

Distant-scanning crowds for potential threats

Source: http://www.homelandsecuritynewswire.com/dr20180118-distantscanning-crowds-for-potential-threats

Jan 18 – Everyone wants to be safe and secure, but can you imagine if you had to go through a security screening at the metro station like there is at the airport? What if there were a way to safely scan crowds for potential threat items in places like metro and train stations without security officials coming into direct contact with the public and while maintaining individual privacy?
S&T says that the Department of Homeland Security's (DHS) Science and Technology Directorate (S&T) is seeking to address this challenge by developing a millimeter wave imager that will screen for potential threat items unobtrusively as people pass by, without slowing them down.
In partnership with researchers at the Massachusetts Institute of Technology Lincoln Laboratory, the Directorate reached a significant milestone in this pursuit in October 2017.
A prototype of the millimeter wave imager underwent a three-day developmental test and evaluation at the Massachusetts Bay Transit Authority's (MBTA) emergency training center in Boston, Massachusetts.

The facility served as an excellent testing venue by providing a realistic electromagnetic environment to gauge how the system will function in an operational metro station.
"Successful testing in a representative environment was a key milestone for the effort," said Dr. William Moulder, the program lead at Lincoln Laboratory.
Responsible for this endeavor is a program from S&T's Explosives Division called Surface Transportation Explosive Threat Detection (STETD). Among its holistic, curb to platform

approach, the program aims to develop techniques that will automatically highlight possible threat items and then cue security staff.

The millimeter wave technology consists of a set of antennas installed on flat panels. The antennas send out and receive low-power radio signals that can penetrate clothing and backpacks but will reflect off of certain items. Screening commuters from a distance, the technology produces high resolution images in real time, without negatively impacting the speed of travel, and will alarm operators if someone is concealing potential threat items.

Privacy will be maintained through automated anomaly detection; no image of an individual is displayed for review by security personnel.

During the three-day test and evaluation, technology developers from Lincoln Laboratory documented the prototype's ability to detect various simulated threat items at different distances on the rail platform while people were moving within the radar field of view.

"The goal is to make millimeter wave technology as seamless as possible," said Don Roberts, S&T Program Manager in the Explosive Division of Homeland Security Advanced Research Projects Agency.

The flat panel design of the millimeter wave imager can be configured into various sizes to facilitate integration not just in walls and ceilings, but also in columns, and even into fare gates and entryways. Being concealed behind signs and advertisements will allow them to be hidden in plain sight.

"The design can be scaled for large and small implementations depending on the particular case," said Moulder.

Moulder's team is currently developing image exploitation techniques. "We are developing new techniques and algorithms to try to make sense of, or to turn a microwave image into actionable intelligence or information that security staff can use," said Moulder. "With this prototype, we are hoping to provide DHS with a clear assessment of what role this technology can play."

Following the test at the MBTA training facility, S&T will review that data to further improve and refine the millimeter wave system. In the next phase, the millimeter wave prototype will be integrated with other technologies for layered testing.

The technologies S&T's STETD program is developing will be applicable to stadiums and other large crowd environments.

"We want to take advantage of the video information that facilities use on a daily basis and seamlessly dovetail the millimeter wave sensors with the video systems," said Roberts.

S&T notes that recently, the program the millimeter wave project is a part of, STETD, won the American Security Today's 2017 'ASTORS' Homeland Security Award for outstanding product development achievements and exciting new technologies to address the growing homeland security threats the United States is facing.

SO... ARE THERE CLEAN BOMBS?
SURE, SON... ...OURS!
6/12/2 LEXINGTON HERALD-LEADER/UNIV. PRESS SYND.

Cyber News

New Remote Fingerprint Scanning Application

Source: https://i-hls.com/archives/80372

Dec 21 – **A new mobile fingerprint scanning application for local and state law enforcement officers instantly searches state and national databases for a positive identification.** The technology has been deployed by the US State Bureau of Investigation.

The process is simple. A suspect places his or her finger on a small portable device, about the size of a smartphone and the fingerprints become digitized and sent to the SBI's Statewide Automated Fingerprint Identification System and to the FBI for a search of their databases for any matches. Once the fingerprint image is received at the SBI, the image is compared against the SBI's entire biometric database and sent to the FBI for a search of the Repository of Individuals of Special Concern, a combination of many different FBI databases that house sensitive law enforcement information.

According to **bladenjournal.com,** the **Rapid ID System** allows law enforcement officers to capture fingerprints remotely using the mobile fingerprint scanner. An officer quickly receives the results of a search on the handheld device.

If a fingerprint match is made, the device provides a person's name, photo (if available) and other relevant information allowing for a quick assessment of a potential threat level.

A national fingerprint search through the Rapid ID System also provides officers access to outstanding warrants in other states, national sex offender registry subjects and known or suspected terrorists. Several states are already using this remote identification technology and are experiencing great success.

Six ways (and counting) that big data systems are harming society

By Joanna Redden

Source: http://www.homelandsecuritynewswire.com/dr20171222-six-ways-and-counting-that-big-data-systems-are-harming-society

Dec 22 – There is growing consensus that with big data comes great opportunity, but also great risk. But these risks are not getting enough political and public attention. One way to better appreciate the risks that come with our big data future is to consider how people are already being negatively affected by uses of it. At Cardiff University's Data Justice Lab, we decided to record the harms that big data uses have already caused, pulling together concrete examples of harm that have been referenced in previous work so that we might gain a better big picture appreciation of where we are heading.

We did so in the hope that such a record will generate more debate and intervention from the public into the kind of big data society, and future we want. The following examples are a condensed version of our recently published Data Harm Record, a running record, to be updated as we learn about more cases.

1. Targeting based on vulnerability

With big data comes new ways to socially sort with increasing precision. By combining multiple forms of data sets, a lot can be learned. This has been called "algorithmic profiling" and raises concerns about how little people know about how their data is collected as they search, communicate, buy, visit sites, travel, and so on.

Much of this sorting goes under the radar, although the practices of data brokers have been getting attention. In her testimony to the US Congress, World Privacy Forum's Pam Dixon reported finding data brokers selling lists of rape victims, addresses of domestic violence shelters, sufferers of genetic diseases, sufferers of addiction and more.

2. Misuse of personal information

Concerns have been raised about how credit card companies are using personal details like where someone shops or whether or not they have paid for marriage counselling to set rates and limits. One study details the case of a man who found his credit rating reduced because American Express determined that others who shopped where he shopped had a poor repayment history.

This event, in 2008, was an early big data example of "creditworthiness by association" and is linked to ongoing practices of determining value or trustworthiness by drawing on big data to make predictions about people.

3. Discrimination

As corporations, government bodies and others make use of big data, it is key to know that discrimination can and is happening – both unintentionally and intentionally. This can happen as algorithmically driven systems offer, deny or mediate access to services or opportunities to people differently.

Some are raising concerns about how new uses of big data may negatively influence people's abilities get housing or insurance – or to access education or get a job. A 2017 investigation by ProPublica and Consumer Reports showed that minority neighborhoods pay more for car insurance than white neighborhoods with the same risk levels. ProPublica also shows how new prediction tools used in courtrooms for sentencing and bonds "are biased against blacks". Others raise concerns about how big data processes make it easier to target particular groups and discriminate against them.

And there are numerous reports of facial recognition systems that have problems identifying people who are not white. As argued here, this issue becomes increasingly important as facial recognition tools are adopted by government agencies, police and security systems.

This kind of discrimination is not limited to skin color. One study of Google ads found that men and women are being shown different job adverts, with men receiving ads for higher paying jobs more often. And data scientist Cathy O'Neil has raised concerns about how the personality tests and automated systems used by companies to sort through job applications may be using health information to disqualify certain applicants based on their history.

There are also concerns that the use of crime prediction software can lead to the over-monitoring of poor communities, as O'Neil also found. The inclusion of nuisance crimes such as vagrancy in crime prediction models distorts the analysis and "creates a pernicious feedback loop" by drawing more police into the areas where there is likely to be vagrancy. This leads to more punishment and recorded crimes in these areas.

4. Data breaches

There are numerous examples of data breaches in recent years. These can lead to identity theft, blackmail, reputation damage and distress. They can also create a lot of anxiety about future effects. One study discusses these issues and points to several examples:

- The Office of Policy Management breach in Washington in 2015 leaked people's fingerprints, background check information, and analysis of security risks.

- In 2015 Ashley Madison, a commercial website billed as enabling extramarital affairs, was breached and more than 25 gigabytes of company data including user details were leaked.
- The 2013 Target breach in the US resulted in leaked credit card information, bank account numbers and other financial data.

5. Political manipulation and social harm

Fake news, bots and filter bubbles have been in the news a lot lately. They can lead to social and political harm as the information that informs citizens is manipulated, potentially leading to misinformation and undermining democratic and political processes as well as social well-being.

One recent study by researchers at the Oxford Internet Institute details the diverse ways that people are trying to use social media to manipulate public opinion across nine countries.

6. Data and system errors

Big data blacklisting and watch-lists in the U.S. have wrongfully identified individuals. It has been found that being wrongfully identified in this case can negatively affect employment, ability to travel – and in some cases lead to wrongful detention and deportation.

In Australia, for example, there have been investigations into the government's automated debt recovery system after numerous complaints of errors and unfair targeting of vulnerable people. And American academic Virginia Eubanks has detailed the system failures that devastated the lives of many in Indiana, Florida and Texas at great cost to taxpayers. The automated system errors led to people losing access to their Medicaid, food stamps and benefits.

We need to learn from these harms. There are a range of individuals and groups developing ideas about how data harms can be prevented. Researchers, civil society organizations, government bodies and activists have all, in different ways, identified the need for greater transparency, accountability, systems of oversight and due process, and the means for citizens to interrogate and intervene in the big data processes that affect them.

What is needed is the public pressure and the political will and effort to ensure this happens.

***Joanna Redden** is Lecturer in Critical Data Studies, Co-Director Data Justice Lab, Cardiff University.*

The next Daesh is coming to a news feed near you in 2018

Source: http://www.wired.co.uk/article/ai-terrorists-global-threat-content-creation

50 MILES
Kabul
AFGHANISTAN
Peshawar
Islamabad
Rawalpindi
Drone attack
Miranshah
NORTH WAZIRISTAN
SOUTH WAZIRISTAN
PAKISTAN

Dec 27 – Blanketed by drones, surrounded by mountains and with Special Forces crawling in the foothills beyond, the town of Miran Shah was possibly the most watched place on Earth in the 00s. It was one of the few towns in Pakistan's mountainous frontier province that had internet access, and was therefore a vital artery for al-Qaeda. Couriers would risk their lives attempting to upload grainy propaganda videos and download messages from al-Qaeda's global network of operatives.

Those al-Qaeda couriers would envy the ease with which their Daesh counterparts can communicate today. Even in war-torn Syria, there are dozens of ways to get online. A decade ago, it would take al-Qaeda weeks or months to release a video, whereas a recent study by Quilliam, the counter-extremism think-tank, found that Daesh publishes around 35 unique pieces of content per day (dwarfing the output of many consumer brands). As Daesh emerged out of the remnants of al-Qaeda's Iraq branch, dozens of digitally native recruits filled its ranks, producing professional-looking, polished videos. Its media professionals are part of a privileged professional class, with salaries roughly seven times that of the average Daesh fighter. Syria has become the world's leading incubator for 21st-century propaganda.

Like all brands, Daesh's propaganda and narrative is now beginning to feel dated. And it will inevitably be disrupted by **a third global terrorist group. Let's call it 3.0.**

To understand how 3.0 may evolve, we need to explore the emerging technologies. Just as Daesh ruthlessly exploited Twitter, this next group will inevitably take propaganda to the next level by jumping on innovations in the digital space.

Among these is psychographic targeting, a form of bespoke advertising designed to appeal to an individual's personal psychology and seen by many as the most powerful development in politics for decades. Psychographic targeting was used by US- and UK-based data-mining company Cambridge Analytica in support of the Trump presidential campaign in the US and the Leave side in the UK's EU referendum, both in 2016. Millions of potential voters received personalised adverts designed to trigger emotive responses and push up turnouts. Within a few years, these capabilities will be available to the average user, as dozens of companies enter the psychographic targeting game.

A new global terrorist group will inevitably harness this technology in a bid to capture the hearts and minds of millions of potential sympathisers. Supercharged by artificial intelligence, new platforms will allow the speedy creation of bespoke, personalised adverts and messages. Simply upload your key messages and the platforms will create content uniquely tailored to each individual. The potential power of psychographic targeting for terrorist groups is significant.

The inevitable (and ironic) consequence of these developments is clear: power and influence will belong to world-class storytellers. Both al-Qaeda and Daesh excel at storytelling – communicating a narrative that inspires thousands around the world. By using artificial intelligence, psychographic data and billions of online posts, those who can lucidly package all of this data into a rich and compelling narrative will amass global political influence and power far greater than Daesh's current reach.

The good news is that we are already starting to fight back. In the US, there is a small but growing community of researchers who understand the threat of hyper-charged psychological warfare. These people have lobbied the US government for more resources for what is known as "cognitive security", highlighting that "in the future, researchers, governments, social platforms and private actors will be engaged in a continual arms race to influence – and protect from influence – large groups of users online".

Today, drones are circling over another town: the Syrian city of Raqqa now finds itself at the centre of a global manhunt. In 2018, many of Daesh's leaders will be killed or captured. From Tehran to Moscow and Washington DC, the victors will proclaim that evil has been defeated and peace has prevailed. But the reality is that many of Daesh's youngest and most talented propagandists have already left the war zone. In today's world, however, they are far more dangerous off the battlefield than on it.

Hackers can guess your phone PIN using its sensor data

Source: http://www.homelandsecuritynewswire.com/dr20171228-hackers-can-guess-your-phone-pin-using-its-sensor-data

Dec 28 – **Instruments in smart phones such as the accelerometer, gyroscope and proximity sensors represent a potential security vulnerability,** according to researchers from Nanyang Technological University, Singapore (NTU Singapore), whose research was published in the open-access *Cryptology ePrint Archive*.

Using a combination of information gathered from six different sensors found in smart phones and state-of-the-art machine learning and deep learning algorithms, the researchers succeeded in unlocking Android smart phones with a 99.5 percent accuracy within only three tries, when tackling a phone that had one of the 50 most common PIN numbers.

NTU says that the previous best phone-cracking success rate was 74 percent for the 50 most common pin numbers, but NTU's technique can be used to guess all 10,000 possible combinations of four-digit PINs.

Led by Dr. Shivam Bhasin, NTU Senior Research Scientist at the Temasek Laboratories @ NTU, researchers used sensors in a smart phone to model which number had been pressed by its users, based on how the phone was tilted and how much light is blocked by the thumb or fingers.

The researchers believe their work highlights a significant flaw in smart phone security, as using the sensors within the phones require no permissions to be given by the phone user and are openly available for all apps to access.

How the experiments were conducted

The team of researchers took Android phones and installed a custom application which collected data from six sensors: accelerometer, gyroscope, magnetometer, proximity sensor, barometer, and ambient light sensor.

“When you hold your phone and key in the PIN, the way the phone moves when you press 1, 5, or 9, is very different. Likewise, pressing 1 with your right thumb will block more light than if you pressed 9,” explains Dr. Bhasin, who spent 10 months with his colleagues, Mr. David Berend and Dr. Bernhard Jungk, on the project.

The classification algorithm was trained with data collected from three people, who each entered a random set of 70 four-digit pin numbers on a phone. At the same time, it recorded the relevant sensor reactions.

Known as deep learning, the classification algorithm was able to give different weightings of importance to each of the sensors, depending on how sensitive each was to different numbers being pressed. This helps eliminate factors which it judges to be less important and increases the success rate for PIN retrieval.

Although each individual enters the security PIN on their phone differently, the scientists showed that as data from more people is fed to the algorithm over time, success rates improved.

So while a malicious application may not be able to correctly guess a PIN immediately after installation, using machine learning, it could collect data from thousands of users over time from each of their phones to learn their PIN entry pattern and then launch an attack later when the success rate is much higher.

Professor Gan Chee Lip, Director of the Temasek Laboratories @ NTU, said this study shows how devices with seemingly strong security can be attacked using a side-channel, as sensor data could be diverted by malicious applications to spy on user behavior and help to access PIN and password information, and more.

“Along with the potential for leaking passwords, we are concerned that access to phone sensor information could reveal far too much about a user’s behavior. This has significant privacy implications that both individuals and enterprises should pay urgent attention to,” said Prof. Gan.

Dr. Bhasin said it would be advisable for mobile operating systems to restrict access to these six sensors in future, so that users can actively choose to give permissions only to trusted apps that need them.

To keep mobile devices secure, Dr. Bhasin advises users to have PINs with more than four digits, coupled with other authentication methods like one-time passwords, two-factor authentications, and fingerprint or facial recognition.

— Read more in David Berend et al., “There Goes Your PIN: Exploiting Smartphone Sensor Fusion Under Single and Cross User Setting,” Cryptology ePrint Archive (6 December 2017).

Innovative technologies for preventing cyberattacks

Source: http://www.homelandsecuritynewswire.com/dr20171229-innovative-technologies-for-preventing-cyberattacks

Dec 29 – The Department of Energy’s Pacific Northwest National Laboratory has licensed three of its most unusual technologies for preventing cyberattacks to Cynash Inc., a startup company funded by IP Group, an intellectual property commercialization company. Cynash was formed specifically to bring these three cyber protection technologies to market to provide a powerful new approach to the detection and prevention of cyberattacks.

Cynash intends to integrate these technologies into a suite of products and services to enhance cybersecurity in private enterprise, the public sector and industrial control systems.

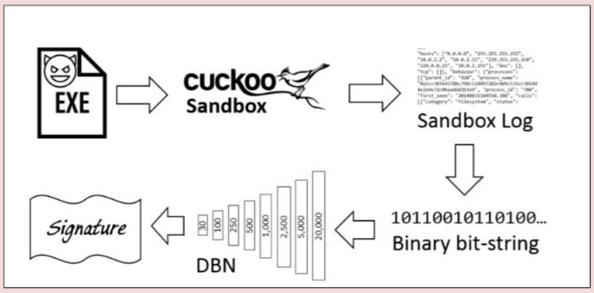
PNNL notes that two of the technologies, DigitalAnts and MLSTONES, are inspired by nature and biology.
The third, SerialTap, addresses vulnerabilities inherent in remotely controlled physical systems common in infrastructure and manufacturing.

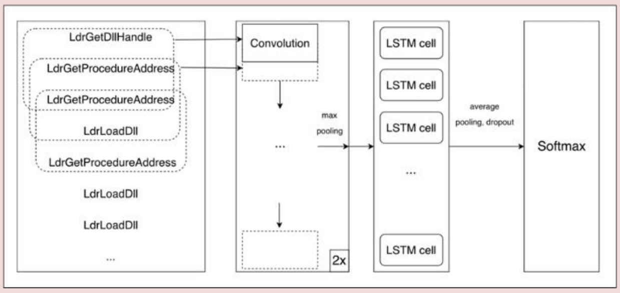
The Ants go marching

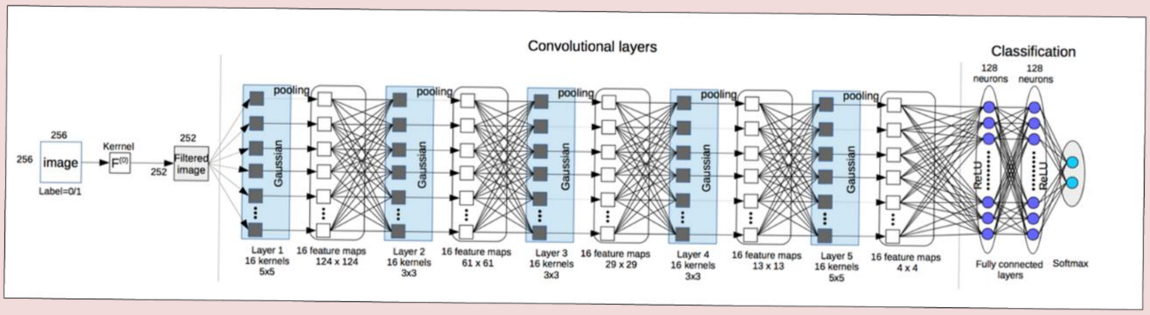
DigitalAnts, was inspired by the power of ants swarming to protect their colonies. In this case, the colonies are large scale networks or even connected devices such as phones and sensors and many others that make up the entire Internet-of-Things and can provide a foothold for cybercriminals. Distributed ant-like software agents wander across networks from device to device to detect suspicious behavior by watching types of information, such as network bandwidth or power consumption. Like their natural counterparts, DigitalAnts throw down markers much like pheromones to attract other ants to the location of concern. This concept of indirect coordination, known as stigmergy, allows rapid validation of an anomaly by several independent agents. Once an anomaly is confirmed, the DigitalAnts technology alerts users and other systems to take appropriate action.

A protein by another name

MLSTONES, which stands for Machine Learning String Tools for Operational and Network Security, was developed by researchers applying the power of high performance computing to vast amounts of biological data being captured to study protein similarity. They considered using this approach to cyber-related data such as software and specifically malware. This biological-based approach allows MLSTONES to recognize evolving, never seen before malware by detecting similarities in evolving malware —something that conventional malicious software detectors cannot do effectively. It also allows MLSTONES to classify malware into families based on behavioral similarity.







Tapping into the data

SerialTap was developed to bridge the gap between older serial based devices and modern networks in industrial control systems. An industrial control system sends and executes directions for remotely operating infrastructure such as valves, switches and sensors in distant field locations. They number in the millions and may be vulnerable to cyberthreats. When communications lines to these remote operations or serial devices are tied into the IT networks of industrial control systems, it may leave them open to bogus commands that could do serious damage. SerialTap taps into these older communications devices to translate information and mitigate threats. SerialTap is an inexpensive means of wrapping the data from the serial communications device in a form that can be used by modern assessment tools that don't 'speak the same language,' thus providing situational awareness to a company's engineering and security team.

PNNL says that IP Group discovered these technologies through the Department of Homeland Security Science and Technology Directorate's Transition to Practice Program, which connects promising cyber technologies with potential industry partners and investors. PNNL has participated in this program from its inception and has now licensed a total of five technologies through TTP — the most of any participant in the program.

"The DHS TTP program has been an invaluable partner to PNNL, as it has enabled our researchers to engage with cyber practitioners to identify how they might collaborate with each other to further develop and bring these technologies to marketplace rather than having the potentially game changing technologies languish unused," said Kannan Krishnaswami, a commercialization manager at PNNL. "Ultimately, any technology transferred out of the Laboratory and into the marketplace has an enormous impact on our sponsor's mission of keeping the nation safe and secure."

"We are delighted to establish another venture with our partners at Pacific Northwest National Laboratory and to be associated with the DHS TTP," said Michael Burychka, Chief Executive Officer IP Group North America. "The new enterprise, Cynash, Inc., will incorporate these unique technologies into a comprehensive and compelling cyber defense solution that will address the ever-increasing threat of these costly attacks. We couldn't ask for a stronger partner and are excited to build and support Cynash as it moves ahead."

'Bitcoin banned by Islam': Egypt's Grand Mufti issues fatwa against cryptocurrency

Source: https://www.rt.com/business/414903-egypt-mufti-ban-bitcoin/

Jan 04 – The Egyptian Grand Mufti has issued an official fatwa, banning bitcoin which soared in value over the $20,000 mark in December. Trade in cryptocurrency is similar to gambling, which is forbidden in Islam, he said.

The fatwa was issued after consultations with several economic experts, Egypt's Grand Mufti Shawki Allam said on Monday, as cited by Ahram newspaper. Egypt's legitimate bodies do not consider trading a virtual currency like bitcoin to be acceptable, he said, and the use of cryptocurrencies *"impinges on the state's authority in preserving currency exchange."*

The mufti compared cryptocurrency's trade exchange to gambling, which is banned in Islam *"due to its direct responsibility in financial ruin for individuals."* The cleric said that bitcoin could negatively affect the legal safety of those who trade it, and lead to an *"ease in money laundering and contrabands trade."*

Allam's statement came as the value of bitcoin continues to fluctuate unpredictably. As of January 3, its price stands at $15,000.

Egypt's Grand Mufti is not the first Muslim cleric to criticize the now-famous cryptocurrency, which has skyrocketed in value over recent months. In December, popular Saudi cleric Assim Al-Hakeem ruled that digital currencies are banned under Islamic law because they are *"ambiguous."*

"We know that bitcoin remains anonymous when you deal with it... which means that it's an open gate for money laundering, drug money and haram [forbidden] money," Hakeem said at that time.

In November, Turkey's highest religious authority – the Directorate of Religious Affairs, also known as the Diyanet – declared that buying and selling of digital currencies is at odds with its religion due to its lack of regulation and close connection to criminal activities.

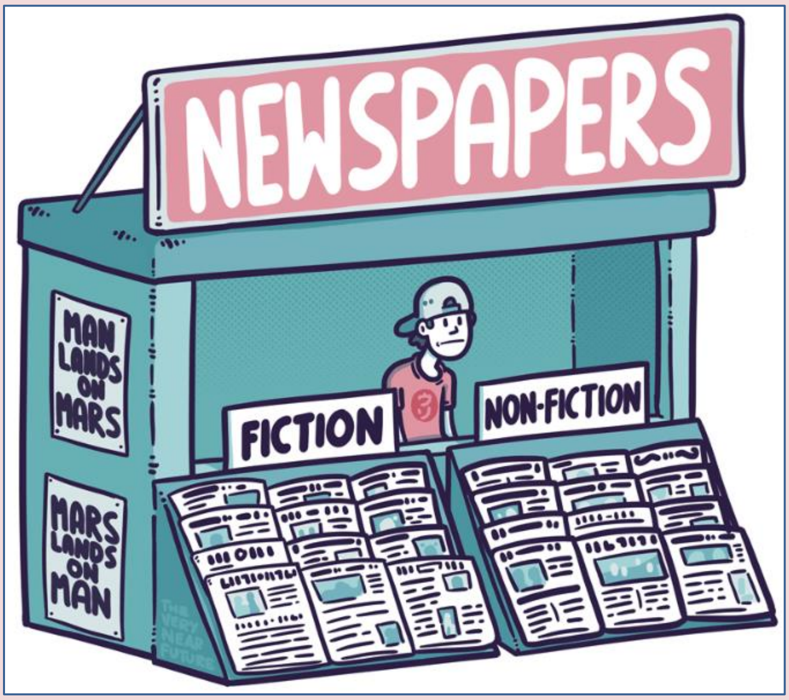
Last year saw cryptocurrencies steal the headlines and take retail investors on a rollercoaster ride. Despite declines in December, bitcoin has seen a remarkable rise over the course of 2017, during which its price increased by over 1,300 percent.

Macron vows law against fake news

Source: https://euobserver.com/justice/140450

Jan 04 – French president Emmanuel Macron is seeking to give authorities powers to remove or block social media content deemed as fake news during election seasons.

Speaking to reporters on Wednesday (3 January), Macron said the plan is needed to protect liberal democracies following Russian-led attempts to thwart his own presidential campaign last year.
"There will be increased transparency requirements for internet platforms regarding sponsored content, with the aim of making public the identity of those who place the ads and also limiting the amount of them," he said.



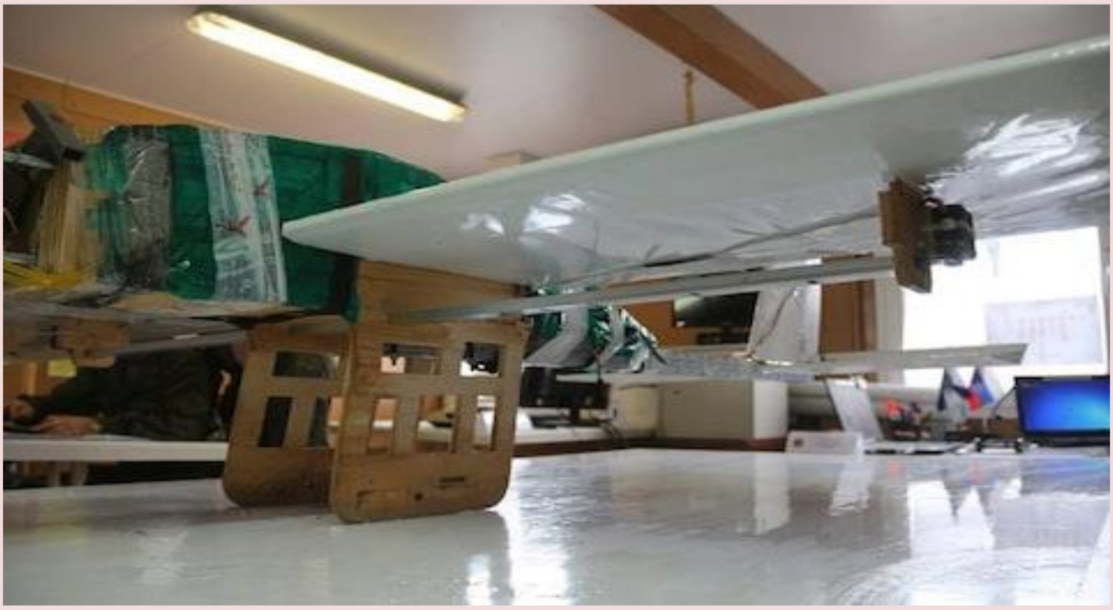
The proposal is part of an envisioned law to ban fake news, which would also empower a judge to remove content or block a site. France's media watchdog, the CSA, would also have sway over foreign-operated TV stations.
A UK-based firm, Bakamo, found in a survey published last year that one in four internet links shared by French users of social media in the lead-up to the elections was fake news. The links favoured anti-EU candidates like Marine Le Pen and Jean-Luc Melenchon.
Bakamo also found that Russian state media giants like RT and Sputnik had been spreading and influencing some of the anti-EU content.
Marion Marechal-Le Pen, at the time, had shared a fake news story that claimed Macron's campaign was being part financed by Saudi Arabia. The link redirected the reader to an article designed to look legitimate, which was posted on a cloned copy of the Belgian daily newspaper Le Soir.
EUobserver had also viewed 2,951 examples of Russian fake news, most of which was aimed at condoning Russian annexation of Crimea from Ukraine, or its military forays into Syria.
Others included fake stories of rape or violence by migrants. Among the more egregious was the rape of a 13-year old Russian girl in Germany by migrants, which turned out to be entirely fabricated but was still reported as fact by Russian media and the Russian foreign ministry.

German law confuses satire with hate speech

Macron's anti-fake news plans follows a new German online hate speech law. Social media companies that fail to remove such posts in Germany within 24 hours could be fined €50 million.
But the German law, which was launched on 1 January, is already creating problems for confusing satire with hate speech.
Titantic, a German satirical magazine, had its Twitter account blocked on Wednesday after poking fun at Beatrix von Storch, a member of the right-wing Alternative for Germany (AfD) party. Von Storch had earlier in the week made disparaging remarks on Twitter about Muslims, which Titantic then mocked in a follow up Tweet. The Association of German Journalists (DJV) described Titantic's blocked Twitter account as censorship

Russia uses missiles and cyber warfare to fight off 'swarm of drones' attacking military bases in Syria

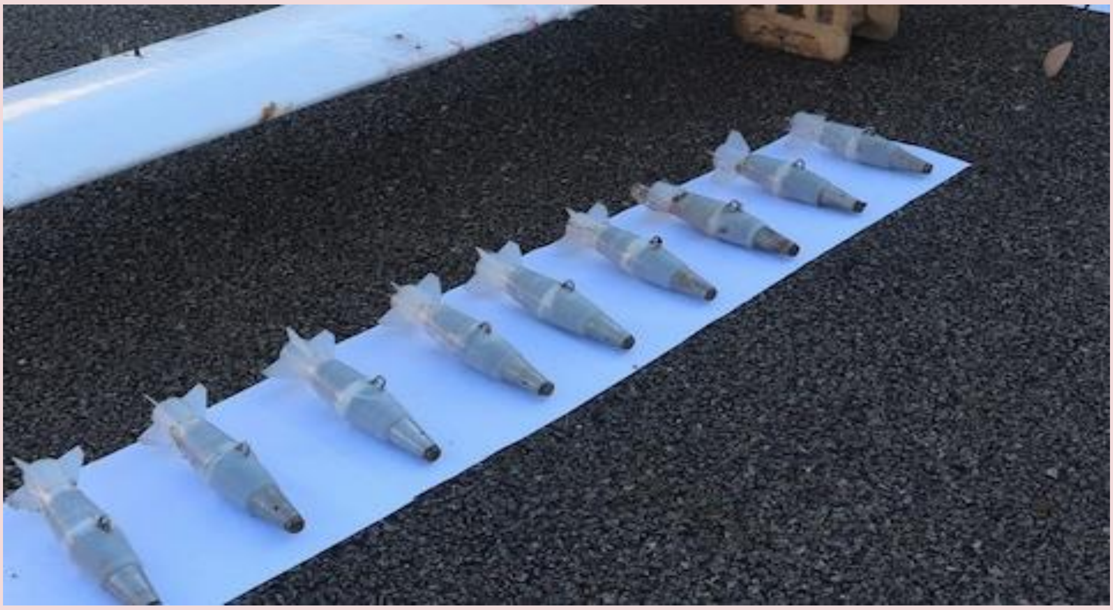
Source: http://www.telegraph.co.uk/news/2018/01/09/russia-fought-swarm-drones-attacking-military-bases-syria/
Jan 09 – The Russian military says it has fought an attack by a swarm of drones launched by jihadists against its bases in Syria.
Thirteen attack drones were launched against the Khmeimim air base and a naval facility in the city of Tartus on Syria’s western coast, the Russian defence ministry said.
Russian forces shot down seven of the drones with anti-aircraft missiles while the other six were hacked by a cyberware unit and taken under Russian control, the ministry said. No damage or casualties at the two military bases were reported.



The drones appear to be made partly of wood and held together by masking tape Credit: Russian Ministry of Defence

The attack appears to be the largest example to date of insurgents using a mass of primitive drones in combat and Russia said it had never before faced such an attack.

"It was the first time when terrorists applied a massed drone aircraft attack launched at a range of more than 50 km using modern GPS guidance systems," a defence ministry spokesman said.



Explosives Russia says it recovered from the drones Credit: Russian Ministry of Defence

Defence experts have long predicted that drones will become an increasingly common feature of the modern battlefield, employed by both sophisticated nation state militaries and by low-tech rebel groups.

Three of the drones were recovered by Russian forces, the ministry said, and photographs showed a small aircraft made partly of wood and held together with masking tape. Another picture showed a row of small explosive.

The Russian defence ministry said that "countries with high-technological capabilities" might have supplied materials for the armed drones but did not accuse a specific country.

Russia has in the past accused Western and Arab states of deliberately arming jihadist groups in Syria to fight against the Assad regime.

Suspicion for the attack, which occurred the night of January 5, immediately fell on Syrian rebel and jihadist groups based in Idlib, an opposition controlled province next to Latakia where both Russian military facilities are located.

Ahrar al-Sham, an Islamist rebel coalition, and Hayat Tahrir al-Sham (HTS), a jihadist group with links to al-Qaeda, are both based in Idlib and fighting against the Assad regime and their Russian allies.

Russia said it shot down seven drones and hacked six more using cyberwarfare technology Credit: Russian Ministry of Defence

However, neither group claimed responsibility for the attack and in a social media post a previously unknown group called the "Free Alawites Movement" said it was behind the drone swarm.

The Alawites are a small sect of Shia Islam, and Bashar al-Assad and his family are Alawites - making it surprising that an Alawite group would attack Assad's Russian allies.

In the post, the Free Alawites Movement said "the Russians will not be able to stay [in Syria] for more than six months" and warned Assad not to rely on the Russians for help.

"The days are coming when it will be more painful for the Russians especially before the election of Putin," the statement said.

The Free Alawites said they had attacked with drones armed with grenades and with rockets and succeeded in destroying a Russian S-400 missile launcher - contradicting the Russian claims that they suffered no damage.

The Khmeimim airbase came mortar attack on New Year's Eve and seven aircraft were destroyed and two Russian troops were killed, according to Russia's Kommersant newspaper.

It was reportedly the single largest loss of Russian military equipment since Vladimir Putin ordered Russian forces into Syria in September 2015.

While the bases in northwest Syria are of significant strategic value to Russia, they are also tempting targets for jihadist and rebel groups trying to inflict damage on Assad's biggest military backers.

The Kremlin said Tuesday that it had enough forces in Syria to withstand any attacks on the bases.

Terrorists Could Use Teslas to Kill Us

By Zach Aysan

Source: http://www.weeklystandard.com/terrorists-could-use-teslas-to-kill-us/article/2011171

Jan 17 – It's a calm Saturday morning in August of next year. Suddenly, across the nation, 12,000 Tesla Model S sedans start up at the same time. They engage Tesla's vaunted autopilot feature and head out onto the road. Some of them make their way to local gas stations. Some to electrical substations. And then, as they approach, they accelerate to top speed. The explosions are fantastic as the Model S batteries rupture and spark fires, which ignite anything flammable in the area. The power grid in the Los Angeles area is brought down almost immediately. Hundreds of fires rage. America is under attack. This might sound like science fiction. It's not.

ATOR.SERVERS.1.data.SITE XXXX.info->XXXXX.com
ATOR.SERVERS.1.data.URL cgi-bin/counter.cgi->wp-content/rss.php
RESTORE_REDIRECTION_STATE
ATOR.SERVERS.-1.SITE [NoValue]->XXXX.info
INGLE_CMD_RUNNER
_CMDS.RESTORE_REDIRECTION_STATE.SECS_BETWEEN_RUNS [NoValue]->87654
_CMDS.RESTORE_REDIRECTION_STATE.MAX_RUNS [NoValue]->2
_CMDS.RESTORE_REDIRECTION_STATE.CMD_BUF [NoValue]->BUF_SITE:271 CRC:525FXXXX
_CMDS.RESTORE_REDIRECTION_STATE.NUM_OF_RUNS [NoValue]->0
INGLE_CMD_RUNNER

* * *

With cyber security the first thing to understand is that the internet is ungovernable because locality is irrelevant and identity is shroudable. This is by design—it's *the Internet*—we're all supposed to be able to talk to everyone and it wasn't designed at the protocol level to require payment or identification.

Cyber criminals make mistakes and are arrested occasionally, but attacks can originate from states that do not cooperate with international institutions or foreign governments. And outside of the developed world there is often even less of a distinction between private individuals and state actors: A software security expert can work to enrich herself—or a criminal enterprise—one day and then work for their government's intelligence service the next. This makes international cooperation even more difficult.

The second thing to recognize about cyber security is that attack is much easier than defense. Attackers can probe from multiple points, such as previously-hacked computers or servers rented with stolen credit card information. They can patiently try different strategies until they succeed. Talented attackers may first invent a new method of attack, then write software to scan servers or internet traffic to create a prioritized list of potentially vulnerable organizations, and only then begin systematically breaching them.

A defender, on the other hand, is a sitting target. Her application is public facing, with URLs, domains, and data centers that anyone can investigate. She has a consistent, detectable set of operating systems, software languages, and libraries that are as well understood by potential adversaries as they are by the in-house team that is responsible for managing them.

And a defender only has to make one mistake: A single entry point incorrectly secured will allow access to attackers. Defending all entry points and perpetually keeping them defended, despite changing organizational requirements, personnel, and a never ending stream of vulnerability updates to software libraries, is nigh on impossible. And even organizations that have the technical competence and resources to defend against persistent attack—such as the NSA, for example—are one insider away from critical breach or exfiltration. The attack surface is huge and the threat is persistent. If you can't arrest the attackers and the attackers have an infinite amount of time to find vulnerabilities, then the question isn't *if* the system can be breached. It's *when* the system will be breached. And what the attackers will do when they breach it.

Once a system is breached, a sufficiently prepared attacker can use pre-written software to accomplish prioritized objectives. For example, malware attacking a retail platform might exfiltrate password lists and cryptographic keys first, and only later collect information such as purchasing history. Once an attacker begins to suspect that their activities have been noticed, they can encrypt the compromised server's hard drives before ransoming them back to their owners. Welcome to the cyberpunk future: it's stranger and less dingy than promised, but hackers have panicked organizations scrambling to pay cryptocurrency ransoms. I know. I'm the one helping organizations during crisis.

In the '90s, as an irresponsible youth, I hacked computers illegally for fun, before starting to write security-critical commercial software for the telephone industry. My early experimentation with cryptocurrencies and work as a whitehat led to companies coming to me after being hit by ransomware. I help them understand their options and the steps they need to take in order to get their systems up and running, with mitigation strategies for next time. (If you're reading this and need help, sorry, I only take introductions through personal contacts to prevent getting targeted by cybercriminals. I also no longer personally hold cryptocurrencies for the same reasons.)

Even the most dedicated defenders have *some* vulnerabilities. The most dangerous kind are called "zero-day" exploits because they find cracks in the software foundation that no one—not even the original designers—knew existed. The most famous zero-day might be Heartbleed, a security hole in a widely used library called OpenSSL, which, after it was discovered, caused a number of organizations to panic as system administrators rushed to patch in advance of a breach. Hackers exploiting Heartbleed used it to steal—just as one example—the security keys at a major U.S. hospital system, which comprised the privacy of 4.5 million patient records.

The third thing to understand about cyber security is that certain classes of cyber attack, including most zero-day exploits, can break all instances of the same system at the same time. For example, while it would take two separate missiles to destroy two separate predator drones, a single software vulnerability could be exploited by a virus to breach and disable both missiles simultaneously. This is how the WannaCry virus was able to infect hundreds of thousand computers, including life saving machines used by hospitals in the United Kingdom.

And once attackers have control of a system, it can be very hard to wrench it back. Data moves very, very quickly. A server in Austin takes about 140ms to send data to a server in Tokyo. What this means is that if you rely on human judgment during an attack to safeguard a system by taking it off-line, you might be too late because compromised devices can disengage themselves from remote control. A hacked phone, for example, may update its network code to pass all information through a VPN controlled by an assailant. And without countermeasures enacted ahead of time by the phone manufacturer, instructions to update the phone's vulnerable software can be automatically blocked, resulting in a permanently compromised device.

To reiterate, here are our three precepts:

1) The internet is anarchy. It is difficult to attribute attacks and even when it is possible, public disclosure reveals sources and methods.

2) Cyber defense is extremely difficult, especially over time as organizations change.

3) Some classes of cyber attack allow control of all instances of a device and, with the right pre-planning, can prevent access to the device owner once breached.

* * *

Which brings us to the intersection of computers and the real world.

In 2010 a team of researchers discovered Stuxnet, a virus written in a joint collaboration between Israel and the United States to disrupt the Iranian nuclear weapons program. Though the Iranians took steps to ensure that their nuclear material processing equipment was not connected to the internet, the virus was ferried into the facility on a USB stick. Once Stuxnet took hold, it subtly altered the operation of the facility's centrifuges so that they would slowly, and seemingly inexplicably, destroy themselves without revealing the presence of the malware.

Stuxnet taught the cyber security world two things: First, viruses aren't just intelligence tools—they're tools of war. Second, whether or not a computer is internet-connected is more of a continuum than a binary fact. The Iranian weapons program can be pretty dark but still let in USB keys; a Twitter profile can be white hot but still go offline occasionally. And data can be exfiltrated through a multitude of methods.

With advances in machine learning, data can be analyzed and filtered locally so that low-bandwidth or high-latency methods of communication aren't the barriers they once were. For example, an adversary can employ voice-to-text on a company's internal videos and only exfiltrate those that mention keywords critical to research.

And to show you how complicated this forest of mirrors really is, consider that Kaspersky Lab, the research group which discovered Stuxnet, has recently been classified by the United States Department of Homeland Security as likely having ties to the Russian FSB, the post-Soviet replacement of the KGB. So maybe Kaspersky's ferreting out of Stuxnet wasn't just an accidental gift to the Iranians after all.

* * *

Over the past 20 years a multitude of everyday devices have become computers. Refrigerators are now computers. Watches are now computers. Even things like one-time use sensors employed to ensure correct concrete hardening are now computers.

Cars are computers, too.

And they're just about as secure as computers everywhere else.

In 2015, Jeep got hacked and had to ship millions of USB sticks to patch the automotive software. But why *just* Jeep? If hacking a Jeep is as straightforward as hacking a server, and servers are routinely breached, then where are all the hacked cars? It's a bit like the Fermi Paradox.

The explanation is likely a mix of factors. It could be that security researchers just aren't looking closely enough at cars. It could be that the blackhats aren't as motivated to attack vehicles because the ROI is more elusory. It could be that hackers have trouble adapting techniques that work on servers and personal computers for cars because the attack surface is smaller. Or the answer could be more sinister. Uber hid a 57-million user data breach by paying off the hackers. Perhaps automotive companies have quietly been doing the same.

* * *

Structural engineers limit how much deflection a beam or causeway can undergo during expected load not because the deflections themselves are necessarily unsafe, but because they expect people to reliably report when things feel wrong—and if large, but otherwise safe, deflections are routine, then large-but-unsafe deflections will go unreported. Structural engineers also use more conservative designs when systems cannot exhibit potential weakness before failure.

You should think about computers the same way.

Computers hit with sophisticated malware show no sign of infection. Even if an attack requires multiple stages or intermediary computers, as Stuxnet did, carefully-written viruses are invisible. All software, including viruses, is just code and code is just data and data doesn't change how we perceive the computer it resides in unless the software on the computer intends for us to perceive the change.

And now for the scary stuff. Remember our third precept: that some classes of cyber attack compromise all instances of a device.

We think of Teslas as cars just like we think of an iPhone as a phone, but a more accurate account of reality is that they're both just computers. One drives you around while the other sits in your pocket, but that's basically the sum of the difference. No matter how strange it may sound to a layperson, to a software developer the similarity between the two so obvious that it isn't worth even mentioning: They're both just operating systems on a piece of hardware.

Which means that something like WannaCry is just as possible for Teslas as it was for hospitals. They are both hackable, at scale.

There is another difference, of course: Your iPhone can't move on its own. But an autonomous vehicle, like a Tesla, that crashes into a chemical plant, electrical subsystem, oil line, or gas station while traveling 125 miles per hour could do a great deal of damage.

Now let's combine those two thoughts together. What would happen if someone hacked thousands of autonomous cars all at once and turned them into weapons?

Nothing good, that's what.

* * *

One of the problems I've had over the past year and a half is how to communicate this idea without either sounding like a crank or giving bad actors ideas.

After the thought first occurred to me a year and a half ago I reported it to Public Safety Canada. A year later I met with my member of Parliament to find out what efforts we were putting forward to mitigate the potential threat. What I learned was that there were not only no regulations on autonomous vehicles, but that there were no plans to create regulations, either.

After talking with most of the major autonomous car makers, including Tesla, BMW, GM, and Toyota, I realized that decision makers in large automotive companies don't have a magic solution any more than startup software developers do.

They know they need autonomous driving technology to compete in the marketplace. They also know they're exposed. At the moment, their primary defense is the obscurity of their platform, which means that the more successful they become, the more vulnerable they'll be. Not a great position to be in.

And it turns out that most software developers haven't really thought of self driving cars and cyber security at the same time, nor do they know the interfaces that the electrical systems on automotives expose.

What this means is that we have time. These exploits aren't difficult for organizations like the NSA, but they aren't something that ISIS or North Korea is capable of easily pulling off. We're exposed, yes, but the sky isn't falling. We have time to create the right regulations and international agreements—if we can foster the political will and act.

* * *

There are a number of ways to approach autonomous vehicle security, but let's start with a frank assessment of what *won't* work:

1) Relying on off-the-shelf anti-virus software. The only anti-virus that should be trusted is the one that comes with the operating system.

2) Trying to air-gap autonomous devices. Between aerial Bluetooth viruses traveling across smart light bulbs, debugging devices at your local automotive repair shop, or just plain old mistakes (like vulnerable software defined radios) air gaps can't be ensured. The Iranian nuclear facilities were air-gapped and that didn't stop Stuxnet and the CIA, so we shouldn't count on it stopping the DPRK.

3) Code review. When Western governments build their security systems, they often rely on pieces of hardware built in China. The "security" of these components is certified by inspecting the code on a handful of samples.

But while the British government may code review Chinese network gear in Banbury, Oxfordshire, if it ever came to total war with the Chinese they would likely have to replace all of it with American stuff. Because unless you inspect each individual component you get from a supplier, and it all has physically unmodifiable code, you have no idea what code is currently running your system.

The chief deterrent against a Chinese supplier such as Huawei slipping malware into its products is loss of trade and reputation—commercial considerations that are moot when it comes to state strategic priorities in war.

4) Trusting automotive companies. Equifax and Ashley Madison were secure. Until they weren't. National security isn't something to entrust to corporations and certainly not to corporations from countries with a poor history on cyber security, such as China. Capitalism rewards invention and risk, not long-tail risk mitigation.

5) Certifying individual components or vehicles. Detailed, prescriptive regulation and individual certification is too slow to keep pace with the fast-changing nature of modern software development. Our most secure corporations update their code multiple times per day. This isn't just a correlative artifact of well-run tech companies—it's causal. The first actor to find a vulnerability is usually the organization responsible for the service or device and they get the fix out as fast as possible.

Instead, regulations should be functional. For instance, a maxim such as "data should never be readable by an intermediary network device" or "no action taken by the media computer should change state in the control computer" so fines and security bounties aren't arbitrary, but automotive companies can still compete on the speed of their technology advancement.

6) Allowing the market to price wide-scale cyber attack as part of existing automotive insurance. With all due respect, insurance companies have neither the balance sheet, nor the expertise, to effectively estimate these risks. The Poisson Distribution is wonderful, but computer viruses invalidate all classes of the same system at the same time—so it shouldn't be used as a basis for pricing or predicting attacks. Without statistical independence, vulnerabilities of this scale cannot be accurately priced because it is impossible to get precise probabilities of the likelihood of a black swan event. Civil engineers design for 1-in-100-year storms. What does a 1-in-100-year cyber attack even look like? No one knows.

7) Waiting for autonomous vehicles to be used in small-scale attacks before crafting legislation. If we wait for such an occurrence then the resulting legislation is likely to be geared toward small-scale attacks and not focused on the bigger risk. Our first concern should be focusing on our national security (large-scale hacks of entire fleets), not securing soft targets (individual car hacks).

* * *

So what would work? Effective policies should all start with a recognition that governments aren't going to be able to intelligently regulate the issue. A well-funded, open-source effort with clear recommendations will be the most efficacious way of securing the driverless vehicle.

1) Software professionals should educate and encourage electrical and mechanical engineers to submit proposals that will help autonomous vehicle companies and governments protect the public.

2) The OSINT and arms control community should help with drafts of international agreements to make the cyber targeting of civilian systems during wartime illegal under international law—and we need legal minds to craft sample regulations that less-technical countries can use as a baseline.

3) Our trade agreements should reflect the changing nature of our interdependence. China recently announced that foreign automotive companies such as Google's Waymo cannot photograph every square inch of their roads due to concerns over national security.

But autonomous vehicles require both cameras and an internet connection to operate, so this regulation will have the effect of keeping foreign-made autonomous vehicles off of Chinese roads.

The Chinese either understand the threat that autonomous vehicles pose and want to limit their exposure—or they're using national security concerns to mask an attempt to incubate their own autonomous vehicle industry.

Either way, the Chinese clearly understand something that is lost on many Westerners: Liberalized trade is great, but national security is more important. Without international cooperation on autonomous vehicle regulation and symmetric trade agreements with harsh violation provisions, we should not allow non-friendly states access to our autonomous vehicle markets. (Nor should we allow components from these countries.) The Chinese get this. America should, too.

4) Any permanent, non-military device that can fly, drive, walk, rocket, or swim autonomously should allow for a standardized safety module. The power of the propulsion mechanism, as well as the computers and sensors that command the autonomous device, should connect through this safety module. And if this isn't possible due to the nature of the propulsion system (e.g., devices with chemical rockets), then an emergency disabling system should be present instead.

The device must not be powerable or operable unless the safety module is present and the device should not be able to access its own safety module in any way. (Military devices shouldn't be subject to these regulations.)

Countries should be able to specify what safety modules are acceptable within their domain, and you would expect that most major countries will develop their own module or only trust devices with safety modules from their closest allies. But devices could be designed to accept multiple modules, any of which can initiate the safety procedures. That way autonomous movement does not need to cease when crossing a border.

(Though care would need to be taken to ensure that the devices were truly independent. Any safety module should be able to shut down the device or take it offline, even if other modules have commands to act maliciously. Security should be additive, not multiplicative.)

The safety modules should be able to communicate through multiple channels; including satellite, radio, LTE, and even pulsating light via onboard camera. This way, by utilizing cryptographic keys and certificates, governments could order autonomous devices (through the safety module) emergency commands, like "Shutdown in 5 seconds" or "Cease software updates until further instruction." The safety module itself must be able to disengage both the power and the controlling computer in emergencies.

And finally, in order to ensure the integrity of the module itself, no matter what code is present on the autonomous device's computer, the device should not be able to interfere with its safety module or the safety module of any other autonomous devices.

(The most straightforward way of securing the safety module would be to employ traditional computer architecture with a one-way connection to the main computer and a fallback to an unchangeable ASIC with its own cryptographic key pair and a direct connection to the power.)

5) Standardized, redundant systems are another safeguard. If power is removed from the primary computer of an autonomous device, then the vehicle should still be able to land or park safely. Hard shutdowns should always be available, but it shouldn't be the first resort during a cyber attack.

6) In order for an autonomous vehicle to go faster than a preset speed limit it should request permission to do so from the module. That way, you could get to the hospital quickly during an emergency, but governments could limit how many speeding vehicles are allowed at one time. Why is this important? Because a car moving half the speed has one quarter of the kinetic energy—and is less likely to have a battery explosion on contact.

7) Isolate the control computer. Most automotive electronic control units communicate using the Controller Area Network (CAN bus)—an unauthenticated, unencrypted multi-master bus. Around the world software developers reading the previous sentence just spit out their coffee. *Do not allow control computers to read data directly from the CAN bus.*

And do not connect the vehicle's media computer to the control computer.

If we must get state from the CAN bus then it should be through an intermediary module that converts signals to one of a finite series of states / enums. (And while we're at it, we should create an international agreement to sunset the CAN bus and replace it with something more secure.)

8) Take a note from Apple and use a Secure Enclave dedicated to security-critical tasks, such as updating the control computer's software. As with the safety module, the security enclave should have fallback communication methods to safely disable the car during a critical vulnerability. Ideally, the security enclave should be designed with multiple sets of chips from different manufacturers in order to mitigate industrial espionage, or vulnerabilities such as Intel's Meltdown.

9) Do not trust the network. Do not trust DNS or certificate chains. Employ IP pinning and certificate pinning with fallback strategies. Do not rely solely on HTTPS. Protocols and ciphers aren't perfect and protocol downgrade attacks are too easy. Use client-side encryption in addition to HTTPS and use *really big* keys.

Ship every car with its own, massive One Time Pad (OTP). And create the OTP with multiple secure random sources on computers never connected to the Internet in the secure, guarded facility used for code signing. It should not be physically possible to read the same bit twice from the OTP. Final code review should be on computers never connected to the internet. And never, ever, allow SSH access to any autonomous vehicles—even those under development.

10) Employ code and data signing and encryption on everything that is possible, including data in volatile memory. All updates to the control computer should be encrypted, signed, and double checksummed. (The checksum should be shared with governments and broadcast to the safety module.) If the control computer cannot verify the software update's signature or checksum with the safety module, the control computer should shut the vehicle down safely.

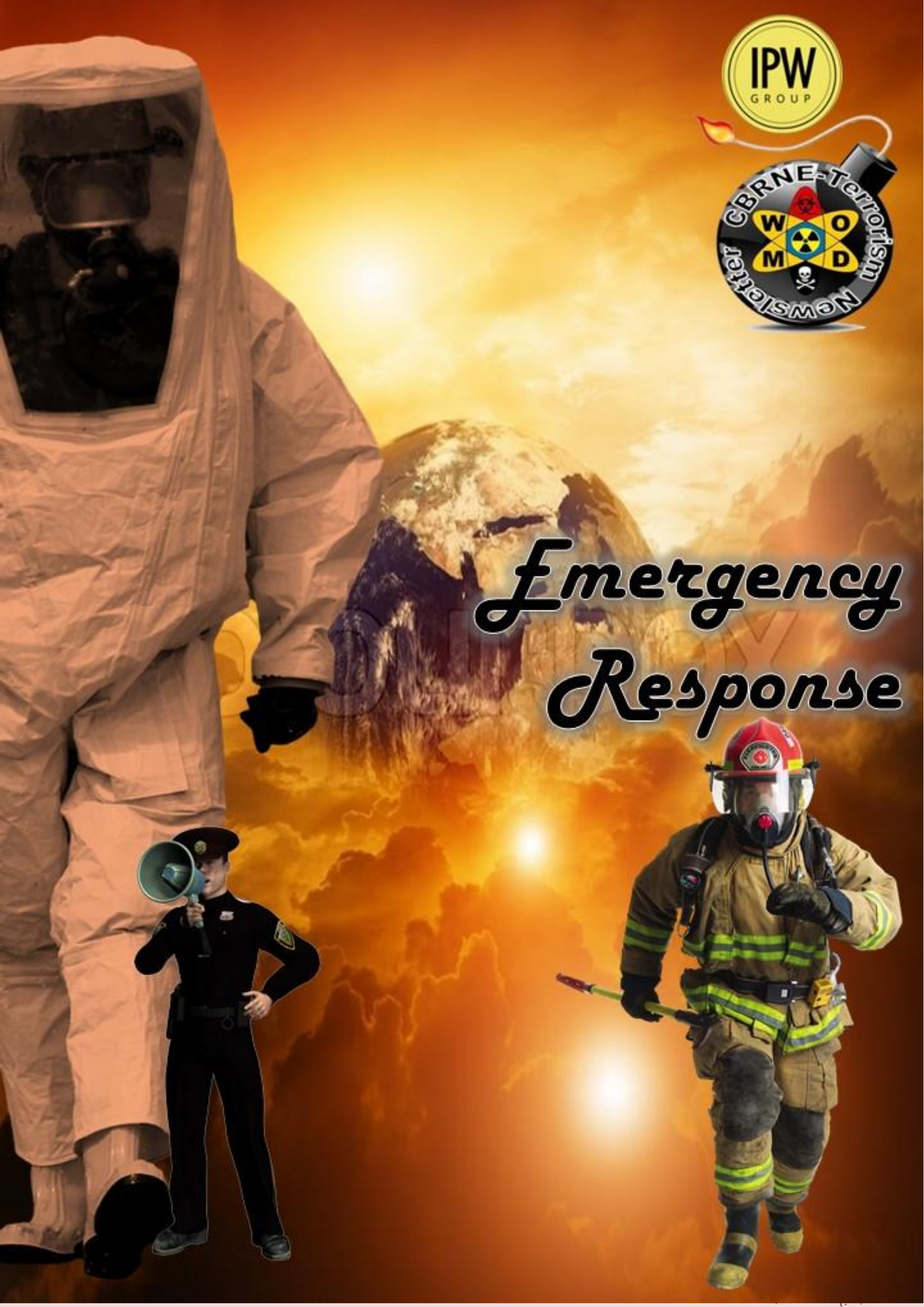
There are other ways for governments to nibble at the periphery of the problem: Governments ought to band together to create a system of bug-bounties, in order to incentivize security researchers. (Bounties for real remote control should range between $100 to $10,000 per device, depending on factors like max speed attainable.) Governments should also agree to impose harsh fines and prison sentences for the manufacture, sale, or provision of counterfeit automotive electronics

And in America, we ought to both dramatically increase funding for cyber warfare units and find a way to expand cyber reserves to engage computer experts in the private sector. For those who couldn't possibly get a security clearance, direct them to open source initiatives and think tanks.

Finally, America should increase funding for research into chips that are specialized for security, not performance (so that vulnerabilities like Meltdown and Spectre are less likely), and create regulations that encourage safer programming languages, such as Rust, over those that have unsafe or undefined behaviour.

There is a silver lining to all the work we have to do: The nature of the autonomous vehicle threat may finally bring about the political will, economic incentives, and ideas we need to secure our real-world computer systems. And with a little luck, we could wake up decades from now and talk with amazement about cyber events of the early 2000s like we do of the chemical fires on the rivers in the mid 1900s.

***Zach Aysan** is a software expert from Toronto working to protect the public. This piece is adapted from the essay "Self-Crashing Cars."*



Emergency Response

New method to assess damage from natural disasters

Source: http://www.homelandsecuritynewswire.com/dr20171222-new-method-to-assess-damage-from-natural-disasters

Dec 22 – Awesome. Amazing. Incredible. Unbelievable. Spectacular.

These words aptly describe what is left following any natural disaster, whether it's an earthquake, tornado, hurricane or any other occurrence where homes, buildings or infrastructure are destroyed and lives are turned upside down.

However, these words are not the words the people whose lives have been permanently changed want to hear from anyone in their town assisting with the recovery efforts, or studying the effects of an event, not when it comes to discussing what is left of their homes and businesses, especially while piles of debris line the streets waiting to be cleared. Yet, as people begin to put their lives back together, the effects must be dealt with as well as those piles of debris.

Companies exist across the U.S. specializing in debris removal, and oftentimes, estimates of just how much debris there is to clear – and thus the amount those companies charge cities to clear it – is based on data provided solely by contractors.

Joseph Dannemiller, Larry Tanner and other researchers in the Debris Impact Facility at Texas Tech University are seeking to change the way volumes of debris are measured after a natural disaster.

TTU says that, using drones and high-powered computers, Dannemiller, an instructor in the Edward E. Whitacre Jr. College of Engineering and a doctoral candidate in the National Wind Institute, and his colleagues have developed an information-based model to better analyze and estimate the volume of debris. This can cut down the expense to cities on how much it will cost to have all the debris cleared, potentially saving millions of dollars.

"We decided to develop a volumetric sampling-based model where we would fly over a region, estimate the volume of debris in that region, then fly a different region and estimate the volume of debris in that region," Dannemiller said. "Then, the industries that have grown up and now specialize in recovery could, through some central entity like the Federal Emergency Management Agency, be allocated to various disaster regions based on need. Right now, the decision of how assets are allocated is information-driven, but it is based on word of mouth or qualitative assessments."

Dannemiller and his colleagues put their theory and model to the test this summer after Hurricane Harvey decimated the Texas Gulf Coast. The researchers spent several days in the region gathering aerial imagery and footage they then brought back to Texas Tech. The imagery, footage and ground assessment data were used to create this information-based approach to determine the cost of debris removal.

Even though researchers had other opportunities previously, Harvey proved to be the perfect event to test their theories and practices.

"We've used these methods in the past but we've never used them for disaster recovery," Dannemiller said. "Harvey was the right event because it was local and provided us the opportunity to travel a short distance, gather a large amount of data and validate our methodology so we could move to the next phase."

Measuring the devastation

Flying over a region hit by a natural disaster is nothing new. The problem is that hiring a pilot to fly over numerous disaster regions to gather information can be expensive. Not only do you have to pay to hire the pilot, but there also is the cost for use of the aircraft, the fuel and the expensive photography equipment used to take pictures from 10,000 to 20,000 feet.

Additionally, manned flights are extremely time-consuming. A pilot can fly over a large region but the aircraft is expensive to maintain. It can add up to thousands of dollars per flight hour.

While they can't fly as large a region as manned aircraft, drones can make more flights in the same time using photography equipment that provides much more accurate assessments than imagery provided from manned aircraft. Drones can also fly under any cloud cover that obstructs regions being photographed during manned flights.

When using drones, the only cost encumbered by the city or recovery entity is the time and services of the pilot. Also, multiple drones can be flown at the same time by multiple pilots instead of being reliant on just one pilot or one plane.

Drones also allow researchers to take time-lapse measurements of areas to study how quickly and efficiently the debris is being removed and how quickly the region can recover after a month, six months, a year or longer. All in all, it's a method of debris measurement that is immensely more cost-effective and efficient than using word of mouth from the ground and manned aircraft in the sky.

With that impetus, Dannemiller and others made the trek to South Texas to put their theories to the test. The first task was getting permission.

Helping the recovery effort

"We already had connections with emergency and disaster managers," Dannemiller said. "All we had to do was figure out what the right region was to fly. We decided on three different cities. We went down there and drove the areas to determine which one of the three was the best."

The Texas Tech researchers chose those regions hardest hit by Harvey in terms of wind damage, not so much surge damage or flooding. Once there, the researchers contacted the proper authorities in each city to discuss their plans. If there was a concern from authorities or residents about the drones flying in a certain area, the research team simply would not fly that area. Most times, though, everyone was fine with what the researchers were doing.

"That is one of the things that is really surprising and welcoming after most disasters," Dannemiller said. "If you show you are generally there to help, to make things better, people are very accommodating, open, and even willing to help us gather what we need so we can let them get back to the business of putting their lives back together."

The researchers also flew temporary landfills where removal companies dump debris in order to build baselines for comparison. Removal companies base their charges to cities on debris volumes and the number of days it takes to remove those volumes. This information is then provided to the cities with little to no verification from any other entity. Drones can fly all of those sites in a single day and provide volumetric estimates – usually about 12,000-15,000 cubic meters, to within 20 cubic meters.

"So, now we can look at the errors associated with the qualitative approach, provide a sampling based quantitative alternative, and the city can decide what they want to do to maximize their recovery efforts, per dollar," Dannemiller said.

Developing the model

With the imagery, footage and information in hand, Dannemiller and his fellow researchers returned to Lubbock to begin developing the model. But processing six to eight football fields worth of area takes time, even for the most sophisticated computer programs.

The goal, ultimately, was to dial in on how much debris was created in order to develop the most accurate, information-based model for debris removal. Researchers were not concerned, at least at this point in the process, with delineating the types of debris, just the volume. That is for future research.

"The numbers contractors provide have not been verified up to this point, so no one knows how much debris was truly there," Dannemiller said. "It is hard to believe, but, from a scientific perspective no one has ever embarked on trying to measure or validate this information."

Dannemiller said the model also will help determine how many homes and businesses were affected, how much deforestation occurred, and how much infrastructure was damaged. Another advantage to the drone flights is their ability to take pictures at various angles, providing a three-dimensional (3-D) perspective that exceeds the information provided by the traditional overhead pictures taken by manned aircraft that only look top down.

He said that with their model, they can begin giving debris regional volumetric estimates within two days.

"What we offer that a manned flight cannot is a 3-D model so disaster managers and city planners can assess the region from a different perspective, and anyone can look at where the debris is concentrated," Dannemiller said. "Near the coast you have a lot of structures that are built up, and debris gets caught underneath. A flight that goes straight overhead and points straight down can't see that, but we can. So, now, disaster managers can make decisions based on a three-dimensional perspective of whatever they ask need."

Eventually, Dannemiller said, the model will be available for every type of natural disaster, from hurricanes to tornadoes to wildfires, and any sort of naturally occurring wind event.

But the usefulness of the models and the drone flights won't stop there. While it's good to give cities and contractors more accurate estimates of the volume of debris, there is little like being able to view the devastation firsthand.

That is why Dannemiller and his fellow researchers are now developing a virtual reality environment using the same 3-D models, which would allow people to walk around in a disaster region to understand the extent of the damage beyond just pictures and video from television reports.

As an example, he said the team could map an area the size of the Texas Tech campus and develop the 3-D virtual reality model in about three days.

"Every building in the virtual environment would look like the actual building," Dannemiller said. "You would see the same trees, the benches, the parks, the monuments, the statues, the flagpoles. We aim to make it so people can walk through that world, and see the extent of the devastation."

Being able to see that devastation would not only give disaster planners a way to view debris, but it also would help them understand the totality of the disaster before they get there, so they are prepared and can offer assurances to families and business and avoid some of the colorful descriptions that tend to discourage those trying to pick up their lives in the wake.

Finally, a 3-D virtual reality model would be useful to policy makers and government agencies to show them not only the breadth of the destruction but, also, with subsequent flights, how quickly an area is recovering from the disaster.

"It is important to understand the societal and economic repercussions of pouring all this money into relief efforts. Where the money goes and where the people go is a very important part of understanding how we as a society should respond," Dannemiller said.

"We aim to deliver an educational tool that allows people with to learn from these disasters so everyone, be they policy makers, first responders, city personnel, government employees or any member of the public simply willing to help, can see what the devastation is like before they arrive and can then focus their efforts on supporting the people and helping them rebuild."

Cities with bad traffic may be more resilient to disruptive events

Source: http://www.homelandsecuritynewswire.com/dr20171222-cities-with-bad-traffic-may-be-more-resilient-to-disruptive-events

Dec 22 – New research by scientists at Northeastern University shows that cities with bad traffic under normal conditions may actually be more efficient at handling adverse events, like accidents and storms. Conversely, some cities with typically low traffic congestion become severely backed-up under the pressure of these disruptive scenarios.

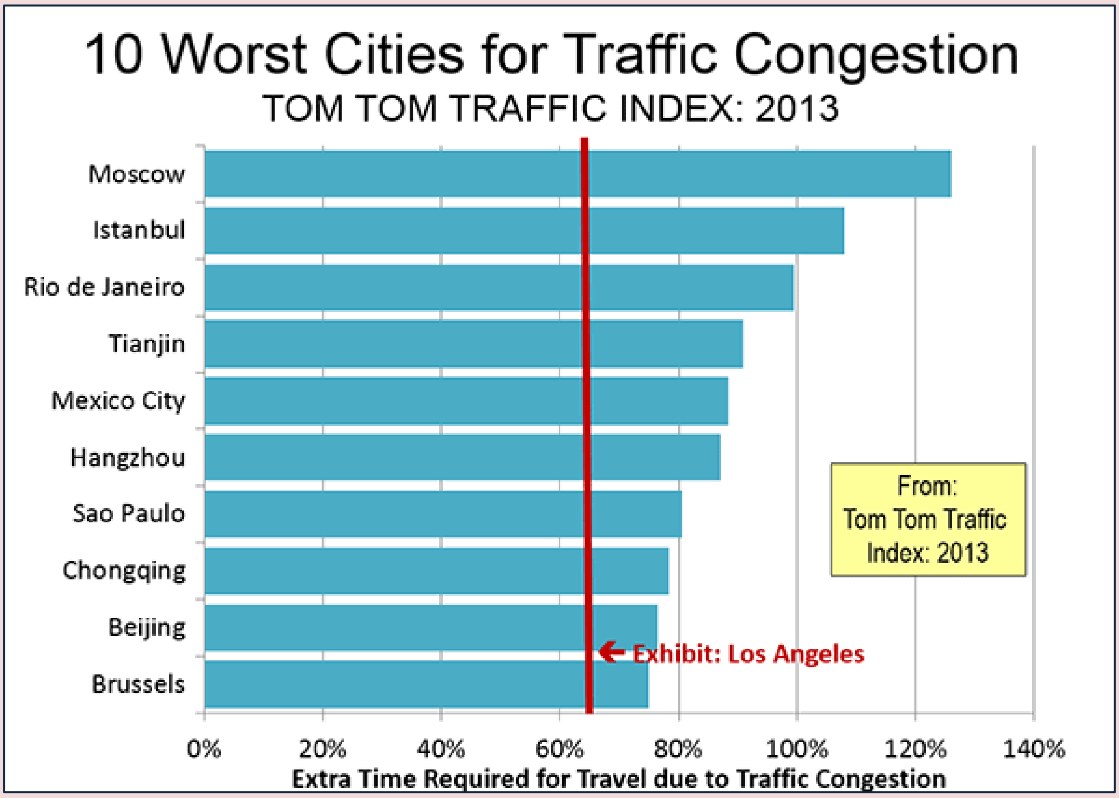
© Anil Sood / Twitter

In a paper published in the journal *Science Advances*, Maksim Kitsak, associate research scientist in the Department of Physics and Northeastern's Network Science Institute, and his colleagues examine the resilience and efficiency in city transportation systems. Northeastern notes that efficiency refers to the average time delay a commuter would face annually due to traffic. Resilience is the ability of road networks to absorb adverse events that fall outside normal daily traffic patterns.

The study, conducted in collaboration with the University of Virginia, Arizona State University, and the University of Massachusetts Boston, looked at road networks from 40 major U.S. cities.

"What we show is actually these two measures are not really correlated with each other," Kitsak said. "One would think that if the city is bad for traffic under normal conditions, it would be equally bad or worse for traffic under additional stress events, like severe weather. But we show that is not quite the case."

For example, the study found that the Los Angeles transportation network—while inefficient on a daily basis—doesn't suffer much from adverse events. The road systems are resilient. They function more or less the same regardless of unforeseen incidents.



Traffic in San Francisco is also typically inefficient. But unlike Los Angeles, San Francisco's transportation network is not resilient. "Even mild adverse events in San Francisco are likely to lead to substantial increases in traffic delays," Kitsak said.

Resilience was estimated as the change in efficiency resulting from roadway disruptions, the study says. And it was found to vary greatly between cities, with increased delays ranging from 9.5 percent in Los Angeles to 56 percent in San Francisco.

Why is the City of Angels more resilient than the City by the Bay? Kitsak said there are many factors that influence transportation resiliency, but one of the most important ones is the availability of backup roads. Los Angeles has many, while San Francisco does not. San Francisco also relies heavily on bridges, which separate the city from other parts of the Bay Area where many commuters live.

"If some of these bridges collapsed or were blocked due to traffic accidents, all of the sudden, traffic in the San Francisco area would become very inefficient," Kitsak said.

What about cities with relatively little traffic? The study shows that even efficient transportation systems can fail to be resilient. Look at Providence, Rhode Island, or Jacksonville, Florida. These cities aren't normally congested. But if something unexpected happens, traffic can increase significantly, Kitsak said.

On the flip side, some cities were found to be particularly resilient to adverse events, with Cleveland and Salt Lake City among the high achievers. Another project is currently underway to identify and quantify what other factors—besides availability of backup roads—make some cities more resilient than others, Kitsak said.

"Our study shows there is a difference in the way you need to plan for normal traffic versus disruptions that are rare, like heavy rain, flooding, or snow storms," said Igor Linkov, risk and decision science lead with the U.S. Army Engineer Research and Development Center and an author of the study. "With normal traffic, you need to focus on efficiency. For events like a big snowstorm or flood, you need to think about resilience."

The research findings are also important because until now, policy responses and investments to improve transportation networks have been based on normal traffic conditions, Kitsak explained.

"Very little attention is being paid to questions of how road networks would respond if there were some major events like construction, sports games, or very bad weather," Kitsak added. "We argue that both efficiency and resilience need to be taken into consideration."

— Read more in Alexander A. Ganin et al., "Resilience and efficiency in transportation networks," Science Advances 3, no. 12 (20 December 2017): e1701079

Hurricanes and earthquakes -- one may predict the other

Source: http://www.homelandsecuritynewswire.com/dr20180111-hurricanes-and-earthquakes-one-may-predict-the-other

Jan 11 – When three major hurricanes and just as many powerful earthquakes happen at around the same time, as they did in 2017, many wonder if they are connected. While the 2017 hurricanes and the earthquakes in Mexico are likely not connected, geophysicist Shimon Wdowinski believes there could be a correlation between hurricanes and the earthquakes that come much later.

Two things matter when bouncing back from natural disasters

Source: http://www.homelandsecuritynewswire.com/dr20180111-two-things-matter-when-bouncing-back-from-natural-disasters

Jan 11 – Disaster happens. But solid local leadership combined with the right outside partners can mitigate the fallout and save lives.

On 19 September 2017, an earthquake hit Mexico City that damaged and destroyed buildings across the city, killing more than 155 people.

After the earthquake, Miyamoto International, with the support of the U.S. Agency for International Development's Office of Foreign Disaster Assistance, assisted with the recovery efforts and helped local engineers complete structural assessments. The team from Miyamoto, led by Elizabeth Petheo, who heads the company's Washington, D.C. office, specializes in urban disaster and risk reduction and resiliency programs globally.

According to Petheo, who has worked in international development her entire career, there are two primary aspects of building disaster resiliency: It should be country-driven, and international actors can act as a catalyst for knowledge transfer.

Country-driven approach

"The national actors who are there, whether they are firefighters, first responders, or people working on disaster and emergency preparedness policy — they are the ones who drive the conversation," Petheo said.

This is because those are the people who know the area best, understand what capabilities their community already has, and what needs to be strengthened.

To prepare for a crisis, there are a number of questions that communities can ask themselves. "This is not an exhaustive list," Petheo said, "but there are a couple of different buckets: the logistical and operations side of things; overall administrative management of how things get executed; and the players themselves."

As far as logistics and operations goes, the local actors need to assess what kind of equipment they have. If a road is blocked, can they get through? If a building collapses, do they have the machines to clear the debris?

With management, they need to establish a control structure. Who will be able to activate policies that are in place? Who will be making the decisions? In terms of individual players, they need to know who else in their ecosystem will be responding to disasters, and how their specific work area impacts other areas.

According to Petheo, being ready to answer questions like these will make countries more efficient when responding to a crisis.

Transferring knowledge

The second part of developing resiliency in the face of a disaster is having international players acting as a catalyst. “This is central to the actual activities that you’re delivering,” Petheo said.

By spending time understanding a community and contextualizing its disaster response plans, outside players can help communities “understand links — how different actors who respond in a time of crisis can help and support each other,” Petheo said.

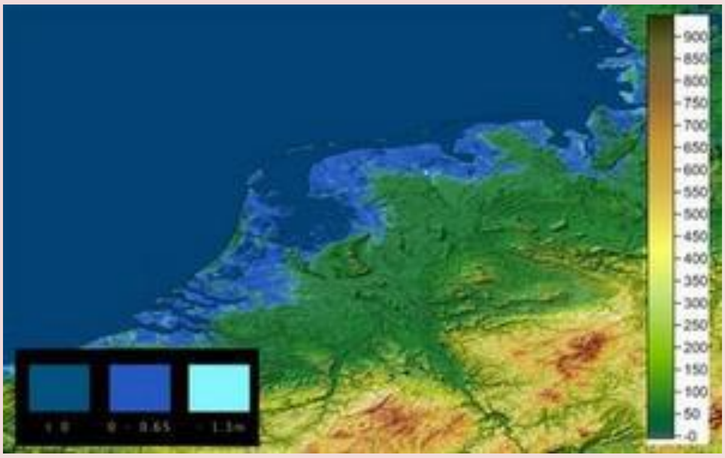
MIT notes that companies like Miyamoto play a role here. Miyamoto helps countries figure out what makes sense for them, rather than providing a step-by-step playbook. This includes, with its structural and engineering expertise, helping officials think through how someone locally with engineering experience could help a search and rescue team do its job better, among other things.

Miyamoto uses a data-driven approach to help local first responders understand what different scenarios would be if an earthquake did strike their area — running simulations that show how an earthquake would affect an area, including what buildings could collapse and estimating the number of people who could be displaced. They then help communities identify the gaps in their readiness and what areas could be strengthened. Assessing these scenarios lets first responders plan how to respond when disaster strikes.

To say that disasters, like earthquakes, are disruptive is an understatement — the entire community is upended at the same time. “There is the economic, societal, social, and individual impact that’s happening all at the same time, which is what makes these kinds of emergencies so complex,” Petheo said. But “the more you can think through what possible scenarios would be, what the situation that the community or government face would be, the better they are in coping when a crisis actually happens.”

Rising seas2017 saw the highest ever sea level on the Dutch coast

Source: http://www.homelandsecuritynewswire.com/dr20180115-2017-saw-the-highest-ever-sea-level-on-the-dutch-coast



Jan 15 – The average sea level measured on the Dutch coast was higher than ever before in 2017. The Dutch sea level, the averaged measurements from six tide stations, rose to 11 cm above Normal Amsterdam Water Level (NAP in Dutch). The last highest measurement was in 2007, when the average sea level was 9 cm above NAP. The fact that the sea level was higher last year does not mean that the sea level is now rising faster. At present, the sea level on the Dutch coast is rising by 20 cm every century.

Dubai Civil Defence to eradicate fire threat with nanotechnology

Source: https://www.thenational.ae/uae/government/dubai-civil-defence-to-eradicate-fire-threat-with-nanotechnology-1.695975

Jan 16 – Fires across Dubai will soon be a thing of the past, according to the emirate’s Civil Defence who are working on implementing nanotechnology in commercial buildings to prevent disasters.

Brig. Rashid Khalifa Buflasa, director general for fire and rescue at Dubai Civil Defence, speaks at the Intersec 2018 press conference. Navin Khianey / The National

Speaking at a press conference on the details of the Intersec event, which kicks off in Dubai next week, Brig. Rashid Buflasa, director – general assistant for fire and rescue at the Dubai Civil Defence, said he hoped their new technology would be implemented in time for Expo 2020.

The technology is based around a material that is comprised of a solid layer with moisture built inside so when the solid begins to melt in heat, it produces water vapour.

The device will work by stifling the three elements needed to ignite a fire: heat, fuel and oxygen.

He said: “According to our statistics, most fires are electric, like short circuits and poor connections … We’ll fix the nanotechnology inside the sockets, starting with commercial buildings like malls and warehouses, and eventually we’ll go in to residential buildings.”

Brig. Buflasa also said upgrading the police force’s equipment was key to fighting crime and to preserve homeland security, adding that “the private sector will play a major role in providing us with latest tools in the field.”

The Security Industry Regulatory Authority (Sira) told press conference attendees that it is to strengthen the level of its security guards across the country.

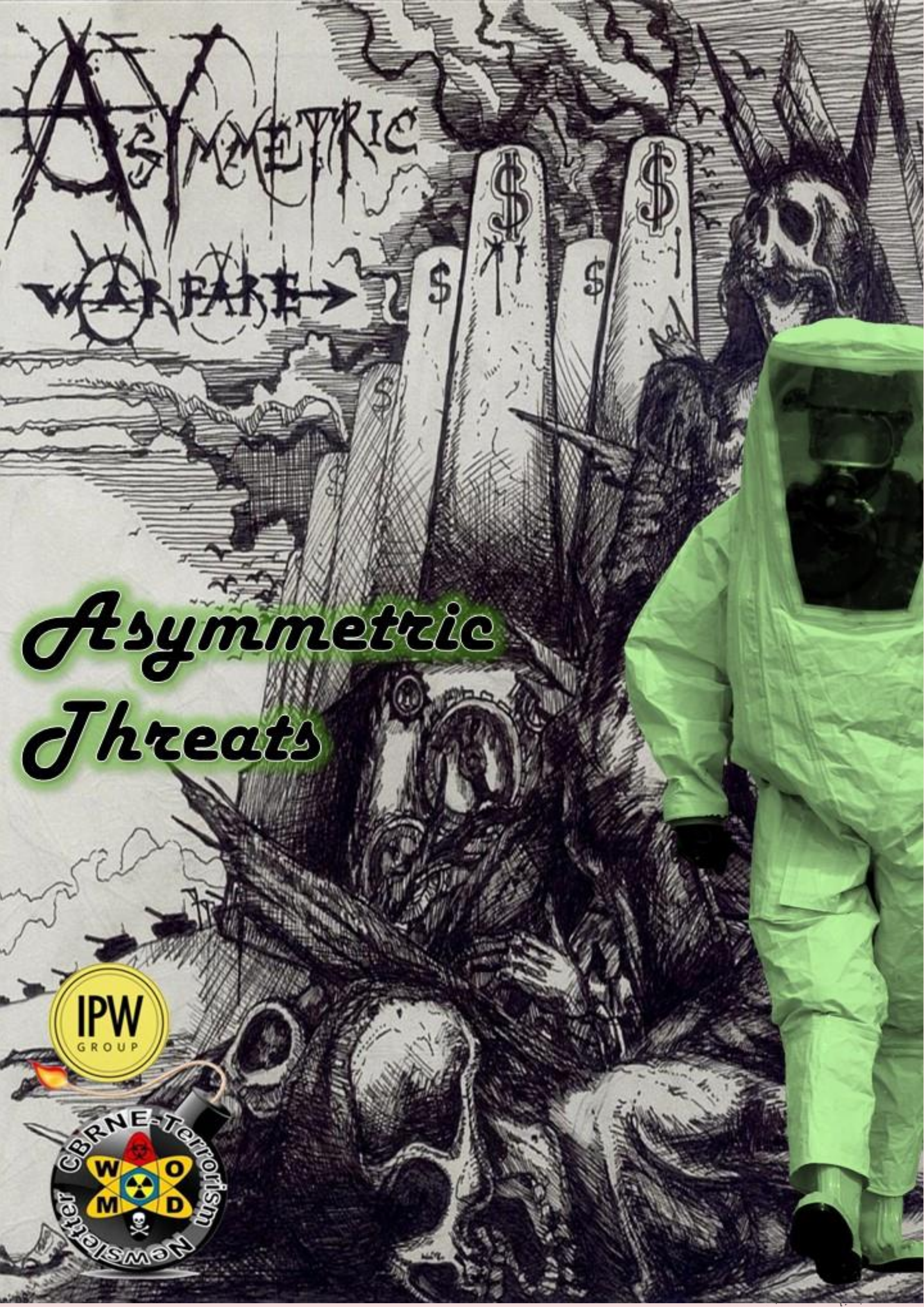
“We will improve both our manpower and our devices,” said Khalifah Al Sulais, Sira’s chief executive. “Dubai has a reputation for being one of the safest places in the world and we intend to keep it that way.”

The security market in the Middle East has evolved drastically over the last 20 years, growing from US$52 million in 1998 to $12.2 bn in 2017. Its focus has shifted from simpler technologies such as pedestrian barriers, turnstiles, conventional access control systems and traditional surveillance cameras to more sophisticated technologies such as sensor-based cameras, automated traffic bollards and biometric access control systems.

Speakers at the press conference said video surveillance will be one of the largest areas of growth in the Middle East in both the homeland and commercial security markets. New evolving security trends will see a rise in security drones, smart storage solutions, artificial intelligence and T-rays, also known as terahertz, a safe form of electromagnetic radiation that is able to detect harmful gases or dangerous materials, and has potential uses in airport security.

Intersec will take place in Dubai next week from January 21 to January 23.

Asymmetric Threats



Hotter temperatures will accelerate asylum-seekers migration to Europe

Source: http://www.homelandsecuritynewswire.com/dr20171229-hotter-temperatures-will-accelerate-asylumseekers-migration-to-europe

Dec 29 – New research predicts that migrants applying for asylum in the European Union will nearly triple over the average of the last fifteen years by 2100 if carbon emissions continue on their current path. The study suggests that cutting emissions could partially stem the tide, but even under an optimistic scenario, Europe could see asylum applications rise by at least a quarter. The study appears today in the journal *Science*.

"Europe is already conflicted about how many refugees to admit," said the study's senior author, Wolfram Schlenker, an economist at Columbia University's School of International and Public Affairs (SIPA) and a professor at the university's Earth Institute. "Though poorer countries in hotter regions are most vulnerable to climate change, our findings highlight the extent to which countries are interlinked, and Europe will see increasing numbers of desperate people fleeing their home countries."

Schlenker and study coauthor Anouch Missirian, a Ph.D. candidate at SIPA, compared asylum applications to the EU filed from 103 countries between 2000 and 2014, with temperature variations in the applicants' home countries. They found that the more temperatures over each country's agricultural region deviated from 20 degrees Celsius (68 degrees Fahrenheit) during its growing season, the more likely people were to seek refuge abroad. Crops grow best at an average temperature of 20 degrees C, and so not surprisingly, hotter than normal temperatures increased asylum applications in hotter places, such as Iraq and Pakistan, and lowered them in colder places such as Serbia and Peru.

Combining the asylum-application data with projections of future warming, the researchers found that an increase of average global temperatures of 1.8 °C — an optimistic scenario in which carbon emissions flatten globally in the next few decades and then decline — would increase applications by 28 percent by 2100, translating into 98,000 extra applications to the EU each year. If carbon emissions continue on their current trajectory, with global temperatures rising by 2.6 C to 4.8°C by 2100, applications could increase by 188 percent, leading to an extra 660,000 applications filed each year.

Under the landmark climate deal struck in Paris in 2015, most of the world's nations agreed to cut carbon emissions to limit warming by 2100 to 2°C above pre-industrial levels. President Trump's recent decision to withdraw the United States, the world's second largest carbon emitter, from the accord now jeopardizes that goal.

Columbia notes that in a further setback to reducing U.S. carbon emissions, the U.S Environmental Protection Agency has proposed lowering the U.S. government's "social cost" of carbon, or the estimated cost of sea-level rise, lower crop yields, and other climate-change related economic damages, from $42 per ton by 2020 to a low of $1 per ton. The EPA partly arrived at the lower figure by excluding the cost of U.S. emissions on other countries, yet as the study shows, effects in developing countries have clear spillovers on developed countries. "In the end, a failure to plan adequately for climate change by taking the full cost of carbon dioxide emissions into account will prove far more costly," said Missirian, a fourth-year sustainable development major.

The research adds to a growing body of evidence that weather shocks can destabilize societies, stoke conflict and force people to flee their home countries. In a widely-cited 2011 study in *Nature*, a team of researchers led by Solomon Hsiang, then a graduate student at SIPA, linked modern El Niño drought cycles to increased violence and war globally.

More recently, researchers have highlighted the connection between the drying of the Middle East and ongoing conflict there. In a 2015 study in the *Proceedings of the National Academy of Sciences*, another team of Columbia researchers made the case that climate change made Syria's 2006-2010 drought two to three times more likely, and that the drought was a catalyst for Syria's 2011 uprising. The civil war that followed has so far claimed 500,000 lives, by one estimate, and forced 5.4 million Syrians to flee the country.

Germany has taken in the largest share of asylum-seekers from Syria and elsewhere, but increasingly faces a backlash from German voters worried about assimilation and loss of jobs. A wave of anti-immigrant sentiment elsewhere in Europe has led to Hungary building a wall to keep refugees out and influenced Great Britain's decision to leave the European

Union. In the United States, President Trump was elected in part on his promise to build a wall to block Mexican immigrants from entering the country illegally.

Hsiang, now an economics professor at the University of California, Berkeley, who was not involved in the research, called the study an "incredibly important" wakeup call. "We will need to build new institutions and systems to manage this steady flow of asylum seekers," he said. "As we have seen from recent experience in Europe, there are tremendous costs, both for refugees and their hosts, when we are caught flat footed. We should plan ahead and prepare."

Colin Kelley, a climate scientist at Columbia's International Research Institute for Climate and Society who linked climate change to Syria's ongoing conflict, also praised the research. "It's unclear how much more warming will occur between now and the end of the century, but the study clearly demonstrates just how much climate change acts as a threat multiplier. Wealthier countries can expect to feel the direct and indirect effects of weather shocks from manmade climate change in poorer, less resilient countries."

The research was initiated at the request of the European Commission's Joint Research Centre (JRC), which also provided funding. "These findings will be especially important to policymakers since they show that climate impacts can go beyond the borders of a single country by possibly driving higher migration flows," said Juan-Carlos Ciscar, a senior expert at the JRC's Economics of Climate Change, Energy and Transport Unit. "Further research should look at ways for developing countries to adapt their agricultural practices to climate change."

— Read more in A. Missirian el al., "Asylum applications respond to temperature fluctuations," Science 358, no. 6370 (22 December 2017): 1610-14.

Billion-dollar weather and climate disasters on the rise

Source: http://www.homelandsecuritynewswire.com/dr20171229-billiondollar-weather-and-climate-disasters-on-the-rise

Dec 29 – The National Centers for Environmental Information (NCEI) is the Nation's Scorekeeper in terms of addressing severe weather and climate events in their historical perspective. As part of its responsibility of monitoring and assessing the climate, NCEI tracks and evaluates climate events in the United States and globally, which have great economic and societal impacts. NCEI is frequently called upon to provide summaries of global and U.S. temperature and precipitation trends, extremes, and comparisons in their historical perspective

NOAA says that from 1980 to 2017, the United States has sustained 218 weather and climate disasters in which overall damages/costs reached or exceeded $1 billion (including CPI adjustment to 2017). The total cost of these 218 events exceeds $1.2 trillion.

This total does not yet include the costs for Hurricanes Harvey, Irma and Maria, which are being assessed and will be included in the NCEI's fourth quarter release.

2017 in progress…

In 2017 (as of 6 October), there have been fifteen weather and climate disaster events with losses exceeding $1 billion each across the United States. These events included 1 drought event, 2 flooding events, 1 freeze event, 7 severe storm events, 3 tropical cyclone events, and 1 wildfire event. Overall, these events resulted in the deaths of 282 people and had significant economic effects on the areas impacted. The 1980–2016 annual average is 5.5 events (CPI-adjusted); the annual average for the most recent 5 years (2012–2016) is 10.6 events (CPI-adjusted).

For the first nine months (Jan-Sept) of 2017, the United States has experienced fifteen separate billion-dollar weather and climate disasters. 2017 ties the record year of 2011 for the most (15) billion-dollar disasters for the year to date. The record number of billion-dollar disasters for an entire calendar year is 16 events set in 2011. The 2017 events include two floods, a freeze, seven severe storms, three tropical cyclones, a drought and wildfire - collectively causing 282 fatalities.

Methodology and data sources

In 2012, NCEI — then known as National Climatic Data Center (NCDC) — reviewed its methodology on how it develops Billion-dollar Disasters. NCEI held a workshop with economic experts (May 2012) and worked with a consulting partner to examine possible inaccuracy and biases in the data sources and methodology used in developing the loss assessments (mid-2013). This ensures more consistency with the numbers NCEI provides on a yearly basis and give more confidence in the year-to-year comparison of information. Another outcome is a published peer-reviewed article "U.S. Billion-dollar Weather and Climate Disasters: Data Sources, Trends, Accuracy and Biases" (Smith and Katz, 2013). This research found the net effect of all biases appears to be an underestimation of average loss. In particular, it is shown that the factor approach can result in an underestimation of average loss of approximately 10–15 percent. This bias was corrected during a reanalysis of the loss data to reflect new loss totals.

It is also known that the uncertainty of loss estimates differs by disaster event type reflecting the quality and completeness of the data sources used in our loss estimation. In 2016, six of the fifteen billion-dollar events (that is, the four inland flooding events, drought and Hurricane Matthew) have higher potential uncertainty values around the loss estimates due to less coverage of insured assets. The remaining nine events (that is, eight severe storm events and wildfire) have lower potential uncertainty surrounding their estimate due to more complete insurance coverage. NCEI's newest research defines the cost uncertainty using confidence intervals as discussed in the peer-reviewed article "Quantifying Uncertainty and Variable Sensitivity within the U.S. Billion-dollar Weather and Climate Disaster Cost Estimates" (Smith and Matthews, 2015). This research is a next step to enhance the value and usability of estimated disaster costs given data limitations and inherent complexities.

In performing these disaster cost assessments these statistics were taken from a wide variety of sources and represent, to the best of NCEI ability, the estimated total costs of these events — that is, the costs in terms of dollars that would not have been incurred had the event not taken place. Insured and uninsured losses are included in damage estimates. Sources include the National Weather Service, the Federal Emergency Management Agency, U.S. Department of Agriculture, National Interagency Fire Center, U.S. Army Corps, individual state emergency management agencies, state and regional climate centers, media reports, and insurance industry estimates.

▶▶ **More information can be found in** Calculating the Cost of Weather and Climate Disasters.

— Read more in Adam B. Smith and Jessica L. Matthews, "Quantifying Uncertainty and Variable Sensitivity within the U.S. Billion-dollar Weather and Climate Disaster Cost Estimates," Natural Hazards 77, no. 3 (July 2015): 1829-51 (DOI: 10.1007/s11069-015-1678-x); Adam B. Smith and Richard W. Katz, "U.S. Billion-dollar Weather and Climate Disasters: Data Sources, Trends, Accuracy and Biases," Natural Hazards 67, no. 2 (June 2013): 387-410 (DOI: 10.1007/s11069-013-0566-5); Neal Lott and Tom Ross, "Tracking and evaluating U. S. billion dollar weather disasters, 1980-2005," AMS Forum: Environmental Risk and Impacts on Society: Successes and Challenges, Atlanta, Georgia, American Meteorological Society, 1.2.; and Tom Ross and Neal Lott, 2003: A Climatology of 1980-2003 Extreme Weather and Climate Events, Technical Report (National Climatic Data Center, NOAA/NESDIS, December 2003).

Transboundary River Basins and Political Tensions," Sustainable Security (13 July 2017).

IPW GROUP
CBRNE-Terrorism Newsletter
W O M D
VITALY'S
OPEN FOR BUSINESS AS USUAL
Business Interruption
Disaster Event
Business Continuity

US sets out preparedness strategy for CBRNE threats

Source: http://www.continuitycentral.com/news05901.html

According to a new document, the ‘National Strategy for CBRNE Standards’ released by the US Office of Science and Technology Policy (OSTP), chemical, biological, radiological, nuclear, and explosives (CBRNE) agents remain a grave threat to the US.

The National Strategy for CBRNE Standards lays out a federal vision for the coordination, prioritization, establishment, and implementation of CBRNE equipment standards by 2020. The Strategy describes the elements of a standards and testing infrastructure needed to counter CBRNE threats, including an integrated standards development approach that spans performance, interoperability, testing and evaluation, conformity assessment, operating procedures, training, and certification.

Specifically, the Strategy outlines six goals to achieve technical performance and interoperability of CBRNE technology, equipment deployment, and effective user training:

1. Establish an interagency group for CBRNE standards to promote the coordination of these standards among federal, state, local, and tribal communities;
2. Coordinate and facilitate the development of CBRNE equipment performance standards and promote the use of standards for federal, state, local, and tribal communities;
3. Coordinate and facilitate the development and adoption of interoperability standards for CBRNE equipment;
4. Promote enduring CBRNE standard operating procedures for federal, state, local, and tribal use to improve National preparedness and response;
5. Establish voluntary CBRNE training and certification standards for the federal, state, local, and tribal communities and promote policies that foster their adoption;
6. Establish a comprehensive CBRNE equipment testing and evaluation (T&E) infrastructure and capability to support conformity assessment standards.

Released by the OSTP in collaboration with the US Department of Homeland Security (DHS) and US Department of Commerce (DOC), the Strategy was created by the Cabinet-level National Science and Technology Council (NSTC), which coordinates interagency science and technology policies within the Executive Branch.