Dedicated to Global First Responders

CBRNE NEWSLETTER TERRORISM

April 2018

www.cbrne-terrorism-newsletter.com

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

DIRTY R-NEWS

White House has secret 5-story-deep doomsday bunker: Book

By Steven Nelson

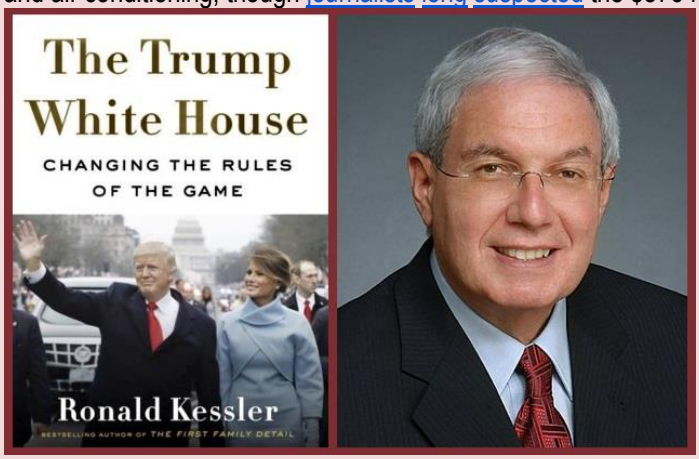
Source: https://www.washingtonexaminer.com/news/white-house/white-house-has-secret-5-story-deep-doomsday-bunker-book

Apr 02 – **A new book says the White House has a massive secret bunker beneath its north lawn for doomsday scenarios, while staffers battle a more immediate menace — insects — with pressurized salt guns.**

The bunker, built during former President Barack Obama's administration, was toured by members of President Trump's staff last year, author Ronald Kessler wrote in *The Trump White House: Changing the Rules of the Game*, which was released Monday.

Kessler, a former Washington Post reporter and author of several books on the Secret Service and national security, wrote that the facility is large enough to fit the White House workforce indefinitely.

A large north-lawn construction project began in 2010, officially to improve White House electrical wiring and air conditioning, though journalists long suspected the $376 million project involved a bunker.



The White House already had a bunker, under the East Wing, called the Presidential Emergency Operations Center, where Vice President Dick Cheney and other senior officials hid during the 9/11 terrorist attacks. The new facility is much larger, Kessler wrote.

"At least five stories deep, the bunker, which was completed near the end of Obama's tenure, can house the staff of the entire West Wing indefinitely in the event of a weapons of mass destruction attack," Kessler wrote. "After Trump became president, top staffers toured the bunker, whose existence is classified."

A spokesperson for the Secret Service declined to comment on the bunker's existence, or Kessler's reporting that the Secret Service is actively surveiling approximately 100 people deemed to have uttered serious "Class III" threats against Trump.

Kessler wrote that Trump has received about as many threats each day — between six and eight — as did Presidents Obama and George W. Bush.

Most threats are deemed "Class II" — made by incarcerated or institutionalized people without the means to make good on their threats — or less-serious "Class I" threats, which may be uttered drunkenly or otherwise without intended action.

"For operational security purposes the Secret Service does not comment on specific White House security measures or protective intelligence matters," said Secret Service spokesman Mason Brayman.

Kessler interviewed Trump, members of his family, and many current and former White House officials for his book, which also reports that the president himself often is an anonymous quotes "senior White House official" in news reports.

Although prepared for a nuclear winter, Kessler wrote that White House staff struggle with a more pressing fight, against flies, with salt-powered guns.

Kessler wrote that a widely reported news story last year about Trump ordering then-chief of staff Reince Priebus to swat a fly was untrue.

"The story had its origin in the fact that the West Wing, built on a swamp, is beset by flies. Trump hates flies. Staffers use air-pressured salt guns called Bug-a-Salt to kill them. Priebus was attacking an especially annoying fly in the Oval Office when Trump said jokingly, 'Kill it! Kill it!'"

***Steven Nelson** joined the Washington Examiner as a White House reporter after five years at U.S. News & World Report. He attended the College of William and Mary and lives in Washington, D.C.*

Hollywood Has No Idea How Nukes Work

Source: https://www.popularmechanics.com/culture/movies/a19600925/hollywood-nuclear-weapons/

Apr 02 – Nothing offers more drama than the ticking countdown to a devastating bomb, and the bigger the bomb, the bigger the thrills. That's why nuclear weapons often show up in cinema as the ultimate threat to our heroes—and humanity.

You wouldn't expect the movies to depict nuclear weapons with perfect realism, but some blockbusters do a much better job than others. Here's a guide that separates the good from the useless when it comes to fictional treatments of nukes.

The Avengers

At the end of *The Avengers*, some brutally pragmatic big brother types have ordered an F-35 warplane pilot to launch a nuclear-tipped missile at New York City to halt an alien invasion. Iron Man, knowing there's a less pyrrhic victory at hand, races to stop it.

To give the filmmakers credit, people tend to forget the F-35 is rated to carry nuclear weapons. But the warplane shown in the film is an F-35B operated by the U.S. Marine Corps, seen in a jumpjet configuration. In reality only the F-35A, the Air Force variant, carries nukes. Forgivable, but there's more nitpicking to come.

The F-35A is equipped to carry the B-61 nuclear gravity bomb, but that's not what's in the movie. As the name implies, gravity bombs drop and are guided by fins. *The Avengers* shows a nuclear cruise missile and the Pentagon's mainstay in that department is the AGM-86. The problem is that this bomb doesn't fit on an F-35. It's so large that only the huge B-52 Stratofortress bomber can carry these weapons.

Maybe we're seeing something new. The U.S. military is designing the Long Range Standoff Weapon, which will carry a nuke and load into an F-35. The LSRO would work here, but the filmmakers make an unfortunate error.

A close look at Iron Man's helmet display identifies the missile as a "AGM-154 Joint Stand Off Weapon." However, the JSOW doesn't carry a nuclear warhead. Against ships and armored vehicles, it's a good precision weapon, but for bringing mass destruction against inter-dimensional invaders, it sucks.

Also, Iron Man's high-speed grapple with this weapon wouldn't happen like it does on screen. The AGM-154 is a glide bomb, not a cruise missile. These weapons have wings but no engines, and what Iron Man chases, grabs, and grapples with in the film has a tongue of flame roaring behind it. But maybe the special effects designers had the experimental Extended Range version in mind. Raytheon did strap on an engine to the glide bomb and tested this JSOW-

ER (left) in 2008. The Navy took renewed interest in the program in 2017. Perhaps S.H.E.I.L.D could have adopted the concept as well?
Even accepting this long-shot loophole, the scene still doesn't work. The extended-range JSOW cruises at subsonic speeds rather than racing toward targets like an air-to-air missile. Here's what the extended range JSOW looks like. It's a cool design, but not anything that's too fast for Iron Man to handle.
Grade: B-

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

Preventing a Dirty Bomb: Resources for Hospitals

Source: http://www.nti.org/analysis/articles/preventing-dirty-bomb-resources-hospitals/

Feb 22 – **Hospitals around the United States—and around the world—are addressing security, safety and liability concerns by replacing blood irradiators that use cesium-137 with FDA-approved x-ray technology.** NTI provides resources to prepare you to join them, with answers to technical questions and information on how to get financial support to take this important step.
Why Take This Step?
The ingredients for a radiological "dirty bomb" – among them, the same isotopes that make life saving blood transfusions and cancer treatments possible – are located at thousands of sites in more than 150 countries.

Experts believe that the probability of a terrorist detonating a dirty bomb is much higher than that of an improvised nuclear weapon. Radical terrorist organizations such as the Islamic State have said they are looking to acquire and use radioactive material in a dirty bomb.
A radioactive dirty bomb could cause billions of dollars of damage due to the costs of evacuation, relocation, and cleanup. A dirty bomb that intentionally spreads cesium-137, a common isotope found in blood irradiators, would have the most devastating consequences.

Join New York and California to Eliminate Threats
In October 2017, the New York City Department of Health and Mental Hygiene announced **a first-of-its-kind,** innovative program to replace high-activity radiological sources with effective alternative equipment at hospitals, medical facilities and blood banks throughout New York City. NTI was a partner in this effort that also included the New York City Department of Health and Mental Hygiene, Mount Sinai Health System and the U.S. Department of Energy.
We've also helped organize workshops in California, with the State of California to devise strategies to secure and/or replace high-activity radiological sources that could be stolen and used to build radioactive "dirty bombs."
Emory University Hospital received the "Medical Innovation Award" at the Nuclear Industry Summit for its efforts to help reduce radiological threats.

These hospitals and city and state agencies have recognized the importance of taking this step for their safety, security and liability.

Safe and Effective Alternatives

In 2012, the U.S. Food and Drug Administration approved the use of non-radioactive x-ray devices for sterilizing blood that provide the same medical outcomes as cesium-137 blood irradiators. As of 2015, two types of these devices are available with a typical cost of approximately $270,000 per unit.

The x-ray units require far less security and shielding, eliminate liability, and do not require expensive disposal at the end of the machine's life-cycle.

Replacement to x-ray technology also protects hospitals that don't have insurance to cover terrorism losses; otherwise, there is a possibility of financial devastation from having to pay huge damages in the wake of a dirty bomb attack using hospital materials.

A Department of Energy (DoE) cost-sharing incentive program, the Cesium Irradiator Replacement Project (CIRP) - encourages the move away from cesium-137 irradiators.

EDITOR'S COMMENT: New York is not the first! France and Norway have already replaced all their irradiators, and Japan — additionally cautious due to the Fukushima nuclear disaster — has reduced its supply of irradiators by up to 80 percent.

▶▶ Read also (and cry) this GAO report: https://www.gao.gov/assets/650/647931.pdf

Going Underground: The Radioactive Market is Resurging

By Andy Oppenheimer

Source: https://www.cbrneportal.com/going-underground-the-radioactive-market-is-resurging/

Apr 04 – Since 'R' for 'radiological' was added to the unholy trinity of nuclear-biological-chemical weapons to create the acronym CBRN, smuggling of radioisotopes has been consistently placed high on the list of terrorist threats. The possibility that a well-funded group could acquire the materials to fashion a radiological dispersal device (RDD) or otherwise cause a radioactive dispersal event (RDE) has featured in many reports from government departments, institutes and expert bodies.

While radioisotopes in civilian use could be purloined or acquired through criminal gangs, the fabrication and emplacement of a RDD has long been deemed too risky to complete even for a suicide bombing mission. Therefore, there are few examples of RDDs.

But, coinciding with the rise of ISIS, radiological smuggling has resurged. On 18 March, police detained four men in the Turkish capital Ankara for possession of californium, a radioisotope produced in US and Russian laboratories and nuclear reactors. With a half-life of 2.6 years, it is used mainly in nuclear warheads, nuclear power plants, and the oil and mining industries, and is

worth $4 million per gram. The 1kg 441 g found in the suspects' vehicle was intended for sale to unnamed buyers for $72 million.
Other incidents may involve accidental theft. In December 2013, an armed gang stole a truck being hauled to a waste facility by Mexican authorities, who had parked it a petrol station. It was filled with obsolete medical equipment containing cobalt-60 – which was found about a kilometre from the truck and its empty protective lead container somewhere near Mexico City. Radioactivity was detected in the nearby town of Hueypoxtla.

Radioisotopes for Bombs
The components for a RDD are the very same isotopes used to save, not take lives are used in cancer radiotherapy as well as in industry and mining. Cesium-137 (half-life, 30 years) and cobalt-60 (5.2 years) for medicine are among the most commonly used – produced in nuclear reactors. They are tissue-penetrating gamma emitters, so if not shielded, handling and moving even small amounts would cause injury or death. As civilian-use radioisotopes they are installed, and discarded, in thousands of sites in more than 150 countries. Many are poorly secured and vulnerable to theft or loss.

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

*<u>**Andy Oppenheimer**</u> AIExpE MIABTI is Editor-in-Chief of CBNW (Chemical, Biological & Nuclear Warfare) and CBNW Xplosive journals, a consultant in CBRNE and counter-terrorism, and author of IRA: The Bombs and the Bullets (Irish Academic Press, 2008).*

STOP! Who goes where?

By Dr. Ram Athavale
Source: https://www.cbrneportal.com/stop_who_goes_there/

Tajikistan – Afghanistan border crossing on river Pyanj.

Managing National Borders is a complex mechanism. Various agencies from Armed Forces, Police, Coast Guard, Paramilitary forces and Customs are engaged in securing the borders. Optimal management of movement of personnel and goods across borders within agreed upon protocols and treaties is necessary to maintain sovereign integrity, safety and security.

CBRN material can be and is being transported across land, air and sea frontiers on daily basis. There is a need to institute specific measures to ensure only permitted and valid goods are entering your borders. In addition, there is a need to ensure prevention of unwanted entry and respond effectively to incidents of CBRN nature.

International Protocols and Obligations

Most nations are signatories to a range of international protocols, treaties and organisations that mandate strict monitoring and control of CBRN material. The important ones are :

- UN Security Council Resolution 1540 mandates all member states to
  - adopt measures that criminalize WMD proliferation;
  - enact effective export and other controls (including financial, transit, transshipment and brokering controls);
  - and secure sensitive materials.
- Basel Convention on the Control of Transboundary Movements of Hazardous Wastes and their Disposal.
- WCO Strategic Trade Control Implementation Guidelines.
- The Rotterdam Convention (formally, the Rotterdam Convention on the Prior Informed Consent Procedure for Certain Hazardous Chemicals and Pesticides in International Trade) is a multilateral treaty to promote shared responsibilities in relation to importation of hazardous chemicals
- Convention on the Physical Protection of Nuclear Material (CPPNM).
- International Convention on the Suppression of Acts of Nuclear Terrorism.
- The Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (Chemical Weapons Convention CWC).
- The Stockholm Convention on Persistent Organic Pollutants
- United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances

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

*<u>**Dr. Ram Athavale**</u> has been a key advisor to the Government of India on CBRN Security and Incident Management, and is now deployed as a key CBRN Expert for On-Site Technical Assistance to the EU CBRN Risk Mitigation Centres of Excellence Regional Secretariat in Nairobi Kenya.*

FDA Approves New Treatment for Acute Radiation Syndrome Adding to the Country's Available Treatments in the Event of Radiological or Nuclear Emergency

Source: https://www.domesticpreparedness.com/updates/fda-approves-new-treatment-for-acute-radiation-syndrome-adding-to-the-countrys-available-treatments-in-the-event-of/

On March 29, 2018, the FDA approved use of **Leukine (sargramostim)** to increase survival in adult and pediatric patients acutely exposed to myelosuppressive doses of radiation (Hematopoietic Syndrome of Acute Radiation Syndrome, or H-ARS).

Myelosuppression occurs when radiation damages the bone marrow. Suppression of the bone marrow blocks the production of blood cells. Leukine can help patients with H-ARS by facilitating recovery of bone marrow cells that develop into white blood cells that help fight off infections.

Leukine was shown to increase survival when administered up to 48 hours after total body

irradiation exposure at doses expected to be fatal to 50% of those exposed subjects under conditions of minimal supportive care.

Leukine is the third FDA-approved medical countermeasure (MCM) that is indicated to increase survival in patients exposed to myelosuppressive doses of radiation. It was approved by FDA based on efficacy studies in animals (under the Animal Rule), as efficacy studies in humans could not be ethically conducted. Leukine was originally approved in 1991 and was originally indicated to shorten time to neutrophil recovery and to reduce the incidence of severe and life-threatening infections following induction chemotherapy in adult patients 55 years and older with acute myeloid leukemia (AML), and subsequently approved for several oncology-related indications.

The most commonly reported side effects associated with Leukine injections are fever, injection site reactions, and shortness of breath.

Other products from a similar pharmacological class and approved for the same indication are:

- Neupogen (March 2015)
- Neulasta (November 2015)

What if a nuke goes off in Washington, D.C.? Simulations of artificial societies help planners cope with the unthinkable

By M. Mitchell Waldrop

Source: http://www.sciencemag.org/news/2018/04/what-if-nuke-goes-washington-dc-simulations-artificial-societies-help-planners-cope

Apr 12 – At 11:15 on a Monday morning in May, an ordinary looking delivery van rolls into the intersection of 16th and K streets NW in downtown Washington, D.C., just a few blocks north of the White House. Inside, suicide bombers trip a switch.

Instantly, most of a city block vanishes in a nuclear fireball two-thirds the size of the one that engulfed Hiroshima, Japan. Powered by **5 kilograms of highly enriched uranium** that terrorists had hijacked weeks earlier, the blast smashes buildings for at least a kilometer in every direction and leaves hundreds of thousands of people dead or dying in the ruins. **An electromagnetic pulse fries cellphones within 5 kilometers**, and the power grid across much of the city goes dark. Winds shear the bomb's mushroom cloud into a plume of radioactive fallout that drifts eastward into the Maryland suburbs. Roads quickly become jammed with people on the move—some trying to flee the area, but many more looking for missing family members or seeking medical help.

It's all make-believe, of course—but with deadly serious purpose. Known as National Planning Scenario 1 (**NPS1**), that nuclear attack story line originated in the 1950s as a kind of war game, a safe way for national security officials and emergency managers to test their response plans before having to face the real thing.

Sixty years later, officials are still reckoning with the consequences of a nuclear catastrophe in regular NPS1 exercises. Only now, instead of following fixed story lines and predictions assembled ahead of time, they are using computers to play what-if with an entire artificial society: an advanced type of computer simulation called an agent-based model.

Today's version of the NPS1 model includes a digital simulation of every building in the area affected by the bomb, as well as every road, power line, hospital, and even cell tower. The model includes weather data to simulate the fallout plume. And the scenario is peopled with some 730,000 agents—a synthetic population statistically identical to the real population of the affected area in factors such as age, sex, and occupation. Each agent is an autonomous subroutine that responds in reasonably human ways to other agents and the evolving disaster by switching among multiple modes of behavior—for example, panic, flight, and efforts to find family members.

The point of such models is to avoid describing human affairs from the top down with fixed equations, as is traditionally done in such fields as economics and epidemiology. Instead, outcomes such as a financial crash or the spread of a disease emerge from the bottom up, through the interactions of many individuals, leading to a real-world richness and spontaneity that is otherwise hard to simulate.

That kind of detail is exactly what emergency managers need, says Christopher Barrett, a computer scientist who directs the Biocomplexity Institute at Virginia Polytechnic Institute

and State University (Virginia Tech) in Blacksburg, which developed the NPS1 model for the government. The NPS1 model can warn managers, for example, that a power failure at point X might well lead to a surprise traffic jam at point Y. If they decide to deploy mobile cell towers in the early hours of the crisis to restore communications, NPS1 can tell them whether more civilians will take to the roads, or fewer. "Agent-based models are how you get all these pieces sorted out and look at the interactions," Barrett says.

The downside is that models like NPS1 tend to be big—each of the model's initial runs kept a 500-microprocessor computing cluster busy for a day and a half—forcing the agents to be relatively simple-minded. "There's a fundamental trade-off between the complexity of individual agents and the size of the simulation," says Jonathan Pfautz, who funds agent-based modeling of social behavior as a program manager at the Defense Advanced Research Projects Agency in Arlington, Virginia.

But computers keep getting bigger and more powerful, as do the data sets used to populate and calibrate the models. In fields as diverse as economics, transportation, public health, and urban planning, more and more decision-makers are taking agent-based models seriously. "They're the most flexible and detailed models out there," says Ira Longini, who models epidemics at the University of Florida in Gainesville, "which makes them by far the most effective in understanding and directing policy."

A plume of radioactive fallout (yellow) stretches east across Washington, D.C., a few hours after a nuclear bomb goes off near the White House in this snapshot of an agent-based model. Bar heights show the number of people at a location, while color indicates their health. Red represents sickness or death.

(Image) Dane Webster, University of Colorado in Denver; (Data) Network Dynamics and Simulation Science Laboratory (NDSSL)

The roots of agent-based modeling go back at least to the 1940s, when computer pioneers such as Alan Turing experimented with locally interacting bits of software to model complex behavior in physics and biology. But the current wave of development didn't get underway until the mid-1990s.

One early success was **Sugarscape**, developed by economists Robert Axtell of George Mason University in Fairfax, Virginia, and Joshua Epstein of New York University (NYU) in New York City. Because their goal was to simulate social phenomena on ordinary desktop computers, they pared agent-based modeling down to its essence: a set of simple agents that moved around a grid in search of "sugar"—a foodlike resource that was abundant in some places and scarce in others. Though simple, the model gave rise to surprisingly complex group behaviors such as migration, combat, and neighborhood segregation.

Another milestone of the 1990s was the Transportation Analysis and Simulation System (**Transims**), an agent-based traffic model developed by Barrett and others at the Los Alamos

National Laboratory in New Mexico. Unlike traditional traffic models, which used equations to describe moving vehicles en masse as a kind of fluid, Transims modeled each vehicle and driver as an agent moving through a city's road network. The simulation included a realistic mix of cars, trucks, and buses, driven by people with a realistic mix of ages, abilities, and destinations. When applied to the road networks in actual cities, Transims did better than traditional models at predicting traffic jams and local pollution levels—one reason why Transims-inspired agent-based models are now a standard tool in transportation planning.

A similar shift was playing out for epidemiologists. For much of the past century, they have evaluated disease outbreaks with a comparatively simple set of equations that divide people into a few categories—such as susceptible, contagious, and immune—and that assume perfect mixing, meaning that everybody in the affected region is in contact with everyone else. Those equation-based models were run first on paper and then on computers, and they are still used widely. But epidemiologists are increasingly turning to agent-based models to include factors that the equations ignore, such as geography, transportation networks, family structure, and behavior change—all of which can strongly affect how disease spreads. During the 2014 Ebola outbreak in West Africa, for example, the Virginia Tech group used an agent-based model to help the U.S. military identify sites for field hospitals. Planners needed to know where the highest infection rates would be when the mobile units finally arrived, how far and how fast patients could travel over the region's notoriously bad roads, and a host of other issues not captured in the equations of traditional models.

In another example, Epstein's laboratory at NYU is working with the city's public health department to model potential outbreaks of Zika, a mosquito-borne virus that can lead to catastrophic birth defects. The group has devised a model that includes agents representing all 8.5 million New Yorkers, plus a smaller set of agents representing the entire population of individual mosquitoes, as estimated from traps. The model also incorporates data on how people typically move between home, work, school, and shopping; on sexual behavior (Zika can be spread through unprotected sex); and on factors that affect mosquito populations, such as seasonal temperature swings, rainfall, and breeding sites such as caches of old tires. The result is a model that not only predicts how bad such an outbreak could get—something epidemiologists could determine from equations—but also suggests where the worst hot spots might be.

In economics, agent-based models can be a powerful tool for understanding global poverty, says Stéphane Hallegatte, an economist at the World Bank in Washington, D.C. If all you look at are standard metrics such as gross domestic product (GDP) and total income, he says, then in most countries you're seeing only rich people: The poor have so little money that they barely register.

To do better, Hallegatte and his colleagues are looking at individual families. His team built a model with agents representing 1.4 million households around the globe—roughly 10,000 per country—and looked at how climate change and disasters might affect health, food security, and labor productivity. The model estimates how storms or drought might affect farmers' crop yields and market prices, or how an earthquake might cripple factory workers' incomes by destroying their cars, the roads, or even the factories.

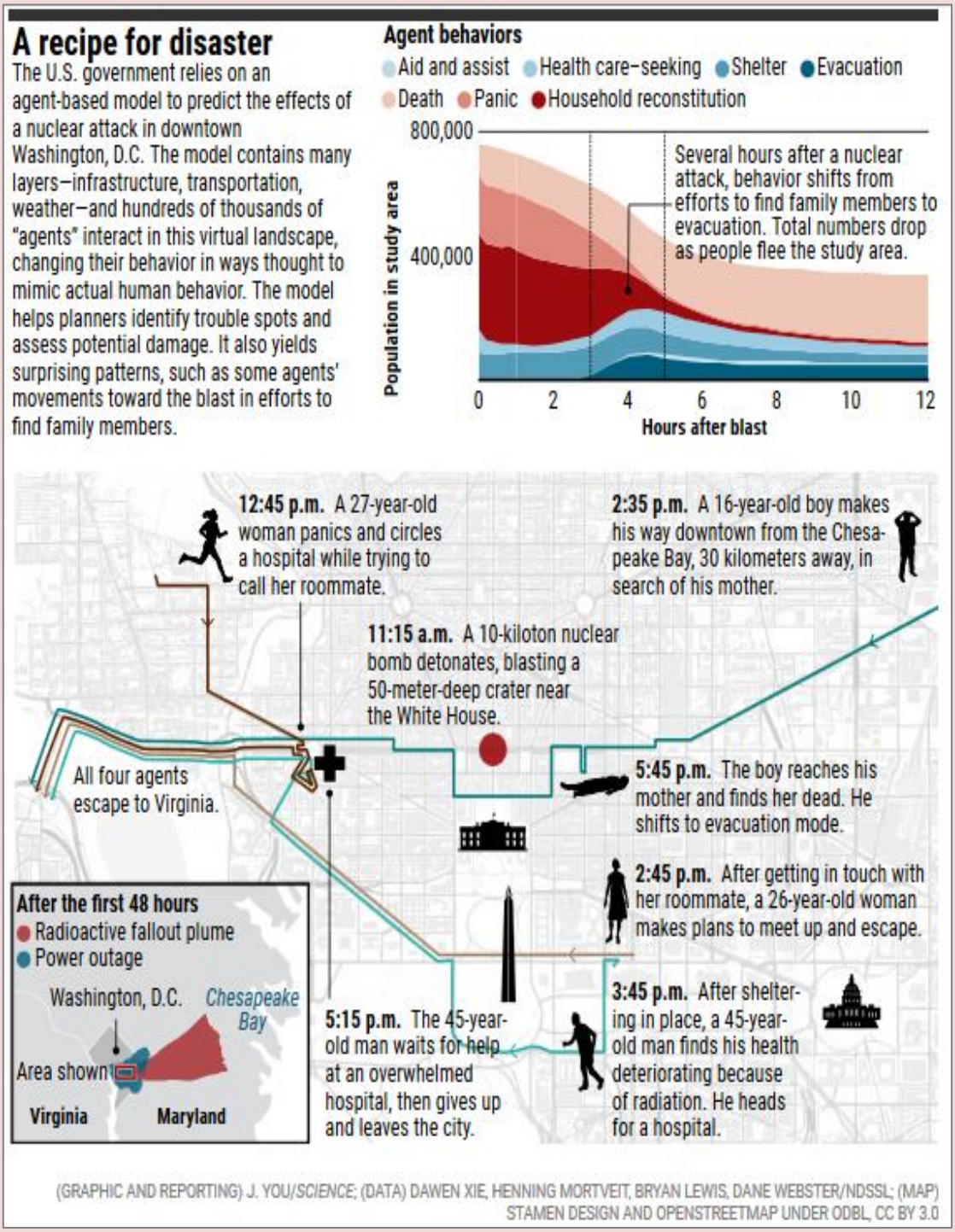
The model suggests something obvious: Poor people are considerably more vulnerable to disaster and climate change than rich people. But Hallegatte's team saw a remarkable amount of variation. If the poor people in a particular country are mostly farmers, for example, they might actually benefit from climate change when global food prices rise. But if the country's poor people are mostly packed into cities, that price rise could hurt badly.

That kind of granularity has made it easier for the World Bank to tailor its recommendations to each country's needs, Hallegatte says—and much easier to explain the model's results in human terms rather than economic jargon. "Instead of telling a country that climate change will decrease their GDP by X%," he says, "you can say that 10 million people will fall into poverty. That's a number that's much easier to understand."

Given how much is at stake in those simulations, Barrett says, users always want to know why they should trust the results. How can they be sure that the model's output has anything to do with the real world—especially in cases such as nuclear disasters, which have no empirical data to go on?

Barrett says that question has several answers. First, users shouldn't expect the models to make specific predictions about, say, a stock market crash next Tuesday. Instead, most modelers accommodate the inevitable uncertainties by averaging over many runs of each scenario and displaying a likely range of outcomes, much like landfall forecasts for

hurricanes. That still allows planners to use the model as a test bed to game out the consequences of taking action A, B, or C.



(Graphic and Reporting) J. You/*Science*; (Data) Dawen Xie, Henning Mortveit, Bryan Lewis, Dane Webster/NDSSL; (Map) Stamen Design and Openstreetmap Under Odbl, CC by 3.0

After the first 48 hours Washington, D.C. Area shown Radioactive fallout plume Power outage ChesapeakeBay Maryland Virginia 11:15 a.m. A 10-kiloton nuclear bomb detonates, blasting a 50-meter-deep crater near the White House. 2:35 p.m. A 16-year-old boy makes his way downtown from the Chesa- peake Bay, 30 kilometers away, in search of his mother. 5:45 p.m. The boy reaches his mother and finds her dead. He shifts to evacuation mode. 3:45 p.m. After shelter-ing in place, a 45-year-old man finds his health deteriorating because of radiation. He heads

for a hospital. 5:15 p.m. The 45-year-old man waits for help at an overwhelmed hospital, then gives up and leaves the city. 12:45 p.m. A 27-year-old woman panics and circles a hospital while trying to call her roommate. 2:45 p.m. After getting in touch with her roommate, a 26-year-old woman makes plans to meet up and escape. All four agents escape to Virginia. 0 2 4 6 8 10 12 Hours after blast 400,000 800,000 Population in study area Death Panic Household reconstitution Aid and assist Health care–seeking Shelter Evacuation Agent behaviors Several hours after a nuclear attack, behavior shifts from efforts to find family members to evacuation. Total numbers drop as people flee the study area. A recipe for disasterThe U.S. government relies on an agent-based model to predict the effects of a nuclear attack in downtown Washington, D.C. The model contains many layers—infrastructure, transportation, weather—and hundreds of thousands of "agents" interact in this virtual landscape, changing their behavior in ways thought to mimic actual human behavior. The model helps planners identify trouble spots and assess potential damage. It also yields surprising patterns, such as some agents' movements toward the blast in efforts to find family members.

Second, Barrett says, the modelers should not just slap the model together and see whether the final results make sense. Instead, they should validate the model as they build it, looking at each piece as they slot it in—how people get to and from work, for example—and matching it to real-world data from transit agencies, the census, and other sources. "At every step, there is data that you're calibrating to," he says.

Modelers should also try to calibrate agents' behaviors by using studies of human psychology. Doing so can be tricky—humans are complicated—but in crisis situations, modeling behavior becomes easier because it tends to be primal. The NPS1 model, for example, gets by with built-in rules that cause the agents to shift back and forth among just a few behaviors, such as "health care–seeking," "shelter-seeking," and "evacuating."

Even so, field studies point to crucial nuances, says Julie Dugdale, an artificial intelligence researcher at the University of Grenoble in France who studies human behavior under stress. "In earthquakes," she says, "we find that people will be more afraid of being without family or friends than of the crisis itself." People will go looking for their loved ones first thing and willingly put themselves in danger in the process. Likewise in fires, Dugdale says. Engineers tend to assume that when the alarm sounds, people will immediately file toward the exits in an orderly way. But just watch the next time your building has a fire drill, she says: "People don't evacuate without first talking to others"—and if need be, collecting friends and family.

The evidence also suggests that blind, unthinking panic is rare. In an agent-based model published in 2011, sociologist Ben Aguirre and his colleagues at the University of Delaware in Newark tried to reproduce what happened in a 2003 Rhode Island nightclub fire. The crowds jammed together so tightly that no one could move, and 100 people died. Between the police, the local paper, and survivors' accounts, Aguirre's team had good data on the victims, their behavior, and their relationships to others. And when the researchers incorporated those relationships into the model, he says, the runs most consistent with the actual fire involved almost no panic at all. "We found that people were trying to get out with friends, co-workers, and loved ones," Aguirre says. "They were not trying to hurt each other. That was a happenstance."

The NPS1 model tries to incorporate such insights, sending its agents into "household reconstitution" mode (searching for friends and family) much more often than "panic" mode (running around with no coherent goal). And the results can sometimes be counterintuitive. For example, the model suggests that right after the strike, emergency managers should expect to see some people rushing toward ground zero, jamming the roads in a frantic effort to pick up children from school or find missing spouses. The model also points to a good way to reduce chaos: to quickly restore partial cell service, so that people can verify that their loved ones are safe.

If agent-based modelers have a top priority, it's to make the simulations easier to build, run, and use—not least because that would make them more accessible to real-world decision-makers.

Epstein, for example, envisions national centers where decision-makers could access what he calls a petabyte playbook: a library containing digital versions of every large city, with precomputed models of just about every potential hazard. "Then, if something actually happens, like a toxic plume," he says, "we could pick out the model that's the closest match and do near–real-time calculation for things like the optimal mix of shelter-in-place and evacuation."

At Virginia Tech, computer scientist Madhav Marathe is thinking along the same lines. When a Category-5 hurricane is bearing down, he says, someone like the mayor of San Juan can't

be waiting around for a weeklong analysis of the storm's possible impact on Puerto Rico's power grid. She needs information that's actionable, he says—"and that means models with a simple interface, running in the cloud, delivering very sophisticated analytics in a very short period of time."

Marathe calls it "agent-based modeling as a service." His lab has already spent the past 4 years developing and testing a web-based tool that lets public health officials build pandemic simulations and do what-if analyses on their own, without having to hire programmers. With just a few clicks, users can specify key variables such as the region of interest, from as small as a single city to the entire United States, and the type of disease, such as influenza, measles, Ebola, or something new. Then, using the tool's built-in maps and graphs, users can watch the simulation unfold and see the effect of their proposed treatment protocols.

Despite being specialized for epidemics, Marathe says, the tool's underlying geographic models and synthetic populations are general, and they can be applied to other kinds of disasters, such as chemical spills, hurricanes, and cascading failures in power networks. Ultimately, he says, "the hope is to build such models into services that are individualized—for you, your family, or your city." Or, as Barrett puts it, "If I send Jimmy to school today, what's the probability of him getting Zika?"

So it won't just be bureaucrats using those systems, Barrett adds. It will be you. "It will be as routine as Google Maps.

***M. Mitchell Waldrop** is a journalist based in Washington, D.C.*

North Korea Suspends Nuclear and Long-Range Missile Tests

Source: https://www.globalsecurity.org/wmd/library/news/dprk/2018/dprk-180420-voa01.htm

Apr 20 – North Korea says it has suspended nuclear tests and plans to close its nuclear test site.

The North's official Korean Central News Agency said the military is also suspending long-range missile tests and said the suspensions went into effect on Saturday.

The announcement said the government is making the moves to shift its national focus and to improve the economy.

The development comes less than a week before North Korean leader Kim Jong Un is set to meet South Korean President Moon Jae-in at a summit to try to end the nuclear standoff on the Korean peninsula. The United States and North Korea are planning a separate summit, although no date has been set.

On Friday, the two Koreas opened a hotline between their leaders, ahead of the planned summit in the Demilitarized Zone on April 27. The hotline is the latest step in an intense diplomatic activity on and around the Korean peninsula, initiated with the Winter Olympics in the South.

Also Friday, U.S. Defense Secretary Jim Mattis met with his Japanese counterpart, Itsunori Onodera, at the Pentagon for talks that included North Korea. Mattis said the possible talks between the United States and North Korea will not change the strong relationship the United Stateshas with Japan.

"This is a mutually beneficial alliance between two democratic nations that trust each other. Nothing is going to shake that."

Onodera said the "iron clad US-Japan alliance" must work with the international community to make North Korea abandon all weapons of mass destruction "in a complete, verifiable, and irreversible manner."
South Korea's president said Thursday that North Korea is not imposing conditions on upcoming summits with him and U.S. President Donald Trump.
Moon told corporate executives in Seoul, "They have not attached any conditions that the U.S. cannot accept, such as the withdrawal of American troops from South Korea."He said, "All they are talking about is the end of hostile policies against North Korea, followed by a guarantee of security."
Moon said, "I don't think denuclearization has different meanings for South and North Korea. The North is expressing a will for a complete denuclearization."
North Korea has defended its nuclear development and missile tests, in defiance of the U.N. Security Council mandates, as a deterrent to what it sees as a threat from the United States, which has 28,500 troops stationed in South Korea. But it has not launched a missile test since late November, or conducted a nuclear test since last September.
Trump struck an optimistic note earlier this week about the possibility of a denuclearized North Korea.
"As I've said before, there is a bright path available to North Korea when it achieves denuclearization in a complete and verifiable and irreversible way," Trump said.
But he cautioned that if his talks with Kim did not go the way he hopes, he was willing to walk away.

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

EXPLOSIVE NEWS

3 Explosive Devices Found at French Supermarket After Deadly Rampage

Source: http://time.com/5214027/france-terrorist-attack-supermarket/

Mar 30 – A French judicial official says three homemade explosive devices have been found in the supermarket in southern France that was the site of a deadly attack by a man calling himself "a soldier" of the Islamic State group.

Also found were a 7.65-caliber handgun and a hunting knife, the official said on Saturday. He wasn't authorized to speak publicly about an ongoing investigation.

The supermarket in Trebes was the site of an hours-long attack Friday that killed four people. The 25-year-old Moroccan-born attacker was himself killed when special police stormed the market.

It wasn't clear whether the knife and handgun found were the weapons he wielded when entering the supermarket. French police searching the home of the man found notes referring to the Islamic State group that appeared to be a final testament, the official said.

Also found in the search of the home were a computer and telephone, the official said Saturday, a day after the attack.

Police searched the home of Moroccan-born Redouane Lakdim, 25, after Friday's attack that killed four people — two in a supermarket near the southern city of Carcassonne where the attacker was killed in an assault. The fourth victim, a gendarme who stood in for a female hostage and was shot, died early Saturday.

The official says there apparently was no mention in the notes of the attack plans.

MyDefence and AAU develop Terahertz technology for IED detection

Source: http://counteriedreport.com/mydefence-and-aau-develop-terahertz-technology-for-ied-detection/

Mar 22 – **This project will take the last decade of innovations within Terahertz spectroscopy and bring it in to the future, where detection of explosives at a safe distance, can be used to prevent terror attacks and save lives.**

The Innovation Fund Denmark has decided to fund the project between the physicists at Aalborg University and the MyDefence R&D team, with 6.1 million Danish Kroner (0.8 million EUR).

"Explosives like those used in Improvised Explosive Devices (IED) have a unique "fingerprint" signature which can be clearly identified using terahertz spectroscopy. So far, the equipment for terahertz spectroscopy has been too bulky and fragile for out-of-the-lab applications, or has been limited to measurements at distances of a few meters or less. Together with Aalborg University, we have found a way to produce a portable terahertz spectroscopy device that, when realized, will allow us to detect explosives at safe standoff distances, says, Christian Steinø, CEO of MyDefence.

Terahertz waves are absorbed in water vapor, which causes a number of challenges, one being detection range. This is especially true, when you want the technology to detect hidden explosives in real-world settings. The device must be able to work at far enough distance to, for instance, be able to give a driver on a vehicle enough warning to react on explosives detected on the ground ahead of him. The experience of the Optics and Spectroscopy research group at Aalborg University, together with the knowledge and skills of the former military officers and engineers at MyDefence, is just the right mix of competencies needed, to innovate this truly revolutionary technology.

"A few years ago, MyDefence contacted the physicists at Aalborg University, and presented us with their vision of detecting explosives using terahertz radiation. Christian Steinø and Dan Hermansen had some innovative ideas, and their experience from fighter plane radar technology and anti-drone RF technology, was just the right complement to our expertise in

optics and spectroscopy. Together we came up with a good solution". Says, Esben Skovsen, Associate Professor at the Department of Materials and Production.
The 3-years and 3 months project will include a number of field trials, live test, enhancements of identification algorithms, and a close cooperation with the researchers of Aalborg University.

- **The Innovation Fund Investment**: 6 million DKK.
- **Total project budget:** 8 million DKK.
- **Project duration:** 3 years and 3 months
- **Official project title:** Detection of explosives using terahertz radiation at improved standoff-distances (DETRIS)

ISIS 'to target World Cup players and fans in Russia with drones equipped with bombs'

Source: http://www.dailymail.co.uk/news/article-5567481/ISIS-target-World-Cup-players-fans-Russia-drones-equipped-bombs.html

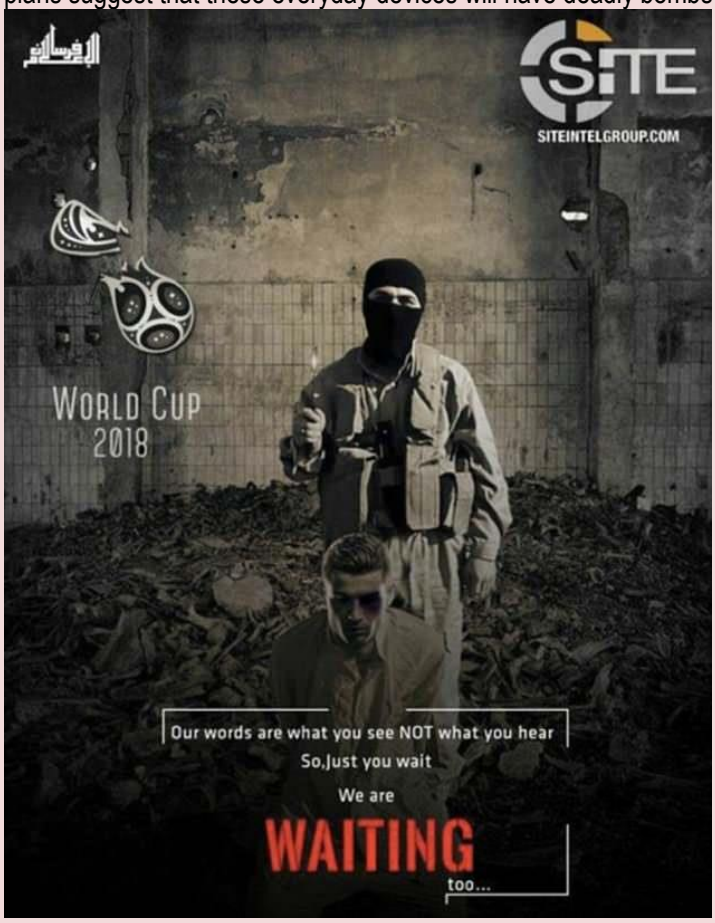
Apr 01 – ISIS are reportedly planning on dropping bombs on players and fans at the World Cup in Russia by using drones.
Shocking photos and videos posted on encrypted app Telegram appear to detail the plans and explain how the terror group intend to carry the attacks out.
The propaganda is believed to show extremists arming the drones with explosives, in preparation for unleashing them at the football tournament in June.
One of the photos apparently shows a drone carrying anti-tank rockets with the collection also showing extremists returning from Syria and Iraq to work with the drones.
The Telegram app has become a breeding ground for extremists, according to the **Daily Star Sunday** who shared the plans.
A cyber security expert said that the app has been plagued by terrorists plotting atrocities at the World Cup/

This shot posted on the messaging app seems to show the drone moving into position moments before the explosion

Elad Ezrachi, of internet surveillance firm Sixgill, told the Star that intelligence suggests the threats to be taken seriously.
'There is no doubt that this technology, if used by Isis in terrorist attacks at the World Cup, can lead to catastrophic results.'

This appears to show one of the drones armed with anti-tank rockets that ISIS are allegedly planning to detonate at the tournament in Russia

The drones that ISIS are planning on using seem to the cheap kind normally used by filmmakers. The plans suggest that these everyday devices will have deadly bombs attached to them.



This disturbing propaganda poster shows a gun-toting militant apparently standing behind football superstar Cristiano Ronaldo, who is pictured kneeling in front of him

Another shocking poster is emblazoned with the words 'target Russia' in capital letters with a picture of Argentinian football sensation Lionel Messi in the background

Posts on the app also claim that ISIS could use planes and other specialised devices that carry bombs.

A pro-ISIS telegram post next to a picture of a drone carrying what appear to be anti-tank rockets, reads: 'These are some of the types of bombs that are being used in the UAVs manufactured by Isis.'

The terrifying report comes after security services admitted the World Cup is a target for ISIS.

ISIS has repeatedly mentioned football's showpiece event in Russian this summer in a series of chilling online threats and communications.

Jihadists may try to use the tournament as a chance to avenge Vladimir Putin's attacks on ISIS in Syria, according to Germany's Federal Criminal Police Office.

This photo appears to show a detailed guide for how ISIS intend to use the lethal drones

One picture appears to show a UAV bomb being deployed by an ISIS militant crouching down behind it

Another image shows what looks like an ISIS fighter launching a drone by hand (left) and detailed technical drawings of the drone's components (right)

The agency estimated that there was a high risk of a terror attack taking place with Russian militants returning from Iraq and Syria, according to an internal BKA report seen by German newspaper Bild.
An earlier poster showed a terrorist armed with a gun and explosives near a football stadium in Russia along with the words: 'I swear that the Mujahideen's fire will burn you... just you wait'.

Rockets feature in the shocking images

This image appears to show a drone designed so it can be stood on (top left), and an image of the drone in action (top right)

Security experts have said it is a 'matter of time' before ISIS start using commercial drones to bomb cities in Europe and in the United States.
Jihadists could use quadcopters, a type of drone widely available to buy online, and often used by photographers to film or capture images from the air, and mount bombs on them, a leading terrorism official warned in September.

Learning from Israel's Experiences with Bus Terrorism

By Michael S. Dorn and Chris Dorn
Source: http://www.stnonline.com/news/web-exclusives/item/9405-learning-from-israel-s-experiences-with-bus-terrorism

Apr 18 – Havens International point to several bus terrorism attacks in Israel as providing valuable lessons for student transporters in the U.S. Pictured: Israeli police investigate a truck attack on a military bus in Jerusalem in 2017.

Editor's note: *Protective intelligence is defined as the training of people in how to spot behaviors and communications that indicate a potential target is being surveilled prior to an attack. School buses are considered "soft targets" because they are mobile, difficult to protect and highly vulnerable to a variety of attack methods.*
Several training opportunities exist for school bus drivers to increase the vigilance of their security preparedness, which includes protective intelligence. While the industry has yet to

experience a widescale school bus security event of the magnitude that buses in Israel have, these incidents serve as valuable lessons student transporters and society at-large can learn from.
The following information is provided by Michael S. Dorn and Chris Dorn of Safe Havens International, a global security firm. The father and son team have written numerous school bus security articles and blogs for School Transportation News and have both presented at the STN EXPO.

Israel Case Studies
"The following case studies from Israeli suicide bombing attacks against buses are highly illustrative of these points (regarding protective intelligence). While the level of risk and operational environment are much different than in the U.S. there are still valuable lessons. These case studies are summarized from "Security Awareness for Public Bus Transportation: Case Studies of Attacks Against the Israeli Public Bus System (MTI Report 11-07)" prepared by the Mineta Transportation Institute.
Aug. 2, 2001: Kibbutzun Junction, No casualties.
A suicide bomber trying to board a bus to carry out a suicide bombing attack aroused the suspicion of the bus driver, who tackled and restrained him as he approached the bus. The driver was trained to stop short of the bus stop and observe passengers before proceeding and allowing them to load.
Feb. 19, 2002: Mehola Junction, No casualties.
A suicide bomber attempted to board a bus near Mehola (an Israeli village in the northern Jordan Valley) to carry out an attack but was pushed away by the driver after he noticed the man was wearing a large puffy jacket and was reaching his hand in his pocket. The bomber blew himself up in an open field near the bus stop after the bus drove away.
Feb. 6, 2002: Ma'ale Adumim, No casualties.
A suicide bomber who tried to board a bus was restrained, taken off the bus, and arrested by border police. The suspicious indicators observed included "a passenger wearing clothes that are out of character with the environment or neighborhood, abnormal behavior, concealed objects in the hand, a clenched fist, etc." This proved effective in alerting the driver to the presence of the bomber.
While it is always helpful to see how attacks have been prevented – it can also be very instructive to study attacks that could have been prevented if proper procedures had been followed.

Nov. 29, 2001: Israeli Defense Forces Base #80; 3 killed and 8 wounded.

A suicide bomber boarded an intercity line bus at a bus stop next to the town of Umm al-Fahm and blew himself up in the center of the bus as it was an Israeli military base. The driver later described the bomber as being freshly shaved, with a new haircut, and wearing very elegant clothing, including a heavy sweater and a coat. Although the driver thought the young man's appearance was unusual, he did not take any other action yet. The bomber paid with a 200 NIS bill, although the ride costs only about 20 NIS, and did not wait for his change. When the driver called to him to collect his change, the terrorist detonated the bomb.

Although the terrorist was instructed to detonate the IED upon the end of a route in a high traffic area, he did so several minutes after boarding, when the bus was fairly empty. The most probable explanation is that he misinterpreted the driver's call for the change and was concerned that if he returned, the driver would become suspicious. It should be noted that a suicide bomber acts under incredible pressure, and any interaction with authority figures may have a great mental impact and can disrupt the bomber's plans.

ISIS threatens to bomb New York's subway in chilling poster showing a militant with sticks of dynamite at High Street Brooklyn Bridge Station

Source: http://www.dailymail.co.uk/news/article-5620103/ISIS-threaten-bomb-New-Yorks-subway-chilling-propaganda-poster.html

IDF: Iranian drone shot down over Israeli airspace in February was armed with explosives

Source: http://www.homelandsecuritynewswire.com/dr20180416-idf-iranian-drone-shot-down-over-israeli-airspace-in-february-was-armed-with-explosives

Apr 16 – According to the IDF, an Iranian drone that entered into Israeli airspace in February was armed with explosives and demonstrated "an Iranian intent to carry out an attack" inside the Jewish State, the *Jerusalem Post* reported Friday.

The target of the attack was not identified. The IDF said that the drone that was identified and intercepted by an attack helicopter "did not pose a danger" while it was in Israeli territory.

According Air Force Chief of Staff Brigadier General Tomer Bar, the drone was an advanced model and possessed a signature that Israel had not previously encountered.

"We waited for it to cross into our territory," Bar said, emphasizing that Israel gave priority to getting "our hands on the drone."

The army made its determination about the threat after examining the remains of the shot down drone.

Following the destruction of the drone, Israel carried out retaliatory strikes in Syria targeting the Tiyas airbase from which the drone had been launched. Earlier this week airstrikes were carried out against the same airbase.

Following the incident, United States Ambassador to the United Nations, Nikki Haley, described Iran's piloting of a drone into Israel a "wake-up call" to the world regarding Iranian efforts to build a permanent military presence in Syria. "Iran and Hezbollah are making plans to stay in Syria," she said.

Only 6 Indian airports have operational bomb detection squads, audit finds

Source: https://www.moneycontrol.com/news/india/only-6-indian-airports-have-operational-bomb-detection-squads-audit-finds-2545323.html

Apr 09 – **Only six of the 59 airports guarded by the Central Industrial Security Force (CISF) in the country have operational bomb detection and disposal squads, according to an audit by the paramilitary agency, raising concerns about safety measures.**

Only the security forces at the airports in Delhi, Mumbai, Chennai, Kolkata, Cochin and Hyderabad are equipped to defuse and dispose off explosives, a *Hindustan Times* report said, quoting the audit report that it reviewed.

An operation bomb defuser squad requires 28 pieces of equipment including explosive vapour detectors, bomb disposal suits, and remote-operated vehicles. All the required pieces of equipment are available only at the six airports named above.

"Even if one equipment is not available, the squad cannot be made functional. We have written to the Airports Authority of India (AAI), Bureau of Civil Aviation Security (BCAS) and civil aviation ministry, asking them to provide this crucial equipment at the earliest," a CISF officer told the paper requesting anonymity.

CISF is responsible for security at 59 of India's 98 operational airports.

The absence of bomb disposal squads at airports poses a potential risk to aviation security as well as the passengers. In case a suspected explosive is found, the CISF has to summon a bomb disposal team from the nearest police station, delaying the security response, an aviation security expert told the paper.

"The report is self-explanatory and there is no doubt that Bomb Detection and Disposal Squad (BDDS) is essential for airport security," Arvind Ranjan, a former director general of the CISF, told the paper.

Bengaluru's Kempegowda International Airport (BAIL) has only 24 of the 28 required pieces of equipment specified by the BCAS, the audit report said.

Responding to the audit report, BAIL stated that requirement of three of the four pieces of equipment are under deliberation with the government and the fourth item entails a long lead time, which will be procured shortly.

"BIAL is firmly committed to comply with all security regulations and has consistently provided the latest and best equipment and facilities to the security forces at the Kempegowda International Airport, Bengaluru. BIAL constantly engages with the CISF and other security agencies to ensure the safety and security of our passengers."

Even the airports operated by AAI lack some of the bomb diffusing equipments such as such as explosive vapour detectors and remote-operated vehicles.

"AAI has also procured 18-21 bomb detection and disposal squad equipment for 13 AAI airports. However, detection equipment-- vapour detector--has not been procured, due to

which we are unable to operationalise the squad. **In 59 airports, we require 1,652 equipments but only 423 are available,**" the CISF officer told the paper.

A spokesperson for AAI said explosive vapour detectors will be procured by September 2018 for installation at 18 airports operated by it.

"In the first phase, we have provided equipment at 18 AAI airports…we have provided 12 of the 13 crucial equipment, which BCAS has described as priority one. We have procured bomb suits but the detector, which is the 13th equipment, will be made available by September 2018," an AAI official told the paper on condition of anonymity.

Mini remotely operated vehicles, which are used to dispose off explosives, are also being procured for 18 airports in phase one of the procurement, the AAI said, adding that the remaining equipment for the airports will be purchased in phase 2.

"For the sake of safety, you need to have complete set of equipment...if something happens to passengers, BCAS will be responsible for it since they are the one responsible for aviation security," Sudhakar Reddy, National President of the Air Passengers Association of India said.

How IEDs may be physically causing PTSD

Source: https://www.cbsnews.com/news/brian-mancini-brain-how-ieds-may-be-physically-causing-ptsd/

Apr 01 – A new medical discovery has profound implications for wounded warriors. It's a previously unknown type of brain injury uncovered in veterans who are exposed to the invisible wave of energy that erupts from high explosives. The evidence was found in the brains of veterans who died. And tonight, we have a rare opportunity to introduce you to one of the vets who made the discovery possible. Retired Army Sergeant First Class Brian Mancini killed himself in 2017 after descending into psychosis. But we met Mancini years before, in 2011, after he made a nearly miraculous recovery from the impact of a roadside bomb in Iraq. There's no one better to begin this story, than the late Brian Mancini himself.

Brian Mancini: I got hit in the face. I knew pretty early that I had lost my eye. I didn't know how severe my injuries were, but I knew I was hurt very bad.

We met Brian Mancini six years before his suicide. We had followed a group of wounded vets back to Iraq on a therapy program, endorsed by the Pentagon, designed to help them come to terms with the day they were wounded and leave that day behind.

Brian Mancini: You know, we often hear about guys that carry these heartaches their whole lives. And it slowly erodes them. I don't want to be that guy, you know? I want to be able to have a successful life and not burdened with the demons that I see here.

Brian Mancini: I'm glad I'm alive.

On that return trip to Iraq, Mancini visited the field hospital that saved him.

Brian Mancini: My whole face has been rebuilt. I used to look like Brad Pitt but this is what I got stuck with.

Brian Mancini: I have a titanium mesh plate in my forehead. They rebuilt my whole orbital socket. My sinuses were replaced or rebuilt.

Scott Pelley: How many surgeries did that come to?

Brian Mancini: I have no idea. I have no idea.

Years of surgeries, pain and struggle were witnessed by Brian Mancini's brother and sister, Michael and Nichole.

Michael Mancini: Oh, he was a patriot. He loved this country. He loved this country.

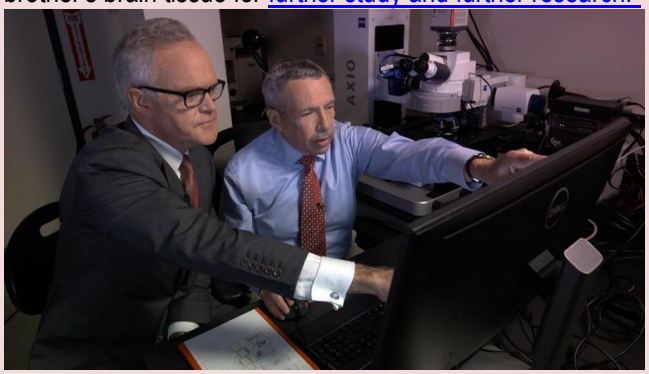
Nichole Mancini: He was a natural leader, and I think that the military was a natural fit for him. And he was good at his job, and he loved it.

After his recovery, he created a new job for himself. At home in Phoenix, he founded "Honor House" to provide wounded vets with therapies that helped him—including yoga, acupuncture, and especially fly-fishing.

Brian Mancini: He came leaps and bounds. And Brian two years ago was the best Brian I've ever known in my life.

But as he reached his peak in 2015, Mancini suddenly began to suffer delusions. He imagined the government was spying on him, that members of the Honor House board were with the CIA. And he thought he was being tracked with cell phones.

Michael Mancini: It was delusional, it was irrational, it was like, a progression.
Nichole Mancini: He wouldn't let us have our cell phones around him.
Michael Mancini: Very paranoid.
Nichole Mancini: His mind had started to almost turn against him. And people that—
Scott Pelley: His mind had turned against him?
Nichole Mancini: Yeah. Brian would often say, "I don't know if this is real or if I had if I dreamt it."
The Honor House board took control of the charity from Mancini. He had been depressed before, but not insane. Last year, Mancini donated his life savings to his church, drove to this remote canal, and shot himself in the head. The betrayal of his mind had been so sudden, so shocking, that his family was certain there must be a cause that no one understood.
Michael Mancini: And the first initial thought to me was, "I need to find someone who would take my brother's brain tissue for further study and further research."



The Mancini's found neuropathologist Dr. Daniel Perl.

Correspondent Scott Pelley with Dr. Daniel Perl

Perl oversees the brain tissue repository at the Uniformed Services University of the Health Sciences, the military medical school in Bethesda, Maryland. Perl also wondered whether some torments of war might be rooted in an undiscovered kind of brain injury caused by the supersonic pressure wave of high explosives.
Dr. Daniel Perl: That started in World War I and we had the whole issue of shell shock. And then in World War II, we had battle fatigue. Then in Korea, we had PTSD. I mean, these were all expressions of responses to being in warfare, much of it being exposed to blast. And we knew nothing about what was going on in the brain.
Perl's team sliced brain tissue from eight veterans and examined the tissue under a microscope. Rare for its power.
Scott Pelley: That doesn't look like the one I had in high school.
Dr. Daniel Perl: No, it's not.
Perl says his microscope is thousands of times more powerful than the best MRI. And it helped them discover this previously unknown form of brain injury when Perl compared the brains of the vets to civilians who had injured their brains in car wrecks.
Dr. Daniel Perl: The difference is just so dramatic.
Scott Pelley: These on the left are people who suffered--
Dr. Daniel Perl: A single individual's brain who suffered an automobile accident. A single individual who was exposed to blast. Stained identically for scarring.
Scott Pelley: The brown--area is the stain that reveals the scarring and you don't see it in the person who hit their head in the automobile accident.
Dr. Daniel Perl: That's right.
Dr. Daniel Perl: When an IED goes off there's a tremendous explosion. And with the explosion comes the formation of something called the blast wave. And it is sufficiently powerful to pass through the skull and through the brain. And when it does that-- it does damage the brain tissue.
Scott Pelley: Do you have a slide of Brian Mancini's brain?
Dr. Daniel Perl: Yes, we do.
The dark brown is scarring, running along lines where two types of brain tissue meet, the so-called gray matter and white matter.
Dr. Daniel Perl: The locations were areas of the brain that had differing densities. This was the interface between gray matter and white matter, between brain and fluid, such as spinal fluid, or brain and blood.
Scott Pelley: Why do you see the scarring where the white matter and the gray matter come together?

Dr. Daniel Perl: The white matter have a somewhat higher density than the gray matter. And that's where the energy of the blast wave is released.
Scott Pelley: They bang together.
Dr. Daniel Perl: In a sense, yeah.
Scott Pelley: Do you see the scarring at these interfaces throughout the entire brain?
Dr. Daniel Perl: We're looking at that now, okay? By and large, yes.
Evidence of this scarring was found in all of the veterans - none of the civilians.
Scott Pelley: Do you believe that you're going to find a connection between this and post-traumatic stress disorder?
Dr. Daniel Perl: In a sense, we already have. Every case that we've looked at has been diagnosed with PTSD And what that connection is, the nature of that connection, whether the scarring in the brain leads one to be more apt to develop PTSD, or whether there's so much overlap between the symptoms that one gets with the damage in the brain that it looks like PTSD, we don't know yet.
Earlier this season we reported on research by another laboratory into vets who showed evidence of "CTE" the kind of brain injury found in football players. Dr. Perl says his team has discovered something distinct from CTE.
Dr. Daniel Perl: Very different, okay? One is a huge blast wave that almost destroys his face, passes through his brain. It's a one-time thing. OK? It's not the sorta daily and weekly impact injury that an NFL player has. The other thing is that our service members are coming home from deployment symptomatic. By and large, CTE in the football player, for instance, occurs in their retirement, after they've played.
Scott Pelley: Years later?
Dr. Daniel Perl: Years later, right. They become symptomatic. So the timing of it seemed to be a very different proposition.
Scott Pelley: But it's absolutely clear to you that Brian Mancini did not have CTE?
Dr. Daniel Perl: That's right. We looked very carefully for CTE in Brian's brain. And he just did not have it.
Scott Pelley: So what you and your colleagues have discovered is something new?
Dr. Daniel Perl: Yes. Yes. This is new. This, this has changed thinking about blast exposure and its consequences.
We were able to add something to Dr. Perl's research that he rarely sees, a description of the blast that wounded one of his deceased subjects.
Brian Mancini: Most of my forehead was blasted out, I had a basal skull fracture along with some fractured vertebrae in my back and some burns and shrapnel. When I was doing the assessment of my injuries, I remember laying down and opening my mouth as wide as possible and reaching in and scraping the debris that had been knocked loose, and the blood, from my airway so I could breathe. And shortly after **that, I lost consciousness.**
Dr. Daniel Perl: It's just stunning to see this it's not something I normally get to experience. I mean that he survived this injury is just remarkable, much less what happened afterwards.
Now that the discovery is known, Perl hopes research can begin into improving the lives of those who suffer with this hidden wound of war.
Scott Pelley: What's your theory today on how this damage manifests itself in a living human being?
Dr. Daniel Perl: Well, obviously wherever there is damage, there must be some loss of function. Persistent headaches. They have problems with sleep. They have problems concentrating, memory problems swings of mood, anger management problems.
The discovery is a lone fact that raises many questions; can the scarring ever be seen in a living patient? How do the scars affect the mind? And what can be done?
Scott Pelley: If Brian Mancini had come to you in the last year of his life, would you have been able to do anything for him?
Dr. Daniel Perl: No, I don't think so. I don't think so. We're not there yet. We have a lotta people now beginning to take it seriously and begin work on it. It's not just us in our lab. It's really been a game changer in terms of our approach to this problem.
Dr. Perl is now searching for preserved brains of World War I veterans to see if the scarring dates to the beginning of widespread use of high explosives in war. Brian Mancini's life was devoted to wounded warriors—first as an Army medic, then in rehabilitation. And now, even in death, his work to heal continues.

Scott Pelley: And this is what Brian would've wanted?
Michael Mancini: Oh, absolutely.
Nichole Mancini: Without a doubt.
Scott Pelley: Brian is still serving his country.
Michael Mancini: Amen.
Brian Mancini: I wouldn't trade any of these horrendous and horrific experiences for anything there's a lesson in everything that we endure in life, And if we can clear all the chaos away and all the heartache away, we can receive that lesson "Why was I here? What was this for? Why did this happen?" And kind of get some of those answers. And I think that helps in healing long-term.

Revolutionary Explosive Sensor Under Development

Source: https://i-hls.com/archives/82502

Apr 12 – The development of sensors for explosives such as TNT is of huge interest. TNT is an explosive material widely used for military, industrial, and mining applications. Its reduction products are known to be toxic and carcinogenic to humans and may contaminate and accumulate in soils and drinking water. The procurement of TNT by terrorists to build improvised explosive devices (IEDs) poses a real and ongoing threat.

Electrochemistry is emerging as a viable technique for explosives detection "in the field" due to its many advantages, including low-cost instrumentation, portability, durability, sensitivity, selectivity, and fast response times. One common electrochemical technique employed in chemical sensors is amperometry, according to sciencetrends.com. It is based upon applying a voltage on the sensor electrode and measuring the current generated – this current is directly related to the concentration of the target analyte.

A research team led by Dr. Debbie Silvester from Curtin University in Perth, Western Australia, have devised a new electrochemical technique to detect and quantify trace amounts of the harmful TNT contaminant in water samples. They have mixed RTILs with common and commercially available methacrylate polymers to produce highly viscous "gel polymer electrolytes" (GPEs) which do not readily flow. The GPE can be easily casted as a film on top of the miniaturized planar electrode device.

The sensor device was able to quickly and easily quantify TNT concentrations at typical groundwater contamination levels of TNT, with a low limit of detection of 0.37 µg/mL. The low-cost and portability of the sensor device, along with the minimal amounts of GPE materials required, make this a very promising technology for the onsite monitoring of explosives. Furthermore, this hydrophobic polymer/RTIL based sensors can be potentially be extended to enable the detection and sensing of other analyte species including gases and other explosive compounds.

Understanding explosive sensitivity with molecule design

Source: http://www.homelandsecuritynewswire.com/dr20180419-understanding-explosive-sensitivity-with-molecule-design

Apr 19 – Explosives have an inherent problem - they should be perfectly safe for handling and storage but detonate reliably on demand. Using computer modeling and a novel molecule design technique, scientists at Los Alamos National Laboratory have replaced one "arm" of an explosive molecule to help unravel the first steps in the detonation process and better understand its sensitivity — how easily it begins a violent reaction.

"It started out with, can we take a common initiating explosive PentaErythritol TetraNitrate (PETN) and replace parts of it to change sensitivity properties," said explosives chemist Virginia Manner. "So we replaced an arm of PETN with various non-energetic groups to see how those different groups could change the sensitivity of the overall molecule. This is the first time we've taken a fundamental system like this and changed different parts of it to see how it could affect sensitivity."

The research was published today in *Chemical Science* the "flagship journal" for the *Royal Society of Chemistry*.

LANL notes that the researchers were able to change the sensitivity of the PETN-type materials, making them both less sensitive and more sensitive. PETN was invented in Germany in 1894, is one of the more powerful explosive materials, and is typically used only in small quantities due to its relatively high sensitivity.

Another novel approach to this research is the close collaboration between chemists and computer modelers at Los Alamos.

"About three years ago I realized that some modeling would really help," said Manner. "So I asked Marc Cawkwell to work with me and realized we had totally different ideas on what made explosives sensitive. I thought it was all just fundamental chemistry and he thought it's the mechanical properties that are controlling whether an explosive is insensitive or sensitive. Over the course of this work we slowly convinced each other that we were both wrong!"

"Or rather, partly right!" added Cawkwell.

Using a molecular dynamics computer code written at Los Alamos called "LATTE" Cawkwell is able to model the making and breaking of chemical bonds in explosives very accurately.

"The chemistry comes from the electronic structure of a molecule," said Cawkwell. "With LATTE we can accurately calculate the energy of a molecule and the force on every atom from its electronic structure, which allows us to propagate the positions of all of the atoms forward in time and let the system evolve. If the temperature and pressure are high enough then we see a cascade of chemistry that initiates an explosion."

The modeling is then used to interpret experiments in the form of a drop-weight impact test, to see if a newly synthesized explosive initiates easily (sensitive) or requires more force (insensitive) to explode.

What the modeling provides is a much deeper understanding of the underlying processes in a detonation.

"It really allowed us to understand these fairly simple drop weight experiments in exquisite atomistic detail," said Cawkwell. "For instance, the 'unzippering' reaction in PETN that was identified by our colleague Ed Kober from the LATTE simulations was something neither of us could anticipate."

"The ultimate goal is to see if can we predictively tune explosives," said Manner. "In the future people are going to want to know, how can we make explosives more or less safe or sensitive, particularly for nuclear stockpile applications. In general, people are just looking at these explosives that have been around for 100 years or more and trying to understand them. So we thought if we can make a system where we're systematically tuning sensitivity, where we

really understand the molecular properties that are affecting initiation the most, then we could guide the development of new explosives in the future."

— Read more in Virginia W. Manner et al., "Examining the chemical and structural properties that influence the sensitivity of energetic nitrate esters," Chemical Science (2018).

ICI International CBRNE INSTITUTE

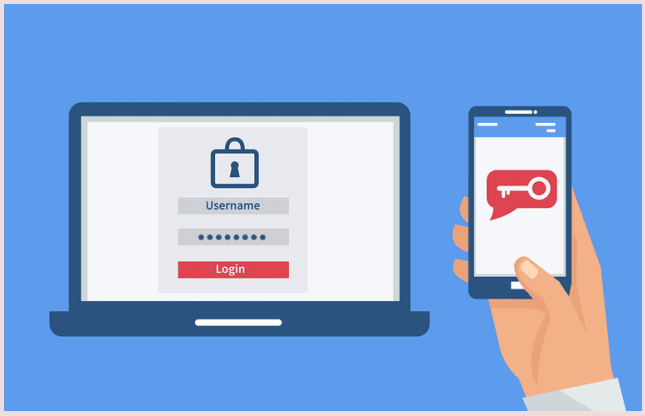
CBRNE-Terrorism Newsletter

CYBER NEWS

A new two-factor password method provides better protection

Source: http://www.homelandsecuritynewswire.com/dr20180330-a-new-twofactor-password-method-provides-better-protection

Mar 30 – A team of BGU cybersecurity researchers pioneered a new form of two-factor authentication that provides every user with stronger protection and is accessible to people with disabilities.
In an interview with *TechRepublic*, Dr. Yossi Oren, a senior lecturer in BGU's Department of Software and Information Systems Engineering and head of the Implementation Security and Side-Channel Attacks Lab at Cyber@BGU, describes how ultrasonic vibrations are used in lieu of memorizing six-digit codes.
This new method of authentication works on today's phones, laptops and tablets. It allows those with disabilities to log in with dignity and privacy.



Excerpts:

> Dr. Yossi Oren says, "People already know that passwords are not a good way to protect your accounts [because] when somebody steals your password you're gone for. So people are starting to use what's called two-factor authentication.
> "You type in your password and then you have to type in an extra code, which used to be sent over text message, but there's now something very terrible called SIM jacking, which means you have to find another way to get these digits to you.
> "So you go to a website and you have to recall your password, and then you have this device which has six digits on it. You have to look at these digits, memorize them, and then put them into your phone or to your computer to log in.
> "And the problem is that this process of looking at these digits, memorizing them, and typing them in, which sounds so very simple, is not so simple if you are a disabled user. Some people don't have the vision required to see these digits. Some people don't have the ability to memorize six digits for the 30 seconds it takes to copy them from one device to the other. And some people don't have the fine motor skills required to log in, to punch in these digits. How do we let these people use two-factor authentication with dignity and with privacy?
> "What we did is we found a way to send this two-factor authentication code using ultrasonic vibrations. What you do to log in is you take a device, which we are prototyping right now, to your phone and just touch them together. Three seconds, that's all it takes for this token to pass from this device to your phone.
> "You don't have to buy new hardware; you don't have to install new software; you don't have to get new permissions for your website or whatever. So any website, any app which uses two-factor authentication can use this to allow disabled users to log in with dignity and privacy."

— Read more in Jason Hiner, "Two-factor authentication gets simplified with a new sonic vibration token," TechRepublic (7 March 2018).

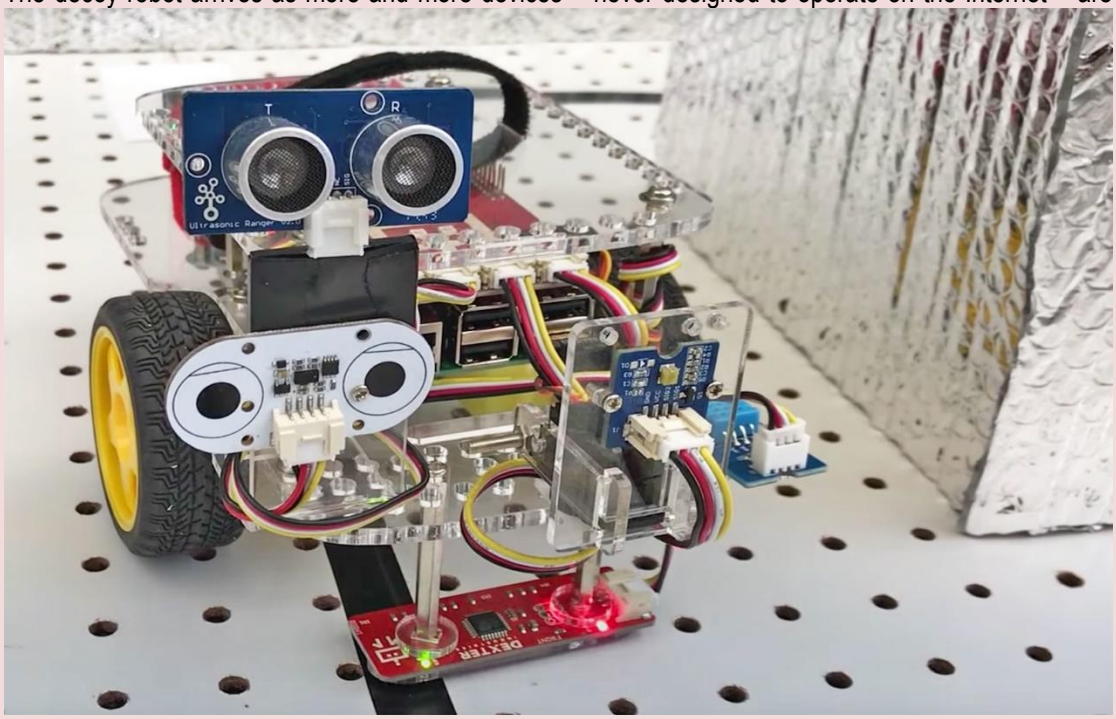
Diminutive robot defends factories against cyberthreats

Source: http://www.homelandsecuritynewswire.com/dr20180404-diminutive-robot-defends-factories-against-cyberthreats
Video: https://www.engadget.com/2018/03/29/honeybot-lures-hackers-protect-fellow-robots/

Apr 04 – It's small enough to fit inside a shoebox, yet this robot on four wheels has a big mission: keeping factories and other large facilities safe from hackers.
Meet the HoneyBot.
Developed by a team of researchers at the Georgia Institute of Technology, the diminutive device is designed to lure in digital troublemakers who have set their sights on industrial

facilities. HoneyBot will then trick the bad actors into giving up valuable information to cybersecurity professionals.

The decoy robot arrives as more and more devices – never designed to operate on the Internet – are



coming online in homes and factories alike, opening up a new range of possibilities for hackers looking to wreak havoc in both the digital and physical world.

"Robots do more now than they ever have, and some companies are moving forward with, not just the assembly line robots, but free-standing robots that can actually drive around factory floors," said Raheem Beyah, the Motorola Foundation Professor and interim Steve W. Chaddick School Chair in Georgia Tech's School of Electrical and Computer Engineering. "In that type of setting, you can imagine how dangerous this could be if a hacker gains access to those machines. At a minimum, they could cause harm to whatever products are being produced. If it's a large enough robot, it could destroy parts or the assembly line. In a worst-case scenario, it could injure or cause death to the humans in the vicinity."

Georgia Tech says that internet security professionals long have employed decoy computer systems known as "honeypots" as a way to throw cyberattackers off the trail. The research team applied the same concept to the HoneyBot, which is partially funded with a grant from the National Science Foundation. Once hackers gain access to the decoy, they leave behind valuable information that can help companies further secure their networks.

"A lot of cyberattacks go unanswered or unpunished because there's this level of anonymity afforded to malicious actors on the internet, and it's hard for companies to say who is responsible," said Celine Irvene, a Georgia Tech graduate student who worked with Beyah to devise the new robot. "Honeypots give security professionals the ability to study the attackers, determine what methods they are using, and figure out where they are or potentially even who they are."

The gadget can be monitored and controlled through the internet. But unlike other remote-controlled robots, the HoneyBot's special ability is tricking its operators into thinking it is performing one task, when in reality it's doing something completely different.

"The idea behind a honeypot is that you don't want the attackers to know they're in a honeypot," Beyah said. "If the attacker is smart and is looking out for the potential of a honeypot, maybe they'd look at different sensors on the robot, like an accelerometer or speedometer, to verify the robot is doing what it had been instructed. That's where we would be spoofing that information as well. The hacker would see from looking at the sensors that acceleration occurred from point A to point B."

In a factory setting, such a HoneyBot robot could sit motionless in a corner, springing to life when a hacker gains access – a visual indicator that a malicious actor is targeting the facility.

Rather than allowing the hacker to then run amok in the physical world, the robot could be designed to follow certain commands deemed harmless – such as meandering slowly about or picking up objects – but stopping short of actually doing anything dangerous.

So far, their technique seems to be working.

In experiments designed to test how convincing the false sensor data would be to individuals remotely controlling the device, volunteers in December 2017 used a virtual interface to control the robot and could not to see what was happening in real life. To entice the volunteers to break the rules, at specific spots within the maze, they encountered forbidden "shortcuts" that would allow them to finish the maze faster.

In the real maze back in the lab, no shortcut existed, and if the participants opted to go through it, the robot instead remained still. Meanwhile, the volunteers – who have now unwittingly become hackers for the purposes of the experiment – were fed simulated sensor data indicating they passed through the shortcut and continued along.

"We wanted to make sure they felt that this robot was doing this real thing," Beyah said.

In surveys after the experiment, participants who actually controlled the device the whole time and those who were being fed simulated data about the fake shortcut both indicated that the data was believable at similar rates.

"This is a good sign because it indicates that we're on the right track," Irvene said.

In Cyber-Defense, Good Enough is Far Better Than Perfect

Source: https://www.informationweek.com/devops/in-cyber-defense-good-enough-is-far-better-than-perfect/a/d-id/1331442?

Apr 04 – Agile and DevOps concepts help businesses get the basics of applications to market quickly, and those same concepts can help prepare the military for its challenges.

In 2015, the National Security Agency's hacking group, Tailored Access Operations, lost code that it uses for spying to hackers working for the Russian government. Following the breach, the NSA had to develop new tools, patch newly-exposed vulnerabilities, and harden its systems swiftly, before Russia could use its own technology against it.

Today, those tools are still being developed and patches being applied. Many of the vulnerabilities are still there.

Why did swiftly not happen?

Because in government, as in much of business, cyber security software development and response times are too slow. The relationship between software development and software operations is still configured for the machine age. In this old environment, stakeholders conceptualize an ideal solution to a problem, write specs, discuss and analyze them, design the software, build it, test it, and then, finally, deploy it. This is called the waterfall method: everything flows downhill from the top.

The NSA had already been compromised by Edward Snowden's massive leak in 2013. Yet a review of the NSA's security improvements concluded in 2016 that although there had been some, the NSA had not effectively reduced the number of user accounts with privileged access, which provides them with more avenues into sensitive data than normal users, nor fully implemented technology to oversee these accounts' activities.

There is a much better way to defend an organization against cyber-attacks: by deploying the rapid development techniques of DevOps.

Enabling Cyber-Security with DevOps

Real-time responses to real-time threats and opportunities demand a development model suited to the cyber age. It takes just a few days (if that) for our enemies to reverse-engineer a newly-released commercial software patch. Consequently, we must develop and apply patches and tools continuously. We can only do that if we design them to do the necessary job for the lowest cost – if we build the minimum viable product. Doing so frees engineers to work on the problem that needs solving, considering the people who will use it (this is called human-centered design), and not so much the specs. It allows them to develop the immediately-needed solution, not the perfect one. In truth, there are no perfect solutions – not for long – because the cybersecurity battleground is continually evolving.

If something breaks in this optimally configured and DevOps-enabled cybersecurity

environment, it gets fixed. Swiftly. If something works, it's scaled and improved. This accelerates the process and allows engineers and operators to work together to leverage new capabilities (such as artificial intelligence). A DevOps environment also increases cognitive diversity and encourages rapid innovation at the edge (not at headquarters) where warfighters and business people operate and need to innovate to win.

The U.S. Air Force created CyberWorx in 2016 – a public-private design center at the Air Force Academy – to accelerate our DevOps environment in partnership with technology companies that could help us think differently and acquire new capabilities. For example, we needed a better way to report anomalies in cyberspace to our cybersecurity professionals – anomalies that could indicate a potential attack, or one underway. Working in agile sprints, three companies collaborated with us to provide our cyber pros with a more comprehensive, crowd-sourced picture of what was happening, and present it in a way that would make sense to a user – that is, a human-centered design that lets operators see changes fast.

The need for speed in the military is self-evident. In conflicts based on information (as they all are, to some degree), winning means moving faster than the opposition, improving the speed of sound decision-making while degrading the enemy's. OODA loop speed (Observe, Orient, Decide, Act) is only increasing as machine learning and artificial intelligence support and secure operations faster and more effectively than humans working by themselves ever could.

In business, especially in finance, the speed of transactions (and the speed with which they can be disrupted by bad actors) requires that infiltrations be identified and responded to in moments. Global banks have recognized this and are becoming increasingly agile in their IT and security departments.

Unfortunately, in many businesses security is still based on people sitting in front of screens looking for intrusions. This is called "swivel-chairing" and, naturally, it's slow and error prone. To respond quickly enough, and more quickly than humans can, cybersecurity must be automated. Netflix, for example, has built tools that monitor changes to security configurations, flag when a change should be more closely examined, and rank them according to the level of risk. "The only realistic way of maintaining security in an environment that grows so rapidly and changes so quickly is to make it automation first," says Netflix director of engineering in cloud security Jason Chan.

Making cybersecurity responsive enough also will require that procurement professionals be rewarded for their agility, acquiring minimum solutions that apply at the bottom and middle edges of organizations, not behemoths applied from the top down. Agile procurement will help our airmen, soldiers, sailors, and Marines to innovate at speeds consistent with modern warfare and economic realities.

In the military, it has become axiomatic that you go to war with the weapons you are going to have tomorrow. Business calls this an innovation mindset.

Realistically, in both business and war, it should be called survival.

Col. Jeffrey A. Collins *directs Air Force CyberWorx, a public-private design center at the Air Force Academy focused on cyber capabilities and melding military, academic and industry expertise to solve problems. Before his assignment to CyberWorx, Col Collins was Deputy Director for Air Force Cyberspace Strategy and Policy, at the Pentagon. The views expressed here are his own and do not necessarily reflect those of the Air Force or Department of Defense.*

Citizen-Centric Solution to Terrorist Attack Response

Source: https://i-hls.com/archives/82425

Apr 07 – In many terrorist attack events, first responders do not have immediate access to real-time information from the scene, or from victims that are being held hostage. A new smartphone app developed in Australia offers a citizen-centric solution that will enable people to upload videos and other information as a terror attack is unfolding, giving emergency services the best chance to respond and prevent further harm.

The app will be enabled through Microsoft's new Azure Australia Central cloud.

The app, being developed by the Citadel Group, will enable users to instantly collect data, such as video and audio, which along with telemetry information about the phone's location can be transmitted to a centralized command and control center. Analysts will then be able to use technology to consolidate data from multiple sources, instantly providing real-time intelligence to help authorities provide a rapid response, and provide information through smartphone notifications to people in the affected area.
It is also expected that citizens will be able to help police crowdsource information in events such as car-jackings or child abductions, with the platform used to issue requests for sightings of vehicles with specified number plates, for example, according to theaustralian.com.au.
The app turns a smartphone into an intelligence gathering device. Emergency services can see what people are seeing, hear what people are hearing and understand whether it's a single incident or co-ordinated attack. The in-built analytics of this platform determines that there are three incidents reported within two km of each other which are atypical and may be a coordinated attack.


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

Nokia Is Developing A Connected Jacket For First Responders

Source: https://www.psfk.com/2018/03/nokia-developing-connected-jacket-first-responders.html

Mar 18 – Multinational communications company Nokia worked with South Korean fashion brand Kolon to create a jacket for first responders. The CHASE (connected health and safety equipment) LifeTech FR (first responders) jacket features the classic neon yellow color of typical first responder gear but features many new capabilities.

According to Engadget, the coat comes equipped with modular sensors, capable of tracking GPS location and heart rate, amongst other things. The information collected from the coat is sent back to the station, allowing the management system to examine and help keep the first responders safe by tracking them if they go missing or by determining if they are too tired from being overworked.

Southeastern European nations are latest to adopt emergency-response system

By Kylie Foy

Source: http://www.homelandsecuritynewswire.com/dr20180405-southeastern-european-nations-are-latest-to-adopt-emergencyresponse-system

Apr 05 – On a Google map of Modrac Lake, located near the city of Tuzla in Bosnia and Herzegovina, icons in the shape of boats move across the water. A commander, looking at the map on a monitor, watches their progress. Each boat in real life holds a disaster response unit that is heading toward the site of a disaster — in this case, a chemical spill. The same

interface that provides the map also shows images from the scene, messages between responders, social media posts from observers, and other real-time information that the commander uses to direct people and resources. The interface is one big picture, created and viewed by everyone involved, of the scene as it unfolds.

The platform enabling this coordination is called the **Next-Generation Incident Command System (NICS).** NICS, developed nearly a decade ago by Lincoln Laboratory and the Department of Homeland Security Science and Technology Directorate (DHS S&T), is used today around the world for emergency response. In its latest development, NICS has been implemented in the southeastern European nations of Bosnia and Herzegovina, Croatia, Macedonia, and Montenegro. Through a four-year partnership with the NATO Science for Peace and Security Programme, Lincoln Laboratory and DHS S&T will work with local and federal response agencies in these countries to adapt and enhance NICS for the specific needs of this multinational community.

"We are working with each country to best decide how NICS can be adapted to meet their disaster-response needs and also how NICS can improve communication across country borders," says Stephanie Foster, a staff member in the Laboratory's Humanitarian Assistance and Disaster Relief Systems Group and the program manager for the NICS NATO project. Foster notes that NICS will help the countries build a standardized method of response to large-scale disasters, such as the cyclone and ensuing floods that devastated the region in 2014.

Modifications to NICS are building on what staff learned during the NATO Euro-Atlantic Disaster Response Coordination Centre's 17th Consequence Management Field Exercise between Sept. 24 and 29 in 2017. Close to 1,300 disaster-response personnel from 34 NATO member and partner nations participated in the exercise.

Conveniently hosted in Bosnia and Herzegovina, the exercise provided the southeastern European disaster teams a first road test of the NICS platform. Foster, joined by Laboratory staff members Gregory Hogan, Robert Hallowell, Greg Gianforcaro, and Christopher Budny, traveled to Tuzla to prepare NICS for the exercise. They created a new workspace in NICS where the exercise could be implemented and, importantly, analyzed afterward. They worked with the countries to prepopulate data and geospatial information into the system and to create a standardized communications workflow that teams from each country would follow. They also trained people to use NICS, although the system's design makes it intuitively easy to use, which is one reason why NICS translates well globally.

For three days, NICS was implemented during water-rescue missions conducted by teams from Montenegro, Bosnia and Herzegovina, and Croatia. The exercise began with an initial emergency request received at the base of operations. From there, teams were deployed to the incident site and given instructions to either lead or assist in different scenarios, such as extracting people from a car that had entered the lake, removing barrels of chemicals and assessing the risk, and saving people from cable cars hanging above the water.

As soon as the emergency was reported, the incident was created in NICS and the information sharing began. At the base camp, commanders logged into the web-based interface using an ordinary web browser and internet connection. The onsite responders logged into NICS through an app on their cell phones. Together, they used NICS to observe the evolving situation and communicate.

"We would get live input from the water-rescue teams that were responding," Foster says. "They used the mobile app to upload images of the damage and to chat with users at base camp and in the incident command tent." The NICS mobile app, which is a relatively new addition to the system, also enabled live-tracking of the teams' locations — resulting in the boat icons moving across the map.

Another new feature of NICS was the incorporation of social media analytics. At the NATO exercise, Douglas Jones, a senior staff member in the Laboratory's Human Language Technology Group, led a research unit whose goal was to simulate social media activity during a disaster scenario and use the data to help responders gain situational awareness.

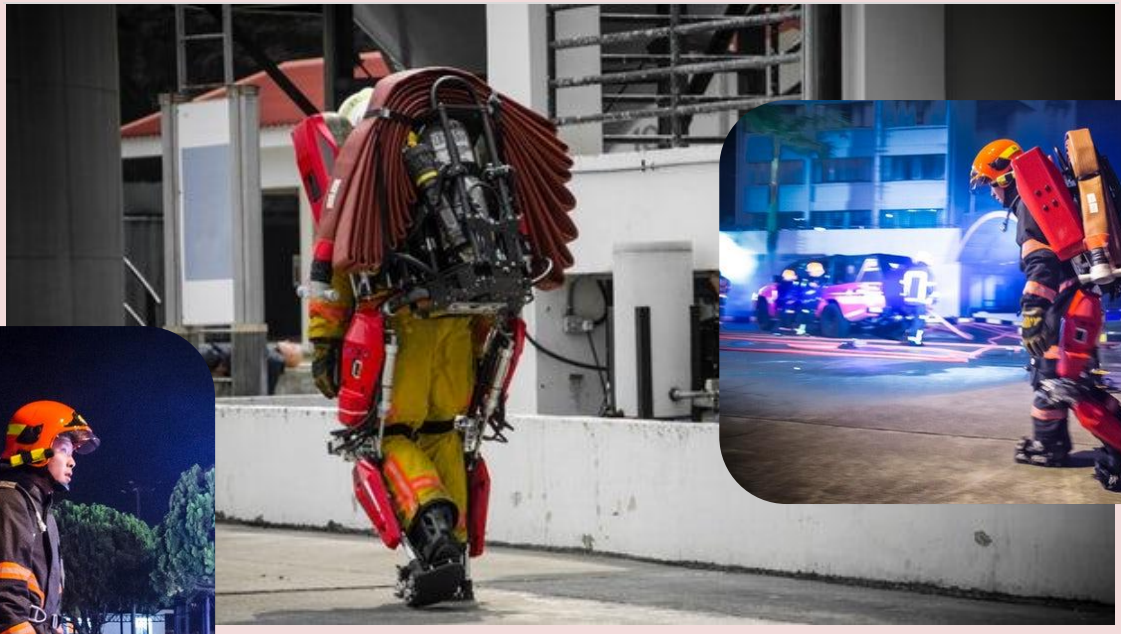
"In a real disaster, people would use social media such as Twitter and Facebook to ask for help or give information, but we couldn't use real social media during the exercise in case someone thought it was real. So, we built a closed system called SIMPOST," Jones says. A group of local journalism students were trained to post messages in real time to SIMPOST, role playing as either journalists, observers, or victims. By the end of exercise, they had

produced a dataset of about 2,000 messages, about half of which were in English and the other half in Bosnian and other languages.
Pulling information from the social media posts is key. The SIMPOST team was supported by a Defense Advanced Research Projects Agency (DARPA) program called LORELEI, a human language technology that aims to provide domain-relevant, essential information from messages written in any language. Using the LORELEI framework, the social media posts from the exercise were categorized by need type (such as medical, water, or search and rescue), urgency level, location, and timeframe.
To get this information out to the responders, the team added layers to the NICS interface that showed posts by need type and a color-coded heat map of social media activity around the incident locations. "We were able to improve this integration while at the exercise to allow the NICS users to search and filter the posts," says Budny, who built the SIMPOST platform and led its integration into NICS. Users could now choose to see posts by specific need type, and the system could pinpoint on the map where those messages were posted from.
"This integration required collaboration from staff working in different groups in a complex and challenging environment, but look what happened," Jones says. "We were able to work together to bring a potential new capability to the humanitarian assistance and disaster relief space."
NICS also offers graphical tools, essentially virtual whiteboards, with which users can draw boundaries or circle locations directly on the map. This feature is especially useful for communicating across language barriers.
NATO is looking for more opportunities to implement NICS internationally. In late September 2017, NATO opened a new center in Kuwait City, called the Istanbul Cooperation Initiative Regional Center, in which NATO researchers can work closely with Persian Gulf partners on a number of important issues, including disaster response. Hogan, senior staff in the Laboratory's Homeland Protection and Air Traffic Control Division, joined NATO Science for Peace and Security Programme staff at the center to present the NICS capability.
Another long-term goal of the NICS NATO partnership is to engage young scientists and engineers in further developing the NICS technology. The vision is to build an active community with the capability to evolve and contribute to the platform's open-source software, which DHS S&T released worldwide on GitHub last year.
The next three years will hold much more development for NICS. For the southeastern Europe project, a milestone each year will be a large-scale capability demonstration, like the NATO exercise, that will provide valuable data to learn from. The system archives all aspects of a created incident, so it becomes a powerful tool for analyzing past responses and informing future planning and execution.
"When it's all over and you can take a step back and analyze the process — that's when the real work begins," Foster says.

Auberon exoskeleton takes the strain out of firefighting in towering infernos

Source: https://newatlas.com/trigen-automotive-auberon-pneumatic-exokeleton/54261/

Apr 18 – Bounding up numerous flights of stairs when the elevator is out is punishing enough for our legs and lungs, but imagine having to do so while carrying heavy equipment needed to extinguish a blazing high-rise fire. Such a scenario has prompted specialist vehicle manufacturer Trigen Automotive to work with Singapore's Civil Defence Force to develop Auberon, a purely mechanical exoskeleton designed to take the strain out of carrying emergency equipment up to tower-top fires.
Trigen says that the breathing apparatus, hose lines, nozzles, power tools and more which often make up a firefighter's emergency toolkit can all add up to 40 kg (90 lb) of back-punishing weight, particularly when having to climb flights of stairs in a burning tower. Such equipment becomes much less of a burden when mounted to the Auberon Pneumatic Exoskeleton's specially-designed frame.
The electronics-free solution sees two 6.8 liter compressed air tanks powering the exoskeleton, which is reported enough to get a firefighter up and down 12 stories of stairs three times and still have a little to spare. Importantly, the design keeps a firefighter's hands



free to tackle the task of putting out a fire, while reducing the heavy burden on the shoulders and back by passing the weight through the exoskeleton and on to the ground via the footplate.

Pneumatic pistons on the legs help the first responder get into an easy stride, making an otherwise daunting stair climb much less of a physical challenge. And should the situation call for the firefighter to escape from the exoskeleton, a quick release mechanism has been included.

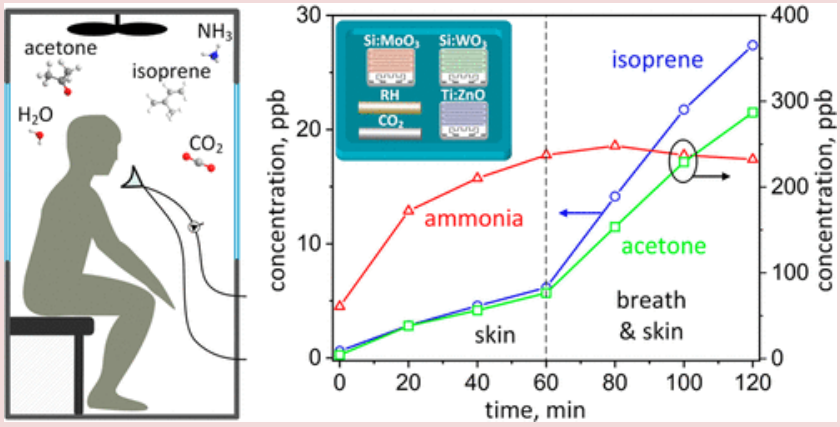
"Auberon demonstrates Trigen Automotive's recognition of the essential and demanding work carried out by firefighters worldwide," said the company's Lim Joo Siang. "We have worked very closely with emergency services to understand their challenges on the ground and engineered a reliable solution that mitigates the harsh conditions faced by firefighters in high-rise firefighting."

The company is taking order for Auberon now.

Portable device to sniff out trapped humans

Source: http://www.homelandsecuritynewswire.com/dr20180419-portable-device-to-sniff-out-trapped-humans

Apr 19 – The first step after buildings collapse from an earthquake, bombing, or other disaster is to rescue people who could be trapped in the rubble. But finding entrapped humans among the ruins can be challenging. Scientists now report in the ACS journal *Analytical Chemistry* the development of an inexpensive, selective sensor that is light and portable enough for first responders to hold in their hands or for drones to carry on a search for survivors.



In the hours following a destruction-causing event, the survival rate of people stuck in the rubble rapidly drops, so it's critical to get in there fast. Current approaches include the use of human-sniffing dogs and acoustic probes that can detect cries for help. But these methods have drawbacks, such as the limited availability of canines and the silence of unconscious victims. Devices that detect a human chemical signature, which includes molecules that are exhaled or that waft off the skin, are

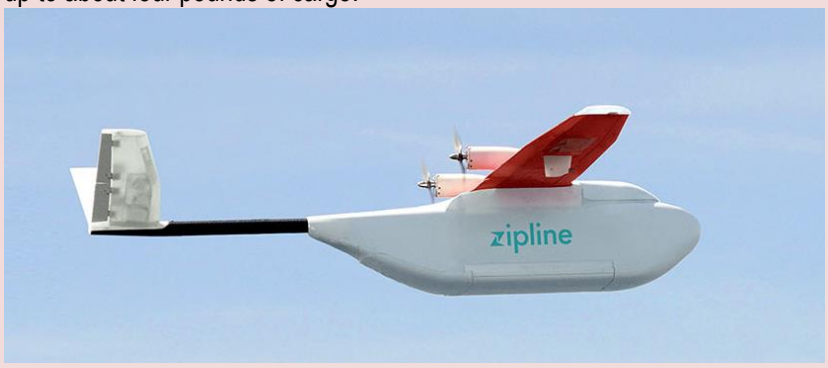
promising. But so far, these devices are too bulky and expensive for wide implementation, and they can miss signals that are present at low concentrations. So, Sotiris E. Pratsinis and colleagues wanted to develop an affordable, compact sensor array to detect even the most faint signs of life.
ACS says that the researchers built their palm-sized sensor array from three existing gas sensors, each tailored to detect a specific chemical emitted by breath or skin: acetone, ammonia or isoprene. **They also included two commercially available sensors for detecting humidity and CO_2.** In a human entrapment simulation, the sensors rapidly detected tiny amounts of these chemicals, at levels unprecedented for portable detectors—down to three parts per billion. The next step is to test the sensor array in the field under conditions similar to those expected in the aftermath of a calamity.

— Read more in Andreas T. Güntner et al., "Sniffing Entrapped Humans with Sensor Arrays," Analytical Chemistry 90, no. 8 (30 March 2018).

Medicine Drone Delivery Service Significantly Improved

Source: https://i-hls.com/archives/82488

Apr 11 – A company which supplies a drone delivery system to send urgent medicines has recently redesigned its system. Zipline's new delivery vehicle is an autonomous fixed-wing style airplane.
The new plane is capable of flying four times faster than the average quadcopter drone and can serve an area of 200 times as large. It can fly up to roughly 80 mph and has round-trip range of 99 miles carrying up to about four pounds of cargo.



The company said that in East Africa, its drones bring people the medicine they need, when they need it in a way that reduces waste, cost, and inventory while increasing access and saving lives.
The new aircraft is part of a complete redesign of Zipline's logistics system, which dramatically improves the system's launch, autonomous flight, and landing capabilities. The improvements will decrease the amount of

time between Zipline's receipt of an order and launch of a fulfilment flight from 10 minutes to 1, increase the number of daily delivery flights that each Zipline distribution center can make from 50 to 500, and expand the radius of each distribution center to serve populations of up to 10 million people.
Zipline's drone delivery has increased the use of some blood products by 175 percent in Rwandan hospitals. Waste and spoilage have been reduced by 95 percent, according to thedrive.com.


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

How Should Business Handle the Changing Nature of Terrorism?

Source: http://www.brinknews.com/how-should-business-handle-the-changing-nature-of-terrorism/

Apr 12 – Terrorism remains a persistent and significant threat to businesses, governments, and individuals. Fewer people were killed by acts of terrorism, insurgency, and politically or ideologically motivated violence in 2017 than in 2016, but the number of incidents is still very large – and the means of attack have shifted. As such, it's critical that businesses take stock of the strategies available to them to manage and finance that risk.

Shifting Threats and Costs

Marsh's *2018 Terrorism Risk Insurance Report*, prepared with support from Guy Carpenter, explores terrorism trends, the state of the terrorism insurance marketplace, and mitigation strategies for global businesses. Among the report's key findings:

- Acts of terrorism have increasingly come against soft targets and been perpetrated by "lone wolves" and small groups with no direct connection to known terrorist organizations, while past attacks were carried out primarily by specific groups against high-value and high-profile targets.
- Weapons of choice now include vehicles, knives, and other handheld devices, and they could include ransomware and other destructive cyber tools in the future.
- Actors backed by nation-states launched destructive ransomware attacks in 2017, raising the prospect that similarly destructive cyberattacks could soon be carried out by terrorists.

Impact on Business

In addition to direct property damage and injury to employees, these attacks can have significant indirect effects on businesses. These include:

- **Supply chain disruption and security costs:** Terrorist groups carried out nearly 350 attacks on global supply chains in 2016, an increase of 16 percent from 2015, according to BSI Supply Chain Services and Solutions. For example, stricter controls along France's borders following the November 2015 Paris attacks cost companies an additional $59 per delayed vehicle.
- **Lost revenue:** Terrorist attacks in Western Europe in late 2015 and early 2016 cost European airlines $2.5 billion in lost revenue in 2016, according to the International Air Transport Association.
- **Consumer confidence:** Although U.S. consumer confidence increased in the third quarter of 2017, terrorism was cited as the top concern for 21 percent of consumers, according to The Nielsen Company.

Risk Financing Options

The most common way for businesses to manage terrorism risk is to purchase property insurance, which can reimburse companies for costs stemming from physical damage and business interruption resulting from acts that are motivated by politics, religion, or ideology.

In 2017, 62 percent of U.S. businesses purchased property terrorism insurance, according to Marsh data. Purchasing, or take-up, rates across all industries have generally stayed close to 60 percent in recent years, but in 2017, rates varied by industry, geography, and company size. Take-up rates for terrorism insurance were higher for larger companies; 67 percent of companies with $500 million or more in total insured values purchased terrorism insurance, and those

companies also allocated more of their property insurance premiums to terrorism coverage than smaller companies.

Geography and Sector Matter

By industry, education entities, health care organizations, financial institutions, and real estate companies had the highest take-up rates, each exceeding 70 percent. This is due in large part to the sizable presence that organizations in these industries have in central business districts and major metropolitan areas that insurers perceive to be at a higher risk of terrorist attacks. For similar reasons, companies headquartered in the northeastern U.S. also purchased terrorism insurance at a higher rate than companies in other regions.

As an alternative to commercial insurance, some businesses choose to self-insure their terrorism risks through captives, which are insurance companies they own or can rent. For captive owners, the cost of implementing terrorism insurance programs often compares favorably to the cost of buying from commercial insurers. Captive insurers can also generally offer broader coverage than commercial insurers.

The Importance of a Government Role

In the U.S., insurers benefit from reinsurance protection in the event of a sizable loss through the federal Terrorism Risk Insurance Program. First established in 2002 following the September 11, 2001, attacks and most recently reauthorized via the Terrorism Risk Insurance Protection Reauthorization Act of 2015 (TRIPRA), this backstop has helped to keep property terrorism insurance costs low and widely available for buyers. The U.S. is one of more than 20 countries in which local terrorism insurance pools or government reinsurance mechanisms are available.

Local pools continue to evolve to meet the changing needs of businesses. For example, both the U.S. backstop and the UK's Pool Re now provide reinsurance protection for cyber-insurance policies. Pool Re also plans to provide coverage for nonphysical damage business interruption losses in the future.

The U.S. federal backstop remains especially important to continued market stability and health. Absent TRIPRA, which expires December 31, 2020, there is not sufficient insurance and reinsurance capital available to provide comprehensive terrorism coverage to U.S. insurance buyers.

As congressional representatives evaluate potential options ahead of TRIPRA's expiration, they will likely focus on trying to expand the private insurance market role in managing conventional acts of terrorism while still providing a critical backstop for large-scale and unconventional attacks.

Modeling Terrorism Risk

To make appropriate decisions on how to finance their terrorism risk, businesses must first understand that risk.

Since terrorism risk models were first developed in 2002, insurers, reinsurers, and modeling companies have continually refined their models and underlying assumptions. This has improved their ability to quantify terrorism risk, but modeling that risk is often more challenging than it is for other hazards.

Less Predictable and Less Data

Compared to hurricanes and earthquakes, for example, acts of terrorism occur less frequently, meaning there's less data to work with. Terrorist attacks are also less predictable because human attackers are unpredictable. Ultimately, this means that businesses can generally calculate the costs they're likely to incur in the event of a potential attack, but it's not as easy to calculate the probability of an attack affecting them.

Still, modeling terrorism risk can inform decisions about how much insurance to purchase, how to structure property terrorism and other insurance policies, and whether to consider a captive or other alternative to commercial insurance. And beyond insurance, modeling can help businesses make smarter choices to mitigate potential attacks and more effectively manage an attack's after-effects.

The cost of potential attacks to global businesses remains high. The ability of organizations to adapt to the changing pattern of terrorism is essential if they are able to limit the effects of terrorism on their operations and employees. This extends to carefully modeling the impacts of different attacks, and evaluating the financing options that are right for them.