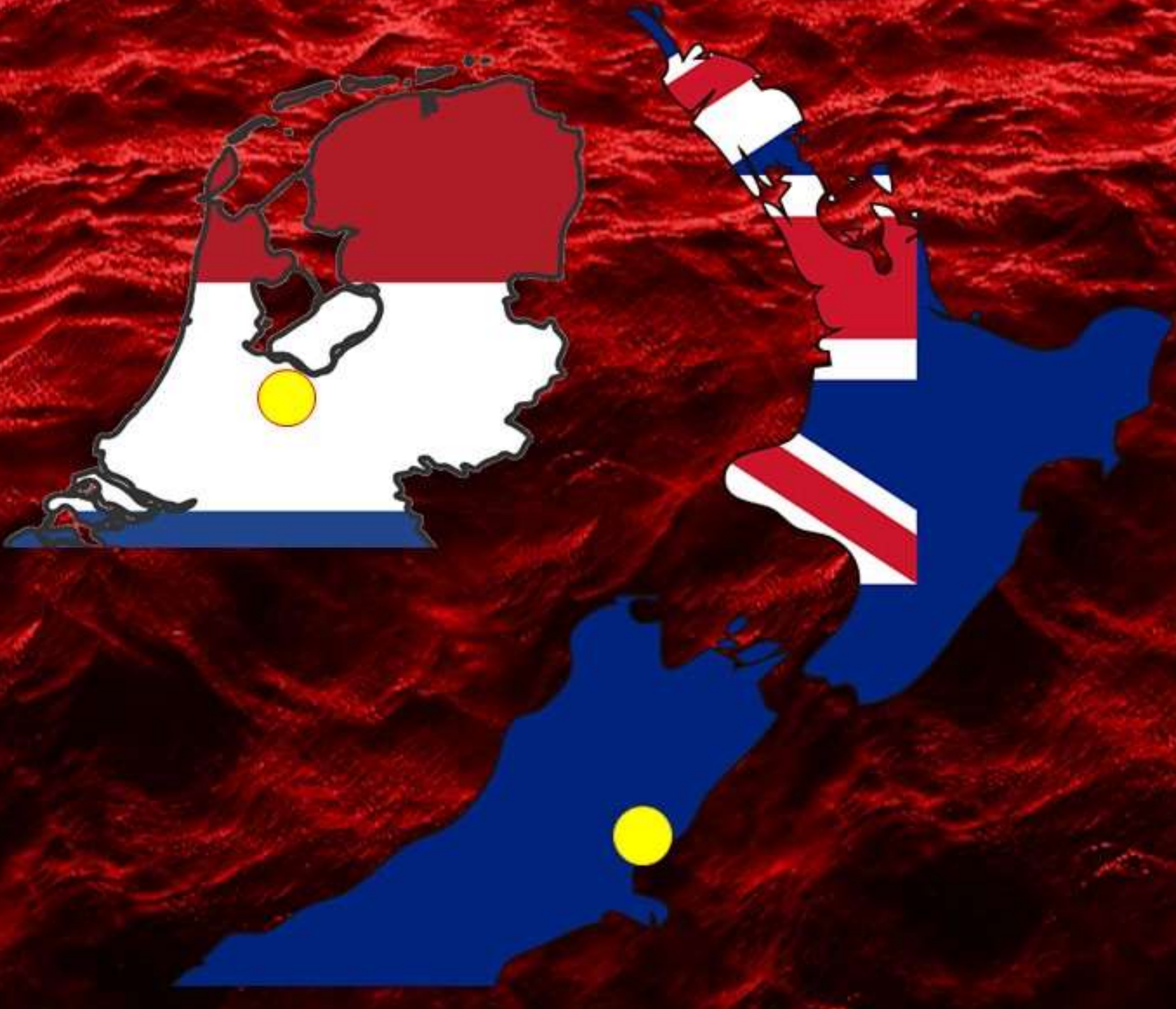
CBRNE DIARY

Dedicated to Global First Responders

March 2019

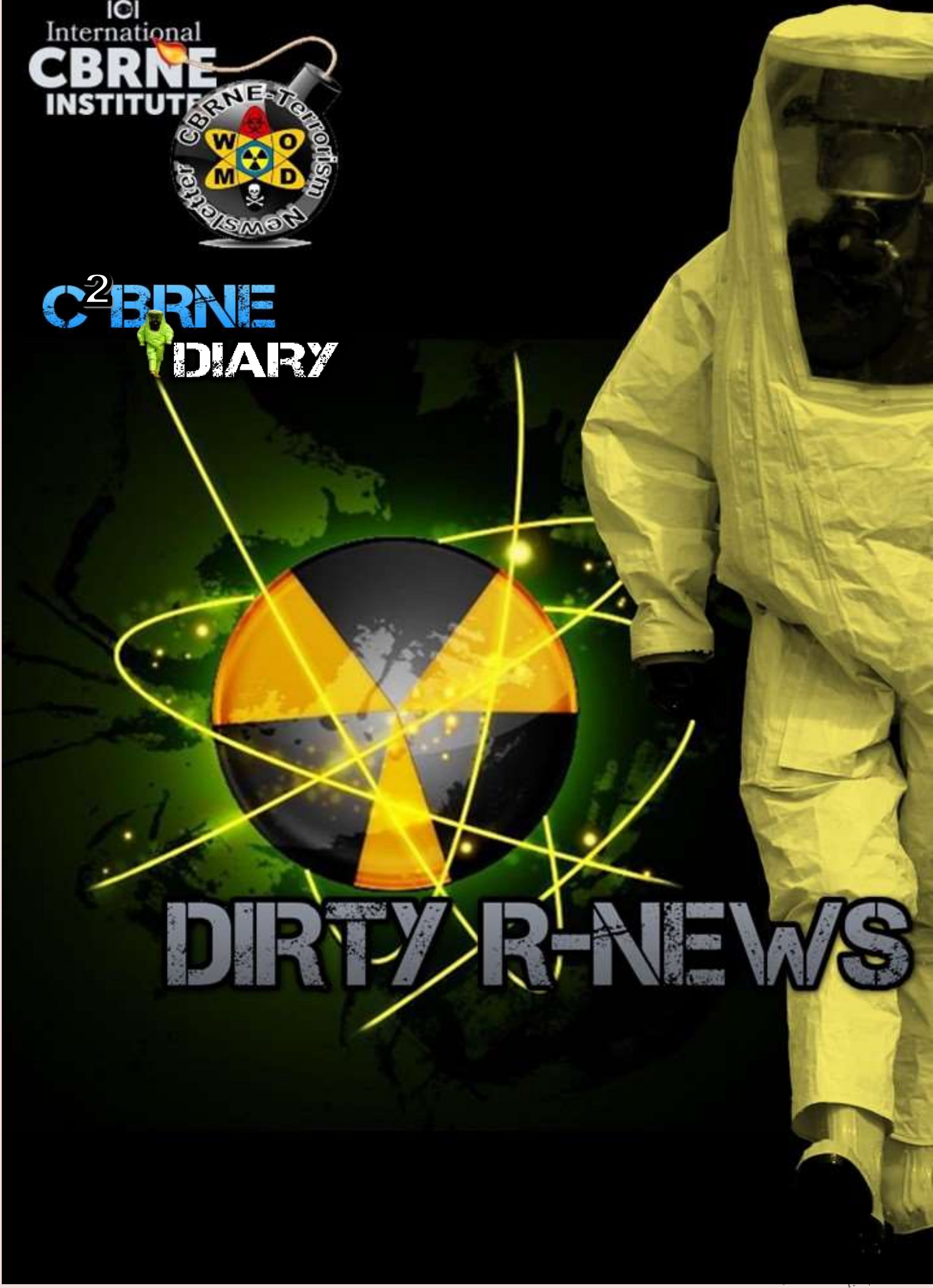


www.cbrne-terrorism-newsletter.com

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C2BRNE DIARY



DIRTY R-NEWS

Russia threatened to vaporize US cities — here are the areas in the US most likely to be hit in a nuclear attack

Source: https://www.businessinsider.com/likely-us-nuclear-targets-2017-5

Russian state media on Sunday made a shocking threat, even by its own extreme standards, that detailed how Moscow would annihilate US cities and areas after a nuclear treaty collapsed and put the Cold War rivals back in targeting mode.

Russian President Vladimir Putin has threatened a new Cuban Missile Crisis with deployments near the US's borders and to aim missiles at the cities that command armed forces — but Russia's media took it a step further by naming their new targets.

Hyping up a new hypersonic nuclear-capable missile, Russian state TV on Sunday evening said the Pentagon, Camp David, Jim Creek Naval Radio Station in Washington, Fort Ritchie in Maryland, and McClellan Air Force Base in California, would be targets, according to Reuters.

But the latter two have been closed for about two decades, making them strange choices for targets.

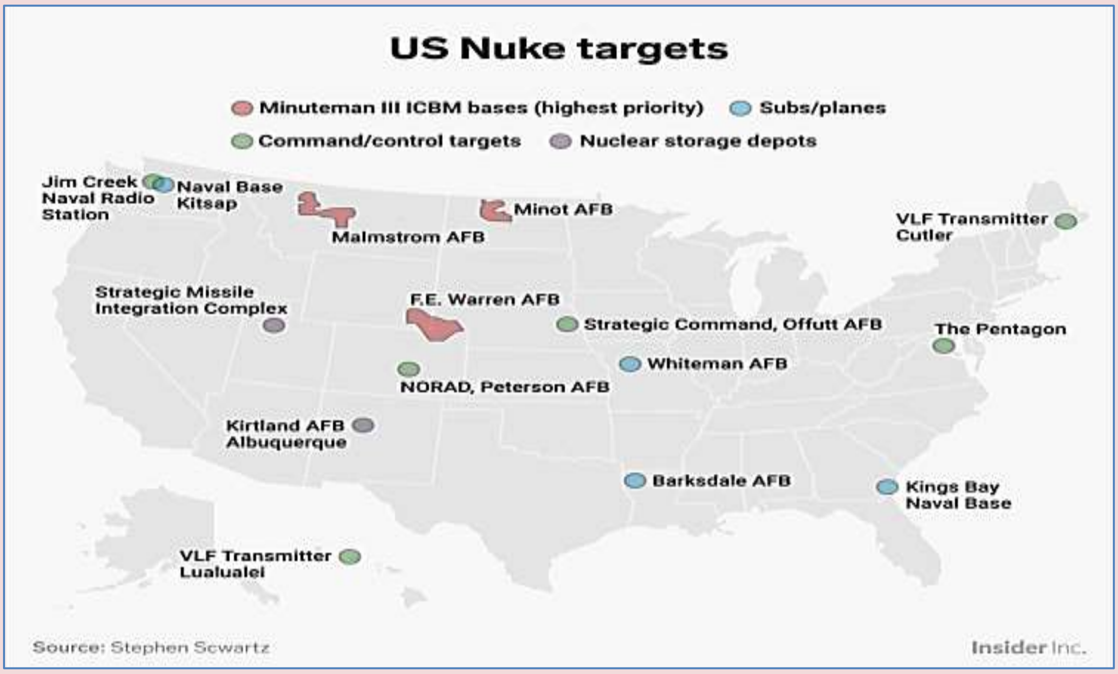
With most everything from the Russia or its heavily censored media, it's best to take its claims with a grain of salt. Instead of taking Russia's word for it when it comes to nuclear targets, Business Insider got an expert opinion on where Moscow would need to strike.

Since the Cold War, the US and Russia have drawn up plans on how to best wage nuclear war against each other; and while large population centers with huge cultural impact may seem like obvious choices, a smarter nuclear attack would focus on countering the enemy's nuclear forces.

So although people in New York City or Los Angeles may see themselves as being in the center of the world, in terms of nuclear-target priorities, they're not as important as states like North Dakota or Montana.

According to Stephen Schwartz, the author of "Atomic Audit: The Costs and Consequences of US Nuclear Weapons Since 1940," as the Cold War progressed and improvements in nuclear weapons and intelligence-collection technologies enabled greater precision in where those weapons were aimed, the emphasis in targeting shifted from cities to nuclear stockpiles and nuclear war-related infrastructure.

This map shows the essential points Russia would have to attack to wipe out the US's nuclear forces, according to Schwartz:



This map represents targets for an all-out attack on the US's fixed nuclear infrastructure, weapons, and command-and-control centers, but even a massive strike like this wouldn't guarantee anything. Skye Gould/Business Insider

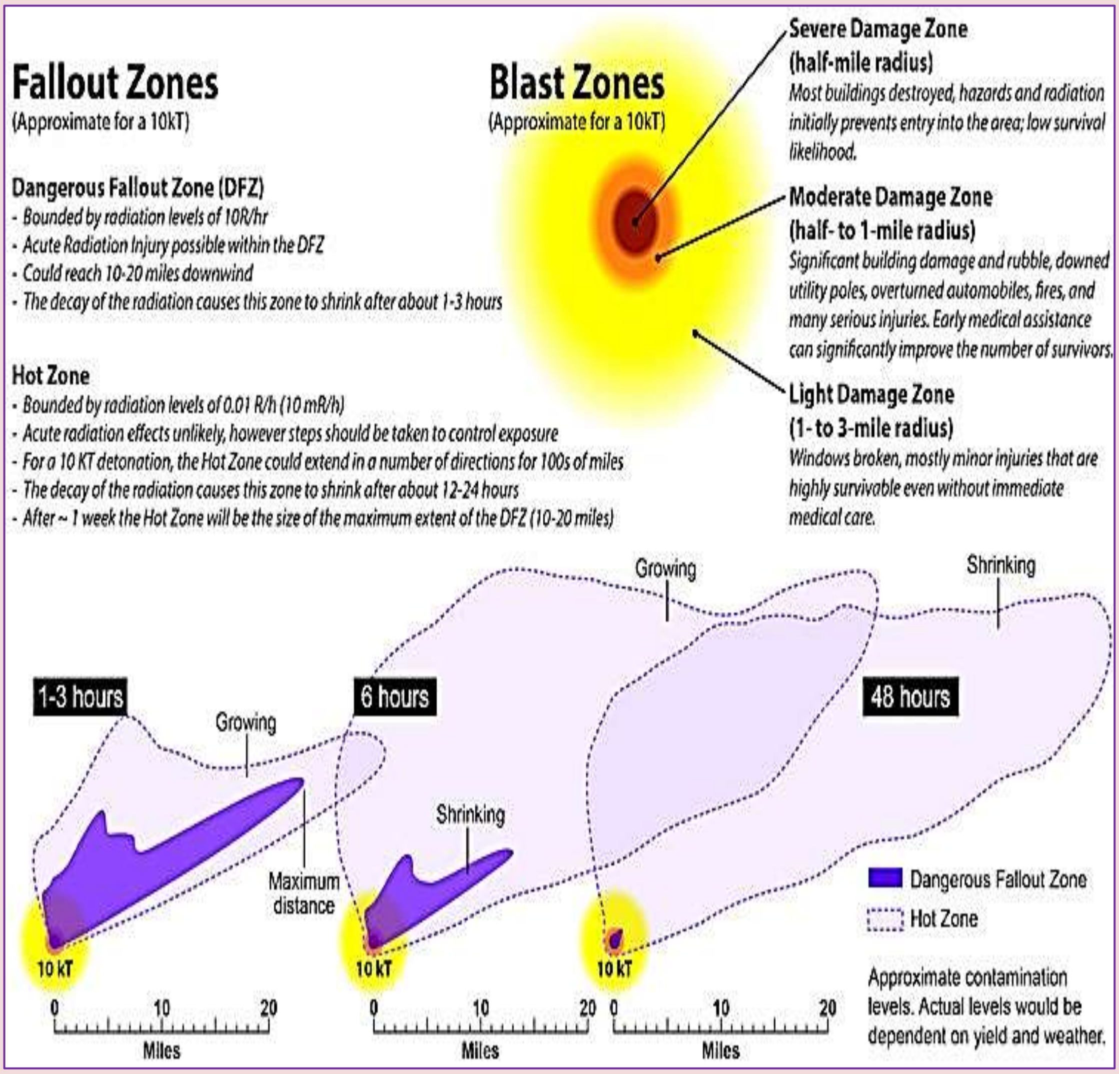
"It's exceedingly unlikely that such an attack would be fully successful," Schwartz told Business Insider. "There's an enormous number of variables in pulling off an attack like this flawlessly, and it would have to be flawless. If even a handful of weapons escapes, the stuff you missed will be coming back at you."

Even if every single US intercontinental ballistic missile silo, stockpiled nuclear weapon, and nuclear-capable bomber were flattened, US nuclear submarines could — and would — retaliate.

According to Schwartz, at any given time, the US has four to five nuclear-armed submarines "on hard alert, in their patrol areas, awaiting orders for launch."

Even high-ranking officials in the US military don't know where the silent submarines are, and there's no way Russia could chase them all down before they fired back, which Schwartz said could be done in as little as 5 to 15 minutes.

But a strike on a relatively sparsely populated area could still lead to death and destruction across the US, depending on how the wind blew. That's because of fallout.


Fallout Zones
(Approximate for a 10kT)

Dangerous Fallout Zone (DFZ)
- Bounded by radiation levels of 10R/hr
- Acute Radiation Injury possible within the DFZ
- Could reach 10-20 miles downwind
- The decay of the radiation causes this zone to shrink after about 1-3 hours

Hot Zone
- Bounded by radiation levels of 0.01 R/h (10 mR/h)
- Acute radiation effects unlikely, however steps should be taken to control exposure
- For a 10 KT detonation, the Hot Zone could extend in a number of directions for 100s of miles
- The decay of the radiation causes this zone to shrink after about 12-24 hours
- After ~ 1 week the Hot Zone will be the size of the maximum extent of the DFZ (10-20 miles)

Blast Zones
(Approximate for a 10kT)

Severe Damage Zone
(half-mile radius)
Most buildings destroyed, hazards and radiation initially prevents entry into the area; low survival likelihood.

Moderate Damage Zone
(half- to 1-mile radius)
Significant building damage and rubble, downed utility poles, overturned automobiles, fires, and many serious injuries. Early medical assistance can significantly improve the number of survivors.

Light Damage Zone
(1- to 3-mile radius)
Windows broken, mostly minor injuries that are highly survivable even without immediate medical care.

Approximate contamination levels. Actual levels would be dependent on yield and weather.

Dangerous radioactive fallout zones shrink rapidly after a nuclear explosion. Brooke Buddemeier/ Lawrence Livermore National Laboratory

The US has strategically positioned the bulk of its nuclear forces, which double as nuclear targets, far from population centers. But if you happen to live next to an ICBM silo, fear not.

There's a "0.0% chance" that Russia could hope to survive an act of nuclear aggression against the US, according to Schwartz. So while we all live under a nuclear "sword of Damocles," Schwartz added, people in big cities like New York and Los Angeles most likely shouldn't worry about being struck by a nuclear weapon.

Better monitoring of nuclear power plants, nuclear proliferation

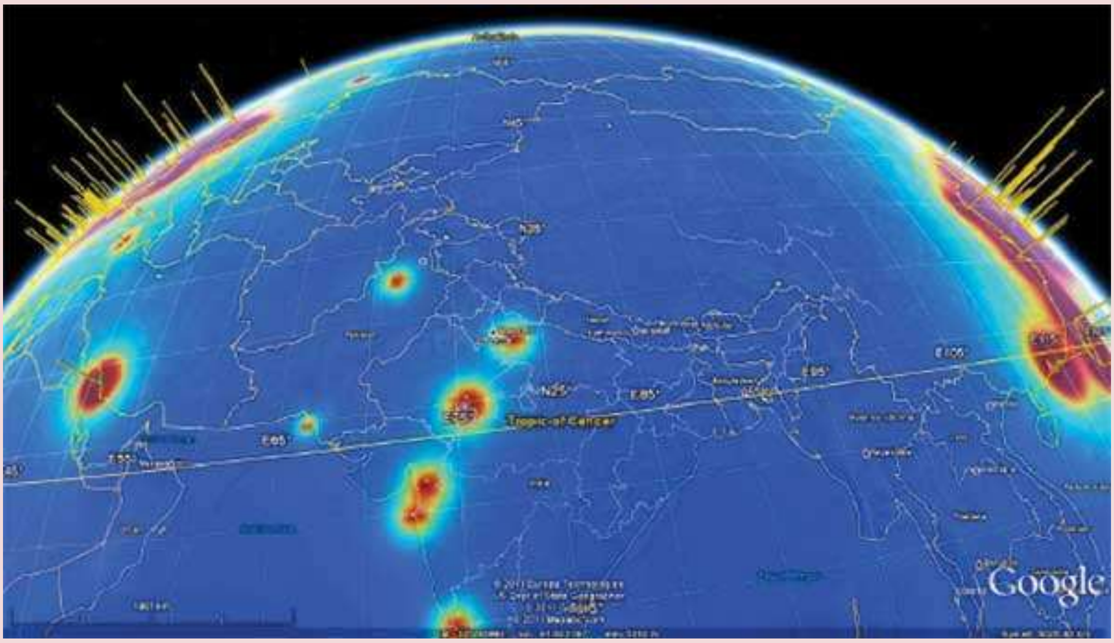
Source: http://www.homelandsecuritynewswire.com/dr20190226-better-monitoring-of-nuclear-power-plants-nuclear-proliferation

Feb 26 – The United Kingdom is investing nearly £10 million (about $12.7 million) in a joint project with the United States to harness existing particle physics research techniques to remotely monitor nuclear reactors.

Expected to be operational in 2024, the Advanced Instrumentation Testbed (AIT) project's 6,500-ton detector will measure the harmless subatomic particles called antineutrinos that are emitted by an existing nuclear power plant 25 kilometers, or about 15.5 miles, away. The National Nuclear Security Administration (NNSA) and Lawrence Livermore National Laboratory (LLNL) are partners in the research effort.

The project will test whether the technique could be scaled up in the future for more distant monitoring of nuclear sites, with the potential for nonproliferation applications.

The AIT detector is called WATCHMAN, an acronym for the WATer CHerenkov Monitor of ANtineutrinos. LLNL says that it will be constructed 1.1 kilometers underground at the Boulby mine in North Yorkshire — the deepest operating mine in Europe. AIT-WATCHMAN will be supported by the Boulby Underground Laboratory, an existing multidisciplinary deep-underground science facility operated by the UK's Science and Technology Facilities Council (STFC).



Abundant throughout the universe, and created by our own sun and other stars, neutrinos are among the most difficult fundamental particles to study, as they carry no electrical charge and rarely interact with ordinary matter.

Studying the properties of neutrinos and antineutrinos is an important component of wider physics research into the origins of the universe, especially the apparent imbalance between matter and antimatter.

“The Boulby site for AIT, with its proximity to an existing reactor complex, is the ideal location for our experiment,” said Adam Bernstein, the AIT-WATCHMAN project director and an LLNL physicist. “WATCHMAN and AIT give the physics and nonproliferation communities a rare opportunity to work together to harness neutrino detection for the practical purpose of non-intrusively monitoring nuclear reactors.”

The UK and U.S. have a long history of scientific collaboration, especially in translating the techniques used for basic science to solve real world problems, explained professor Mark Thomson, executive chair of the Science and Technology Facilities Council overseeing the UK delivery of the project. "Not only will this project help improve global security cooperation, it will provide a boost to joint research efforts into neutrinos and antineutrinos — research that could help solve some of the mysteries around the creation of the universe."

Within the UK, physicists from the Universities of Sheffield, Edinburgh, and Liverpool have been working with national defense and security agencies, including the Atomic Weapons Establishment (AWE), on the AIT-WATCHMAN project.

"The beauty of AIT-WATCHMAN is that it enables us to learn more about the universe on so many levels, while also supporting an innovative program of non-proliferation," said Matthew Malek of the University of Sheffield. "We will study one of the fundamental building blocks of nature, the neutrino, and we will use it to search for supernovae in other parts of our galaxy. At the same time, we are developing new techniques that will have a positive impact on Britain and the rest of the world."

"Identifying nuclear reactors from the emission of antineutrinos at a distance of tens of kilometers will provide a key capability in supporting the UK government's nuclear nonproliferation mission," added Jonathan Burns, from the AWE. "The AIT project is an excellent example of detector technology, developed by the physics research community in the UK and internationally, being used to address global security challenges."

"It is great to be having this world-class research project come to the UK and the North East region," said professor Sean Paling, head of the existing STFC Underground Science Laboratory at Boulby Mine. "Boulby is a special place for science in the UK and already supports a range of pure and applied science studies from astrophysics to studies of life on Earth and beyond. This new project will complement and enhance the existing program and increase the laboratory's standing in the international science community."

In the U.S., the participating institutions are LLNL, Lawrence Berkeley National Laboratory, Pacific Northwest National Laboratory, Los Alamos National Laboratory, Brookhaven National Laboratory, Boston University, Iowa State University, Middlebury Institute of International Studies, Pennsylvania State University, and the Universities of California (at Berkeley, Davis and Irvine), Hawaii, Michigan, Pennsylvania and Wisconsin.

Turkey wants to see world free of nuclear weapons: FM

Source: https://www.aa.com.tr/en/europe/turkey-wants-to-see-world-free-of-nuclear-weapons-fm/1402503

Feb 25 – Turkey's ultimate goal is to see a world free of nuclear weapons, the country's foreign minister said on Monday.

Mevlut Cavusoglu's remarks came at the UN's Disarmament Conference held in Geneva, Switzerland.

"Disarmament, proliferation of nuclear weapons and weapon control is of critical importance for global security and peace," Cavusoglu said, adding that Turkey faced numerous risk and threats in its region.

He noted that Turkey was simultaneously fighting several terror groups -- such as Daesh, PKK/PYD and FETO -- while the civil war in Syria has almost entered its 9th year.

The foreign minister underlined the conference was a unique platform to discuss the issue of weapons of mass destruction.

He emphasized that a world without nuclear weapons could only be achieved by implementing the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) in a successive and universal manner.

He also called on the attendees to hold an international conference on the "weapons of mass destruction in the Middle East".

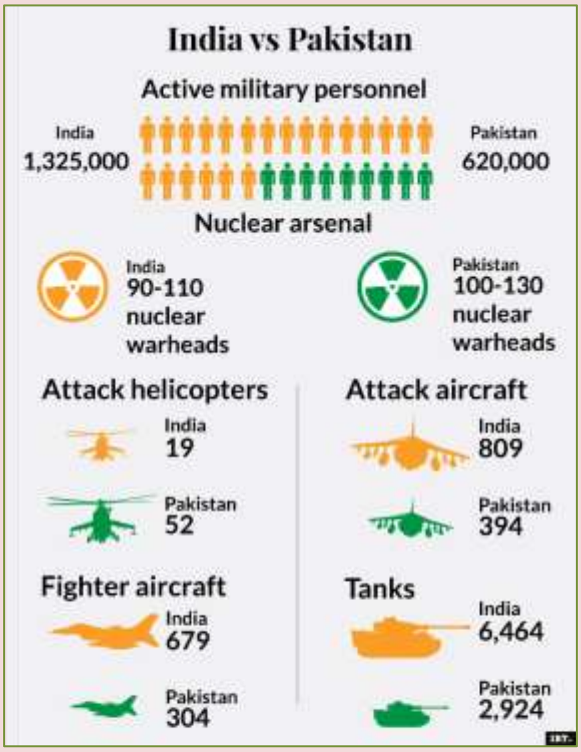
EDITOR'S COMMENT: In an ugly world, we always enjoy a good joke!

India vs. Pakistan: As War Threats Loom, Here's How the Nuclear Rivals' Militaries Compare

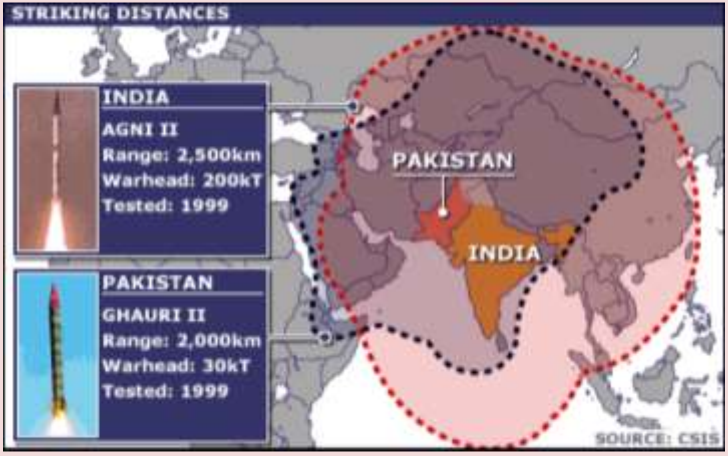
Source: https://www.newsweek.com/india-pakistan-war-military-nuclear-vs-1348109

Feb 28 – India and Pakistan have once again threatened to descend into war after a recent exchange of hostilities across their mutually disputed border, and the state of their armed forces has captured international attention.

Following the suicide bombing two weeks ago that killed more than 40 Indian troops and was claimed by a Pakistan-based Sunni militant group, the Indian air force on Tuesday conducted strikes on what it said were jihadi camps across the contested Line of Control in the Kashmir border region. The following day, Pakistan reportedly downed two Indian MiG-21 jets, arresting the pilot of one, while India claimed to have destroyed a Pakistani F-16.



The actual events of the past couple of days remain hazy, as contradictory statements have emerged from both sides, but the heightened risk of a greater conflict was clear. Pakistani Prime Minister Imran Khan struck a conciliatory tone, promising to release the captured Indian pilot as "a peace gesture."



His Indian counterpart, Narendra Modi, however, has been notably silent amid the recent crisis, saying only that "India will fight, live, work and win as one" at a press conference that made no mention of negotiations to cool down the heated feud.

The South Asian rivals, divided by the bloody 1947 partition of India, command two powerful militaries armed with nuclear weapons that remain a constant source of concern for international powers. Pakistan was believed to have a nuclear stockpile of about 140, with India having an estimated 130, according to the Federation of American Scientists.

Neither nation was a signatory to the 1968 Treaty on the Non-Proliferation of Nuclear Weapons, and both were among the most recent nations to test their weapons of mass destruction, followed only by North Korea. India and Pakistan both have methods of delivering strategic strikes by land and air, but the former was part of an even more exclusive club, being one of only five powers to have a nuclear submarine capable of launching nuclear-capable missiles up to 435 miles away. The others are the United States, Russia, China and France.

New Delhi far outspends Islamabad on defense, devoting some $48.4 billion to its rival's $9.7 billion, according to the Lowey Institute's 2018 Asia Power Index, which ranked India fourth and Pakistan 14th in terms of strength and influence. India, the world's second-largest population, also outnumbers Pakistan in terms of manpower with 2,798,800 military and paramilitary forces versus 935,800.

Citing figures compiled by the Institute for International and Strategic Studies, Al Jazeera reported Thursday that India has 3,565 battle tanks, 3,100 infantry fighting vehicles, 336 armored personnel carriers and 9,719 pieces of artillery. Pakistan has 2,496 tanks, 1,605 armored personnel carriers and 4,472 artillery guns, including 375 self-propelled howitzers.

In the air, India could mobilize 814 combat aircraft, nearly twice that of Pakistan, which has 425. India also has a much larger fleet, including an aircraft carrier, 16 submarines, 14 destroyers, 13 frigates, 106 patrol and coastal combatant vessels and 75 combat-capable aircraft. Pakistan, which has much less access to the sea, commands nine frigates, eight submarines, 17 patrol and coastal vessels and eight combat-capable aircraft.

Global Firepower's 2018 rankings placed India fourth in terms of overall military capabilities, behind only the U.S., Russia and China. Pakistan came in 17th, below Israel and above North Korea—the two other nuclear-suspected nations that have refused to sign the Nuclear Non-Proliferation Treaty.

As for international allies, the two countries were split by a Cold War–era rivalry between Russia and China. Moscow and New Delhi have long enjoyed close ties that were demonstrated by India's recent purchase of S-400 surface-to-air missile defense systems in defiance of Washington's sanctions. Beijing has invested heavily in Islamabad, seeing it as a vital node in the global One Belt, One Road initiative.

Russia and China have called for calm and restraint, as has the U.S. In remarks that followed his Hanoi, Vietnam, summit with North Korea, President Donald Trump told reporters that his administration has been in contact with India and Pakistan. He said that current tensions were hopefully "going to be coming to an end" and that peace was "probably going to be happening."

Cancer patient's treatment leaves radiation contamination in crematory

Source: https://edition.cnn.com/2019/02/26/health/radioactive-crematory-study/index.html

Feb 26 – Radioactivity was detected on the oven, vacuum filter and bone crusher of an Arizona crematory where a deceased man who'd received radiation therapy was incinerated, according to a new case report. Worse still, a radioactive compound unrelated to the dead man was detected in the urine of an employee there.

"It is plausible that the crematory operator was exposed while cremating other human remains," Dr. Nathan Yu of the Department of Radiation Oncology at the Mayo Clinic in Phoenix and his co-authors wrote in the case report, published Tuesday in JAMA.

Radioactive compounds are used in some medical procedures to diagnose and treat disease. PET scans, for example, use a radioactive dye to help doctors see tissues and organs, and some cancer treatments use radioactive compounds to target tumor cells.

The case report tells of a 69-year-old man with a pancreatic tumor who was treated with nuclear medicine at an Arizona hospital in 2017. He died days later and was cremated five days post-treatment.

On learning of the patient's death, a safety officer from the hospital's radiation department notified the crematorium and, one-month post-treatment, surveyed the equipment using a Geiger counter. A urine sample from an employee was also analyzed.

Incineration "volatilizes" radiopharmaceuticals in a dead body, and the radioactive contamination can be "inhaled by workers (or released into the adjacent community) and result in greater exposure than from a living patient," Yu and his co-authors wrote.

The Geiger counter picked up a range of radioactivity (primarily the isotope contained in the medicine given to the patient) on equipment in the crematorium: the oven, vacuum filter and bone crusher.

A different isotope was detected in the employee's urine. Because he'd never undergone a medical procedure using radiopharmaceuticals, the researchers believe that he inhaled the radioactive contaminant while incinerating other bodies.

With the current US cremation rate topping 50%, Yu and his co-authors believe that more studies are needed to understand the extent of radiation contamination at crematoriums and possible health hazards for workers.

Dr. Daniel Appelbaum, chief of nuclear medicine and PET Imaging at the University of Chicago Medical Center, said that although radiotherapies have been around for decades, they are "very recently becoming much more common."

"We have a bunch of new radiotherapies that have just arrived and several more that are on the near horizon for some very common cancers, including prostate cancer," said Appelbaum, who was not involved in the case report. The most recent figures available, from 2006, indicate that 18.6 million nuclear medicine procedures were performed in the United States and nearly 40 million worldwide.

Since this is "only going to become more of a common issue going forward," we need to think about ways to identify and notify crematoriums of the potential risk and evaluate the amount of possible postmortem radioactive contamination, he said.

There are guidelines and regulations on this, Appelbaum said. The Nuclear Regulatory Commission has set a limit below which is safe and does not "pose any significant risk to an individual. This crematorium worker did not receive that amount; he did not receive a 'significant' amount," he said.

"We live in a world with radioactivity. We can't avoid all of it," he said. "You go on an airplane, you climb a mountain, you even watch TV, you've received some radiation." Still, he said, "if there are reasonable and fairly straightforward and simple things that we can do to minimize radioactivity, why not do that?"

Regulations for cremation of patients who'd received nuclear medicine vary by state, and there are no regulations at the federal level in the United States. Yu and his co-authors call for "future safety protocols" that include "postmortem management, such as evaluating radioactivity in deceased patients prior to cremation and standardizing notification of crematoriums."

Appelbaum believes that new guidelines will come, but in the meantime, crematoriums can take it upon themselves and protect their workers. "Start with robust enforcement of mask and gloves and handling techniques," he said.

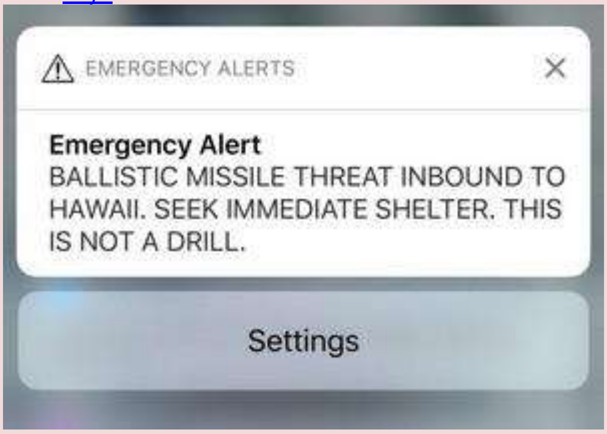
Lessons learned from Hawaii false nuclear attack alarm

Source: http://www.homelandsecuritynewswire.com/dr20190228-lessons-learned-from-hawaii-false-nuclear-attack-alarm

Feb 28 – When people in the Hawaiian Islands received a false alarm text message that said “Ballistic missile threat inbound to Hawaii. Seek immediate shelter. This is not a drill” in January 2018, the result was not panic, according to new research from the University of Georgia. A team of researchers analyzed the unprecedented event—a text that was announced as a false alarm 38 minutes later—to better understand how people react in the face of a potentially catastrophic event. What they found was that people sought information that could verify their risk and help them decide what to do next.

They asked island residents to respond to questions about their perceived level of risk, what actions they took after seeing the warning, and whether the false alarm affected their trust in future warnings.

UGA says that the researchers found that most respondents didn't seek immediate shelter, but instead spent time looking for more information about the incoming attack. This behavior is known among disaster researchers as "social milling."



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

"It's getting a sense of what other people are doing," said Sarah DeYoung," an assistant professor in the Institute for Disaster Management at UGA's College of Public Health. "Social milling means, let's see what's going on, observing the scene but also checking in with others."

When people are milling, she said, they are more likely to find the information they need to make the best decision about what to do. Respondents said they looked to major news outlets and social media to corroborate the alert message.

Social media played a key role in helping to spread the word about the false alarm. Hawaii congressional leader Tulsi Gabbard was quick to tweet the warning was an error, and 16 percent of respondents said they saw and shared the tweet.

"There was a spillover effect of social media that went beyond people who follow it," said DeYoung, the study author. "And it also speaks to the value of following social media because those people who did were able to deliver that message to their immediate network of people."

In the days following the false alarm, respondents reported feeling a mix of emotions. Among feelings of trauma and anger, some respondents also said they didn't trust their local government to handle future emergencies.

The good news for emergency managers and local government, said DeYoung, is that broader findings from disaster research says that false alarms generally don't cause people to disregard future alarms, but she added that respondents in her study said they'd be more likely to trust future tsunami warnings than future missile warnings.

DeYoung said the way to overcome doubt about future emergencies is to send out official warning messages across more platforms than the wireless emergency alert system.

"People wanted multiple cues to validate the warning," she said, "so in order to increase belief and trust in the warning, it should go across multiple channels."

— Read more in Sarah E. DeYoung et al., ""Death was not in the agenda for the day": Emotions, behavioral reactions, and perceptions in response to the 2018 Hawaii Wireless Emergency Alert," International Journal of Disaster Risk Reduction (2 February 2019).

How the US and China collaborated to get nuclear material out of Nigeria — and away from terrorist groups

Source: https://www.defensenews.com/news/pentagon-congress/2019/01/14/how-the-us-and-china-collaborated-to-get-nuclear-material-out-of-nigeria-and-away-from-terrorist-groups/

Jan 14 – At a staging ground in Ghana, a group of nuclear experts watched the clock and nervously waited for the news.

The team — a mix of American, British, Norwegian and Chinese experts, along with Czech and Russian contractors — were supposed to head into the Kaduna region of Nigeria to remove highly enriched uranium from a research reactor that nonproliferation experts have long warned could be a target for terrorists hoping to get their hands-on nuclear material.

But with the team assembled and ready to go on Oct. 20, 2018, the mission was suddenly paused, with the regional governor declaring a curfew after regional violence left dozens dead. As American diplomats raced to ensure the carefully calibrated window of opportunity didn't shut, the inspectors were unsure if the situation would be safe enough to complete the mission.

"Frankly speaking, yeah, I was nervous for my people on the ground and everyone else who was on the ground. It was important, but we had to go at it in a prudent way" said Peter Hanlon, assistant deputy administrator for material management and minimization, an office within the U.S. National Nuclear Security Administration. "As someone responsible for this organization, I was nervous."

Moving the nuclear material out of Nigeria has been a long-sought goal for the United States and nonproliferation advocates. But the goal has taken on increased importance in recent years with the rise of militant groups in the region, particularly Boko Haram, a group the Pentagon calls a major terrorist concern in the region.

Underscoring the importance of the operation: the key role China played in transporting and storing the uranium, with the operation happening just hours after U.S. President Donald Trump made an explicit threat to China about growing America's nuclear arsenal.

For those gathered in Ghana that evening, however, the focus was on watching the clock and hoping that the negotiators could come through and allow them to finally get the material out of Nigeria — and get everyone home safely.

'Material that is attractive to terrorists'

It was the mid-1990s when Nigeria, with technical support and backing from China, began work on what would become Nigerian Research Reactor 1, located at Ahmadu Bello University in Kaduna. The location opened in 2004, and is home to roughly 170 Nigerian workers.

NIRR-1 is classified as a miniature neutron source reactor, designed for "scientific research, neutron activation analysis, education and training," per the International Atomic Energy Agency. Essentially, the reactor powers scientific experiments, not the local grid.

The design, however, used highly enriched uranium, or HEU, a type of nuclear substance often referred to by the general public as weapons-grade uranium. This kind of uranium forms the core of any nuclear weapons material, and the Nigerian material was more than 90 percent enriched, making it particularly attractive for anyone looking to use it.

Since NIRR-1 went online, however, improvements in technology meant that experiments involving highly enriched uranium could now be run with a lesser substance. Across the globe, the IAEA and its partners have worked to swap out weapons-grade material with low enriched uranium, or LEU, which is enriched at less than 20 percent, and hence unusable for weapons. In all, 33 countries have now become free of HEU, including 11 countries in Africa.

With just over 1 kilogram of HEU, the Nigerian material, if stolen, would not be nearly enough to create a full nuclear warhead. However, a terrorist group would be able to create a dirty bomb with the substance or add the material into a stockpile gathered elsewhere to get close to the amount needed for a large explosion.

In a statement released by the IAEA, Yusuf Aminu Ahmed, director of the Nigerian Centre for Energy Research and Training, was blunt about his concerns over keeping the weapons-grade material in his country. "We don't want any material that is attractive to terrorists," he said.

And the nature of these types of reactors, used primarily for research, means they are ideal targets for terrorist groups looking for nuclear material, said Jon Wolfsthal, a nuclear expert who served as senior director for arms control and nonproliferation at the U.S. National Security Council from 2014 to 2017.

"They're small reactors, they're not power reactors where the fuel is so radioactive it kills you," he said. "This is very attractive to a proliferation point of view, and they are research reactors, so they are often at universities without high security."

All of which gave the governments involved incentive to get the material out of Nigeria sooner rather than later, and which led to the group of experts sitting in Ghana, waiting for a call.

The day of

It wasn't until Oct. 22 — two days after the initial delay — that American diplomats, working with their Nigerian counterparts, were able to get an exemption to the curfew in Kaduna and prepare to roll out. But for security reasons, an operation that usually took days would have to happen in just one 24-hour period.

At 1:30 a.m. on Oct. 23, a Russian Antonov An-124 cargo plane touched down in Nigeria. Aboard were the team of experts, but also a TUK-145/C — a 30-ton cargo container designed specifically for moving such uranium from place to place and doing so securely.

From the outside, the TUK-145/C looks like a large, silver cylinder, designed to keep its precious cargo safe even in the event of a plane crash — as part of the safety testing before certification, the container is put into a pool of jet fuel, with the whole thing then lit on fire for 60 minutes. If you somehow could cut it down the middle, the container would appear to be two parts — an outer shell for security, and an innermost cask containing the spent uranium rods.

Both the plane and the TUK-145/C are owned and operated by the Russian Sosny Research and Development Company, a specialty firm that has been used in other HEU removal procedures.

Loading the equipment off the plane took hours, as did the trip from the airstrip to the reactor. But finally, the team arrived at the reactor around 9 a.m. The group now included U.S. State Department security and Nigeria's Army First Division, considered a top-end unit of the Nigerian military.

Tiffany Blanchard-Case, a nuclear expert from the National Nuclear Security Administration, was one of the officials on the ground to oversee the transfer. She described a "grueling" day as the team rushed to condense what needed to be done into the secure window.

Technical experts from Nigeria's Centre for Energy Research and Training stand over the miniature neutron source reactor and prepare to load the HEU reactor core into an interim transfer cask. (U.S. National Nuclear Security Administration)

“No one was concerned about breaks, no one was concerned about lunch, everyone was just working 100 percent in order to make sure we could meet this schedule,” she said. “A long day for everyone.”

Getting at the uranium is tricky business. The reactor core, which holds the actual material, is located at the bottom of a six-meter-deep pool. Above the pool, technicians have to create a platform and then center a vessel, known as the interim transfer cask, above the core. The cask contains a grapple, which reaches into the reactor and lifts out the core; when the core is loaded in, a plug is placed over the core and the cask is sealed, loaded onto the Skoda shipping cask, and then that unit is sealed inside the TUK-145/C.

Replacing HEU with LEU in research reactors naturally requires caution, as anything nuclear-related comes with risks. But the Nigerian mission was particularly difficult because of security concerns, Hanlon said. He noted that Boko Haram, while not in the Kaduna region, has been operating in Nigeria for quite some time.

“We had concerns about the security on the ground, in the region. Working very closely with the U.S. embassy, there were additional security requirements put upon us and limitations for us on having people on the ground at the facility itself,” Hanlon said.

Hanlon and Blanchard-Case declined to discuss details of the security, other than to say it was heavy and that the U.S. State Department added extra forces as part of the agreement to allow the team to go in.

Alice Hunt Friend, a regional expert with the Center for Strategic and International Studies, said that Boko Haram is not necessarily “active” in the region, but added that an attack by the group in that area shouldn’t be ruled out.

The TUK-145/C, carrying a load of highly enriched uranium from the Nigerian reactor, is loaded onto a plane headed for its final destination: China. (U.S. National Nuclear Security Administration)

“The city is a transport hub, pretty much right between Abuja and Kano on the main route. It is also in the belt that has experienced a lot of communal violence over the past 10 years, so I can also imagine that security for HEU sites would be of concern more generally, even absent a specific threat,” she said. “With much of the Nigerian military concentrating on the northeast, I would imagine security for sites in Kaduna is inconsistent.”

Boko Haram is just one threat that worries security teams on the ground, said Peter Haynes, an analyst with the Center for Strategic and Budgetary Assessments.

“Fueled by ethnic and religious differences, there has been lots of violence in the Kaduna region in the last six months, but that has been between Fulani Muslim herders and Christian villagers,” said Haynes, adding that it is not “uncommon as of late to have curfews to dampen the communal violence.”

While the technicians were able to leave the country once their daylong mission was complete, security on site remained thick for the next five weeks as administrators worked the logistics and clearances needed to fly nuclear material over other nations' airspace. Asked about the security level during this down period, Dov Schwartz, an NNSA spokesman, said that “extensive planning went into ensuring the removed highly enriched uranium was safe and secure prior to transport."

"All of our partners understood that operational security was paramount,” Schwartz said. "The world is a safer place today as a result of the determined work to remove this weapons useable Uranium from Nigeria.”

Finally, on Dec. 4, the HEU was escorted by the Nigerian military toward the An-124, loaded onto the aircraft and sent on its way to its final destination.
The material was heading for China.

China's role

The removal operation cost roughly $5.5 million, with the United States contributing $4.3 million. The United Kingdom ($900,000) and Norway ($290,000) also chipped in. But while it didn't contribute money, China's role in the operation was outsized — and occurred as the war of words from the Trump administration toward Beijing was reaching a fever pitch, one that did not die down in the weeks to come.
As the October operation was just hours from starting, U.S. President Donald Trump took to the press to discuss nuclear material and China.
"Until people come to their senses, we will build [the nuclear arsenal] up," Trump told reporters just hours before the Nigeria operation was to begin. "It's a threat to whoever you want. And it includes China, and it includes Russia, and it includes anybody else that wants to play that game. You can't do that. You can't play that game on me."
By the time the Antonov plane — carrying the HEU, along with American inspectors and security — arrived at Shijiazhuang airport in China on Dec. 6, the arrest of a Chinese technology executive in Canada had inflamed fears of a trade conflict between the two countries.
Once the material landed in China, local officials took possession of the uranium, marking the end of the Nigerian mission — but not necessarily the end of the material.

Chinese President Xi Jinping, right, greets Nigerian President Muhammadu Buhari during a plenary session of the 2016 Nuclear Security Summit on April 1, 2016, in Washington, D.C. The summit was organized to highlight accomplishments and make new commitments toward reducing the threat of nuclear terrorism. (Alex Wong/Getty Images)

Hanlon acknowledged the United States doesn't know what China will do with the material, noting they could dispose of it in whatever way they see fit. But Wolfsthal, the former National Security Council staffer, doesn't think Beijing will let it go to waste.
"My guess is China will reprocess it and then recycle some of the materials," Wolfsthal said. "It could end up in China's stockpile after being reprocessed, or used for civilian fuel. But getting it out of Nigeria is the biggest thing."
In a statement released by the IAEA, Shen Lixin, deputy director general of the department of business development and international cooperation at the China National Nuclear Corporation, said the project "manifests the determination and joint effort of several governments and organizations in preventing nuclear proliferation."
"This is also a demonstration of CNNC's meeting its social responsibilities and the commitment to peaceful uses of nuclear energy," the statement continues. "CNNC is more than willing to work together and cooperate whole heartedly with relevant parties to facilitate other MNSR conversion projects."
That the United States and China were able to ignore politics to get the HEU removal done shouldn't be a surprise, Wolfsthal said. Traditionally, countries that supply uranium to partners around the world take that material back if needed.
"Even though the national level conversation is really poor because of trade and other issues, the technical collaboration between laboratories, between nuclear engineers, that's generally gone pretty well," he said. He added that China has invested heavily in LEU over

the last decade, and therefore also has an interest in encouraging others to switch to that technology.

Whether that cooperation continues if relations between the two nations continue to deteriorate will be a true test going forward. On Jan. 3, the U.S. State Department issued a travel warning for China, urging American citizens to use caution when traveling, as the Chinese government may detain Americans.

And an agreement to develop new nuclear technology between CNNC and TerraPower, an American nuclear firm led by Microsoft founder Bill Gates, appears doomed due to American restrictions on technology sharing with China.

Hanlon, for his part, is optimistic that China and the U.S. will continue to work on nuclear security.

“These nuclear security efforts of removing this dangerous material, most countries agree with that,” he said. “That work has continued unabated.”

Adm (ret.) James Stavridis: Nukes aren’t North Korea’s only threat

Source: https://www.the-dispatch.com/opinion/20190303/stavridis-nukes-arent-north-koreas-only-threat

Mar 03 – There is a major danger that the narrow focus on North Korea’s nuclear weapons obscures: North Korean leader Kim Jong Un holds the whip in a three-ring circus of weapons of mass destruction.

The other two rings, adjacent and in many ways more frightening, feature chemical weapons and — above all — biological threats.

The North Koreans are suspected by United States and South Korean intelligence agencies of holding substantial amounts of a variety of biological agents, including smallpox, botulism, typhoid and anthrax. A former Pentagon official who is in charge of countering such programs told reporters that North Korean bioweapons are “advanced, underestimated and highly lethal.”

Bioweapons have some advantages over nuclear weapons in terms of spreading terror: They can easily be smuggled across borders, and their use can be very hard to attribute, unlike a nuclear weapon with an obvious origin.

The final ring of the weapons of mass destruction circus — chemical weapons — is equally disturbing. In 2017, two North Korean agents allegedly killed Kim’s half-brother at a Malaysian airport using the nerve agent VX.

The North Korean military routinely uses simulated chemical weapons when it conducts drills and exercises, and could easily incorporate nerve agents into artillery barrages of Seoul from just over the border.

South Korean intelligence agencies say the North may have as much as 5,000 tons of chemical agents, possibly including ricin, mustard gas, hydrogen cyanide and the nerve agent tabun. North Korea is one of just three nations that have refused to sign the international Chemical Weapons Convention.

Would Kim dare such an attack? There might be some strategic sense. He knows that deploying a nuclear weapon would be signing his own death warrant. But he might be able to create a far more ambiguous situation in which he could consider using some biological or chemical element.

And while U.S. and South Korean forces are trained to operate after such an attack, the civilians on the peninsula are essentially undefended — including the families of 28,000 U.S. servicemen stationed there.

In preparing for this threat, Washington has considerable work to do. It should start by increasing intelligence collection specifically regarding chemical and bio-threats, working in concert with the South Korean allies. At home, there needs to be more research and development of technological counters to known agents.

Above all, the U.S. must bring greater global attention to the threat. This means international pressure on North Korea to sign global agreements banning such weapons; making those weapons part of the agenda alongside nukes in future summit negotiations; and pressuring Russia and China to persuade Kim to rid himself of any stockpiles before sanctions can be fully lifted.

Pursuing a diplomatic conclusion to the standoff on the Korean peninsula is the path forward.

But the U.S. should put other weapons of mass destruction on the table as well.

James Stavridis, *a retired U.S. Navy admiral and former military commander of NATO, is a Bloomberg News columnist.*

Report Managing a Nuclear-Armed North Korea

Source: https://fas.org/wp-content/uploads/media/FAS-DPRK-SG.pdf

The FAS International Study Group on North Korea Policy – 14 experts from 5 countries – released their report providing recommendations to the United States and allies on managing a nuclear-armed North Korea.

US agree to build six nuclear power plants in India

Source: https://www.thehindu.com/news/international/india-us-agree-to-build-six-nuclear-power-plants-in-india/article26529257.ece

Mar 14 – **India and the U.S. said they have agreed to build six American nuclear power plants in India, in a boost to bilateral civil nuclear energy cooperation.**

The two countries said this in a joint statement issued at the conclusion of the 9th round of India-U.S. Strategic Security Dialogue, co-chaired by Foreign Secretary Vijay Gokhale and Andrea Thompson, the U.S. Under Secretary of State for Arms Control and International Security, on March 13.

“They committed to strengthen bilateral security and civil nuclear cooperation, including the establishment of six U.S. nuclear power plants in India,” the joint statement said.

India and the U.S. signed a historic agreement to cooperate in civil nuclear energy sector in October 2008. The deal gave a fillip to bilateral ties, which have been on an upswing since.

A major aspect of the deal was the Nuclear Suppliers Group (NSG), that gave a special waiver to India enabling it to sign cooperation agreements with a dozen countries.

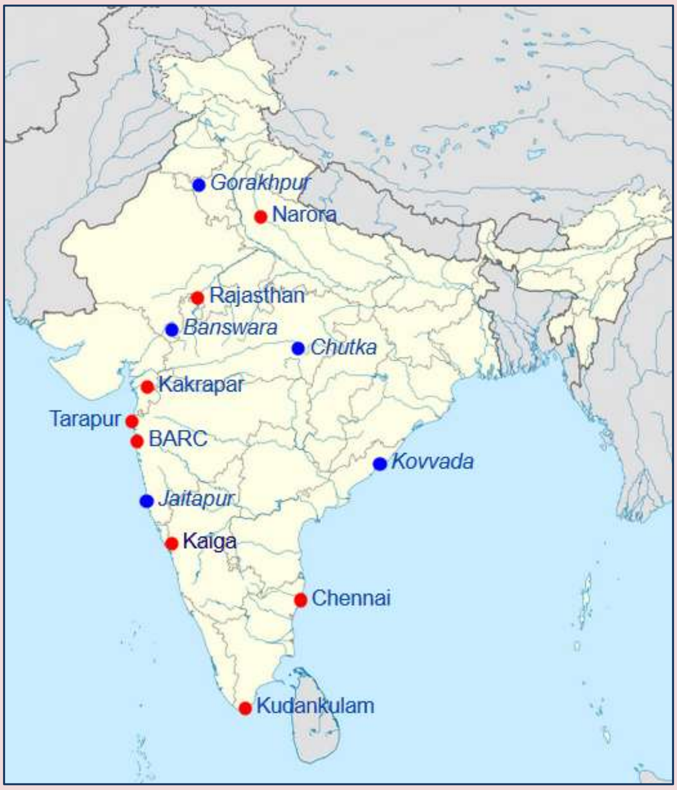
Post-waiver, India signed civil nuclear cooperation agreements with the U.S., France, Russia, Canada, Argentina, Australia, Sri Lanka, the U.K., Japan, Vietnam, Bangladesh, Kazakhstan and South Korea.

On March 13, the United States also reaffirmed its strong support to India’s early membership in the 48-member NSG. Notably, China has blocked India’s pending membership to the elite grouping that seeks to prevent proliferation of nuclear weapons.

During the meeting, the two sides exchanged views on a wide range of global security and non-proliferation challenges and reaffirmed their commitment to work together to prevent the proliferation of weapons of mass destruction and their delivery systems and to deny access to such weapons by terrorists and non-state actors.

On March 12, Indra Mani Pandey, India’s Additional Secretary for Disarmament and International Security Affairs, and Yleem D. S. Poblete, U.S. Assistant Secretary of State for

Arms Control, Verification and Compliance, co-chaired the third round of India-U.S. Space Dialogue. The two delegations discussed trends in space threats; respective national space priorities; and opportunities for cooperation bilaterally and in multilateral fora.



Nuclear power is the fifth-largest source of electricity in India after coal, gas, hydroelectricity and wind power. As of March 2018, India has 22 nuclear reactors in operation in 7 nuclear power plants, having a total installed capacity of 6,780 MW. Nuclear power produced a total of 35 TWh and supplied 3.22% of Indian electricity in 2017. Six more reactors are under construction with a combined generation capacity of 4,300 MW. In October 2010, India drew up a plan to reach a nuclear power capacity of 63 GW in 2032, but after the 2011 Fukushima nuclear disaster in Japan people around proposed Indian nuclear power plant sites have launched protests, raising questions about atomic energy as a clean and safe alternative to fossil fuels

● Active ● Planned

Easier access to radioactive waste

Source: http://www.homelandsecuritynewswire.com/dr20190313-easier-access-to-radioactive-waste

Mar 13 – At the Hanford Site, waste retrieval has been completed in 17 of 149 large concrete underground single-shell tanks. The tanks were constructed of carbon steel and reinforced concrete between 1943 and 1964 to store a radioactive mix of sludge and saltcake waste from past nuclear processing activities.

Management and disposition of this waste is the responsibility of DOE’s Office of River Protection, assisted by Washington River Protection Solutions(WRPS), operations contractor for the Hanford “tank farms.”

Because of the potential to reduce the overall time and cost required to retrieve the waste and prepare the tanks for closure, WRPS is considering options for installing new access holes in the tank domes for future retrieval efforts.

Working with Becht Engineering Co., Inc., in Richland, Wash., PNNL completed a structural analysis of a concrete single-shell tank (SST) dome with new access holes for deploying waste retrieval equipment.

Their analysis is contained in the paper “Finite Element Structural Analysis Evaluating New Retrieval Strategies in the Hanford Waste Tanks.” It confirms the continued structural integrity of the SSTs with new dome penetrations and retrieval equipment loads on the soil above the tank dome. Specifically, the analysis concluded:

- It may be less expensive to bore new penetrations and install new risers in the tank domes than to remove existing contaminated hardware in existing risers.
- The new large access holes could be up to 6 feet in diameter.

Lead author Kenneth Johnson, a mechanical engineer in PNNL’s Experimental & Computational Engineering group, presented the analysis at the Waste Management Symposia 2019.

Modeling loads, making holes

PNNL says that the paper describes the team's analysis procedure, as well as important considerations for installing new risers. Using detailed finite element computer models, they analyzed the tank response to static thermal and operating loads, as well as dynamic seismic loads.

- *Thermal and operating loads*. This model evaluates the degraded condition of the reinforced concrete tanks by including temperature dependent concrete stiffness, strength, and cracking. The model also includes elastic rebar, pressure dependent soil yielding, and contact between the soil and the concrete tank.
- *Seismic loads:*The seismic model includes contact interfaces between the tank and the surrounding soil, between the tank waste and the inner surface of the tank wall, and within the soil above the tank dome.

They evaluated the results from these models to analyze global concrete section demands versus section capacities, as well as rebar and concrete stresses near the new riser hole. All loading scenarios were found to be acceptably low compared to the load capacities of the tank dome.

"Removing long-length equipment from Hanford's SSTs is one of the most difficult and time-consuming activities associated with tank waste retrieval," said Keith Carpenter, WRPS engineer. "The analytical work completed by PNNL is another great step forward in our pursuit of installing new risers in the SSTs and minimizing the amount of long-length equipment that must be removed."

While the paper presents a single example of the analyses considered, a variety of loading conditions were evaluated as well as additional configurations with four dome penetrations. The study team includes Ken Johnson, Naveen Karri, and John Deibler, Pacific Northwest National Laboratory; and F. George Abatt, Ken Stoops, Larry Julyk, and Brian Larsen, Becht Engineering Co., Inc.

This work builds on a comprehensive structural Analysis of Record (AOR) completed by PNNL in 2015 of the four SST designs at the Hanford Site. PNNL maintains computer models for both single-shell and double-shell tanks to assist WRPS in evaluating changes to the tank structures or operating loads.

Georgia detains two for trying to sell radioactive uranium

Source: https://civil.ge/archives/279222

Mar 13 – Two Georgian citizens were arrested for attempting to sell radioactive Uranium 238, the State Security Service, Georgia's domestic counter-intelligence agency, reported on March 13.

The Security Service said the two men were detained in the Black Sea coast town of Kobuleti in the Autonomous Republic of Adjara.

Russia
R.
Sokhumi
Abkhazskaya
(Autonomous)
Ipkhi
Tkvarcheli
Dzhvari
Ts'ageri
Oni
Zugdidi
Black
Senaki
Tkibuli
Rioni R.
South Ossetia
Kutaisi
Chiatura
Pasanauri
Poti
Samtredia
Zestafoni
Tskhinvali
Kura R.
Makharadze
Khashuri
Gori
Akhmeta
Kobuleti
Telavi
Georgia
Sartichala
Sea
Batumi
Adzharskaya
(Autonomous)
Akhaltsikhe
Tsalka
Tbilisi
Tsnori
Alazani R.
Rustavi
Akhalkalaki
Kazreti
Tsiteli-Tskaro
Kura R.
Armenia
Mingechaurskoye Vodokhranilishche

"These individuals were planning **to sell 40.19 grams of radioactive material for USD 2.8 million,**" the agency also noted, but specified neither the customer, nor the source of the uranium.

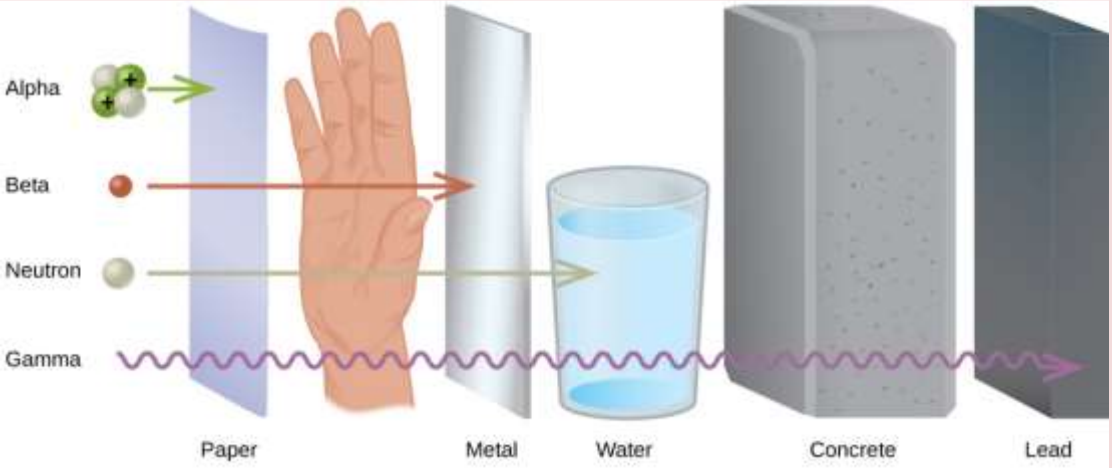
The State Security Service added that it is leading the investigation under article 230 of the Criminal Code, involving illegal handling and sale of radioactive materials. The suspects may face imprisonment from 5 to 10 years.

RADIOLOGICAL TERRORISM – Mental And Physiological Health Effects

By Professor Natividad Carpintero-Santamaría

Source: http://nct-magazine.com/nct-magazine-march-2019/radiological-terrorism/

Radiological terrorism is a challenge that transcends national borders and one of the most disruptive asymmetric threats to security in the 21st century. One of the most important concerns relies on the potential use by a terrorist group, either acting independently or acting as part of a bigger organization that could detonate a Radiological Dispersion Device (RDD) or dirty bomb. The main purpose of a dirty bomb is to cause social chaos as well as panic and traumatic and post-traumatic psychological-psychogenic effects in the population. The physiological and psychological damage caused by the explosion of an RDD would most likely be greater than the effects produced by the radioactive contamination.



Radiological dispersion devices (RDDs) or dirty bombs

Dirty bombs are easily made, with a combination of chemical explosives (such as gunpowder, dynamite, semtex, or C-4) and the kind of radioactive material (ampoule, vial or depot) that is commonly found in hospitals, industries, food sterilization facilities or biochemical research centers. Both the efficiency of the dirty bomb and its radioactive contamination level depend on the chemical explosive used and the radiological toxicity of the material. The greater the amount of chemical explosives, the more effective the scattering of the radioactive material will be.

Although no attacks with radioactive agents have occurred, the relative accessibility of some of these materials presents a continuing threat of radioactive terrorism and governments must develop strategic programs to detect and prevent it, and ultimately, to respond effectively.

▶▶ **You can read the rest of this article at source's URL.**

__Professor Natividad Carpintero-Santamaría__ is Full Professor at the Polytechnic University of Madrid, General Secretary of the Institute of Nuclear Fusion and Member of the Presidium of the European Academy of Sciences. She holds a Diploma in High Studies of Defence and a Diploma as University Expert in Transnational Organized Crime and Security. She is a collaborator in CBRN threats research at the Spanish Centre for National Defence Studies and other institutions. She has been member of the Consulting Board of the International Working Group of the G8 Global Partnership. She has *published several papers on asymmetric threats, WMD terrorism, illicit trafficking of radioactive materials and energy security. She authored the book "The Atom Bomb: The Human Factor during Second World War" (Díaz de Santos, 2007) and co-edited the book Inertial Confinement Nuclear Fusion: A Historical Approach by Its Pioneers (Foxwell and Davies, 2007) considered as recommended reading by the EUROfusion Corsortium of the European Commission. She has been granted the Cross of Aeronautical Merit (white distinctive) and the Cross of Military Merit (white distinctive).*

Italy probes mystery death of Berlusconi sex trial witness

Source: https://www.france24.com/en/20190316-italy-probes-mystery-death-berlusconi-sex-trial-witness

Mar 16 – Italy is investigating the mysterious death of a former model and witness at Silvio Berlusconi's sex trial, with a newspaper suggesting on Saturday she may have been poisoned with a radioactive substance.

Milan prosecutor Francesco Greco said an investigation had been opened following the death on March 1 of Moroccan-born Imane Fadil at one of the city's hospitals.

The 33-year-old had been brought to the hospital on January 29 with unexplained stomach pains.

Fadil was one of the witnesses who testified at the trial of the former Italian premier and media mogul on charges of having sex with an underage prostitute at one of his notoriously hedonistic bunga-bunga parties.

According to Italy's Corriere della Sera daily, the hospital had run a battery of tests to determine the cause of her failing health, but finding nothing, had sent off samples to a specialised laboratory in the northern town of Pavia.

The results came back on March 6, five days after her death, suggesting the presence of "a mixture of radioactive substances which are not normally available for purchase", the paper said, citing unnamed sources.

Fadil's lawyer, Paolo Sevesi, said she had spoken to him about "her fear of having been poisoned," the AGI news agency reported.

The former model first hit the headlines in 2012 when she gave detailed testimony about the goings on at Berlusconi's orgiastic parties at his villa in Arcore near Milan.

She testified that the first time she went to a party, she saw two young women in nun costumes stripping in front of the then prime minister. Later, she said he himself handed her 2,000 euros ($2,600) in cash, telling her: "Don't be offended."

Berlusconi has faced a string of charges over the so-called Rubygate scandal linked to his parties and the underaged prostitute Karima El-Mahroug, also known as "Ruby the heart-stealer".

Now 82, the billionaire businessman is currently on trial for paying a witness to give false testimony about his parties.

Berlusconi is already being investigated or prosecuted for witness tampering in Milan, Sienna, Rome and Turin, each time for allegedly paying people to keep quiet about his bunga-bunga parties.

EDITOR'S COMMENT: It would be interesting to know what methods colleagues in Pavia used along with more details on their finding regarding the "possible" source that caused the death of the unfortunate woman and how this radioactive signature correlates with the origin of the material used. A small Internet search on how to verify exposure to radiation revealed the following info.

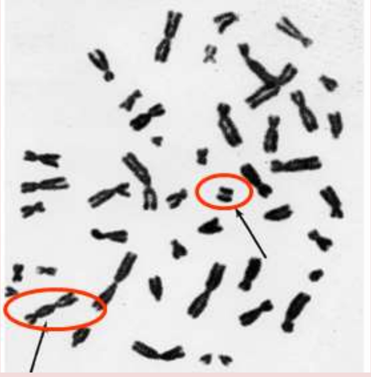
Exposure and vomiting

The time between radiation exposure and the onset of vomiting is a fairly accurate screening tool to estimate absorbed radiation dose. The shorter the time before the onset of this sign, the higher the dose. The severity and timing of other signs and symptoms also may help medical personnel determine the absorbed dose.

Drop in white blood cells count and DNA changes in blood cells

Drops in disease-fighting white blood cells and abnormal changes in the DNA of blood cells indicate the degree of bone marrow damage, which is determined by the level of an absorbed dose.

Dicentric Assay[1]



Chromosomal dicentrics and ring forms are formed during cell division in cells affected by radiation. These can be identified during metaphase. The frequency of formation corresponds to the absorbed dose of radiation. This assay is the most specific and sensitive method for determining absorbed doses from recent (from within days up to six months) exposures to ionising radiation. Dicentric and ring chromosomes are identified from slide preparations of activated lymphocytes arrested in metaphase. From 500 to 1000 cells may require scoring, requiring 2 – 3 person-days at the microscope. At least 100 dicentrics should be identified. The dose is estimated from calibration curves developed by irradiating in vitro samples of blood. The range of absorbed dose detectable using this technique is 0.2 to 5.0 Gy.

MicroRNAs[2]

The test, described in March in *Science Translational Medicine*, detects levels of molecules called microRNAs (miRNAs) in blood and other bodily fluids. Their study identifies seven miRNAs that fluctuate in both mice and macaques exposed to radiation. The monkeys were given lethal doses of 5.8, 6.5 or 7.2 grays of whole-body radiation, similar to levels inhaled by Fukushima workers (all the animals received "lethal" doses, but only some resulted in death). Together three of these miRNAs—miR-133b, miR-215 and miR-375—can indicate with 100 percent accuracy whether a macaque has encountered radiation, and two—miR-30a and miR-126—can predict whether the exposure will be fatal. The signature appears within 24 hours of exposure and can be measured using polymerase chain reaction (PCR), a common technique.

Chromosome 1 (Smc1) protein[1]

The structural maintenance of chromosome 1 (Smc1) protein is a member of the highly conserved cohesin complex and is involved in sister chromatid cohesion. In response to ionizing radiation, Smc1 is phosphorylated at two sites, Ser-957 and Ser-966, and these phosphorylation events are dependent on the ATM protein kinase. In this study, we describe the generation of two novel ELISAs for quantifying phospho-Smc1$^{\text{Ser-957}}$ and phospho-Smc1$^{\text{Ser-966}}$. Using these novel assays, we quantify the kinetic and biodosimetric responses of human cells of hematological origin, including immortalized cells, as well as both quiescent and cycling primary human PBMC. Additionally, we demonstrate a robust *in vivo* response for phospho-Smc1$^{\text{Ser-957}}$ and phospho-Smc1$^{\text{Ser-966}}$ in lymphocytes of human patients after therapeutic exposure to ionizing radiation, including total-body irradiation, partial-body irradiation, and internal exposure to ^{131}I. These assays are useful for quantifying the DNA damage response in experimental

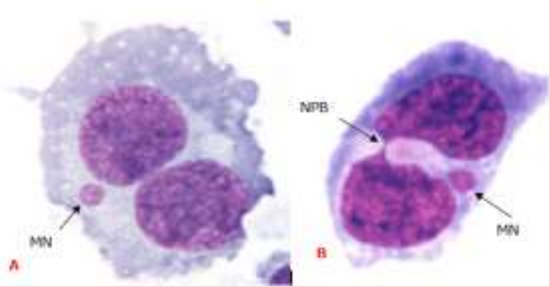
[1] http://www.health.gov.au/internet/publications/publishing.nsf/Content/ohp-radiological-toc~ohp-radiological-14-rad-dose

[2] "Radiation Triage" in Scientific American 316, 6, 19 (June 2017)
https://www.scientificamerican.com/article/detecting-radiation-exposure-with-a-blood-test/
Read also: https://www.dana-farber.org/newsroom/news-releases/2015/new-blood-test-quickly-reveals-severity-of-radiation-injury/

systems and potentially for the identification of individuals exposed to radiation after a radiological incident.[3]

Cytokinesis block micronucleus (CBMN) assay[1]

Micronuclei are formed when acentric chromosomal fragments caused by exposure to ionising radiation do not integrate into the nuclei of daughter cells during ex vivo division in cultured lymphocytes from peripheral blood. In this assay it is also possible to measure nucleoplasmic bridges that are formed from dicentric chromosomes induced by ionising radiation. This technique requires less skill and time than dicentric assay, and is suitable for automated imaging of binucleated cells. Dose estimation correlates well to dicentric assay using appropriate calibration curves. The sensitivity of this technique is limited to thresholds of 0.3 Gy, due to the presence of background micronuclei from other environmental causes. This is still sufficiently sensitive to identify persons needing medical intervention from those requiring continued surveillance. This assay is available in Australia at the DNA Damage Diagnostics Laboratory led by Prof. Michael Fenech at CSIRO Human Nutrition in Adelaide using both visual and automated scoring.



Electron paramagnetic resonance (EPR) / Electron spin resonance (ESR)[1]

When radiation causes ionisation of materials, most electrons recombine. However, in relatively non-aqueous materials, some become trapped. In a magnetic field, the trapped electrons can be induced to provide a resonance spectrum. This technique can be applied to relatively dry materials, such as teeth, bones and fingernail clippings. This is a validated technique with application in palaeontology. It has also been used in studies of atomic bomb survivors, Chernobyl victims and investigation of radiological over-exposures. Radiation-induced changes in teeth are extremely stable, enabling measurement at any time after exposure. Naturally exfoliated teeth have been utilised in retrospective studies. Dental biopsies can also be used. However, rapid techniques have been developed for examination of teeth in situ, although this is not widely available. Molar teeth are preferred as they are not subject to UV radiation exposure. Dental disease may also alter the mineralisation of teeth, affecting measurements. The dose range that can be detected using EPR on teeth is 0.1 Gy to several thousand Gy. Bone has been used in retrospective analysis of amputated limbs in circumstances of localised radiation injury. Fingernail clippings are readily available, although children's nails may have insufficient volume for this technique. Fingernail clippings need to be collected within 30 days. The measurement obtained is the dose received by those specific tissues (teeth, bone or fingernails). If the exposure to the individual was not homogeneous, or occurred from internal contamination, this may not reflect the total dose received. EPR on dental biopsies may be used to verify dose when considering heroic treatment measures for life-threatening exposures.

Comparison of laboratory techniques for biodosimetry[1]

Technique	Dose range detectable (Gy)	Measurement period	Specimen	Purpose	Available in Australia	Turnaround time	Sample capacity per week
Dicentric assay	0.2 to 5.0	1st six months after exposure	Whole blood	Definitive test	From mid-2010	2 weeks	50 - 200

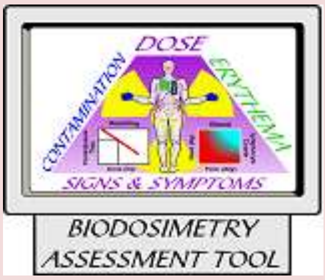
[3] Richard G. Ivey, Heather D. Moore, Uliana J. Voytovich et al. Blood-Based Detection of Radiation Exposure in Humans Based on Novel Phospho-Smc1 ELISA. Radiat Res. 2011 Mar; 175(3): 266–281.

CBMN assay	0.3 to 5.0	1st six months after exposure	Whole blood	Triage cytogenetics, definitive test	Yes	2 – 3 days	80* 300#
FISH		Decades	Whole blood	Retrospective cytogenetics	Research or special interest only		
PCC		1st six months after exposure	Whole blood	Confirmation of doses > 5.0 Gy			
EPR / ESR	0.1 to 1000s	Teeth indefinite; Fingernails < 30 days (or clipped and stored at low temperature)	Teeth, fingernail clippings	Confirmation of doses > 5.0 Gy	Yes, in vitro only	In situ dental readings < 5 minutes	
Luminescence	0.1 to 1000		Building materials, etc	Event reconstruction	Forensic protocols in development		

** Visual scoring. # Automated scoring.*

Biodosimetry Assessment Tool (BAT)

The U.S. Armed Forces Radiobiology Research Institute (AFRRI) has developed a software tool to assist in the dynamic recording of clinical and other data, interpret key parameters for estimation of dose, and summarise diagnostic and therapeutic information. The tool is structured around sets of information pertaining to physical dosimetry, anatomical distribution of contamination, wound type, skin changes, prodromal symptoms, haematological indicators, and signs of manifest illness. The dose estimation is based on the available patient data compared with documented radiation dose responses, and revised as additional information is entered. The software application can be accessed at Armed Forces Radiobiology Research Institute. The software is also available on cd-rom. A series of templates can be downloaded to assist in documenting relevant information.



The urine proteome as a radiation biodosimeter[4]

The global rise in terrorism has increased the risk of radiological events aimed at creating chaos and destabilization, although they may cause relatively limited number of immediate casualties. We have proposed that a self-administered test would be valuable for initial triage following terrorist use of nuclear/radiological devices. The urine proteome may be a useful source of the biomarkers required for developing such a test. We have developed and extensively used a rat model to study the acute and late effect of total body (TBI) and partial body irradiation on critical organ systems. This model has proven valuable for correlating the structural and functional effects of radiation with molecular changes. Results show that nephron segments differ with regard to their sensitivity and response to ionizing radiation. The urine proteome was analyzed using LC-MS/MS at 24 h after TBI or local kidney irradiation using a 10 Gy single dose of X rays. LC-MS/MS data were analyzed and grouped under Gene Ontology categories Cellular Localization, Molecular Function and Biological Process. We observed a decrease in urine protein/creatinine ratio that corroborated with decreased spectral counts for urinary albumin and other major serum proteins. Interestingly, TBI caused greater decline in urinary albumin than local kidney irradiation. Analysis of acute-phase response proteins and markers of acute kidney injury showed increased urinary levels of cystatin superfamily proteins and alpha-1-acid glycoprotein. Among proteases and protease inhibitors, levels of Kallikrein 1-related peptidase b24, precursor and products of chymotrypsin-like activity, were noticeably increased. Among the amino acids that are susceptible to

[4] Sharma M, Moulder JE. The urine proteome as a radiation biodosimeter. Adv Exp Med Biol. 2013;990:87-100. doi: 10.1007/978-94-007-5896-4_5.

oxidation by free radicals, oxidized histidine levels were increased following irradiation. Our results suggest that proteomic analysis of early changes in urinary proteins will identify biomarkers for developing a self-administered test for radiation biodosimetry.

Bioassays[5]

Urine

We can monitor individuals who work with certain beta emitters with a urine bioassay if there is reason to believe we need to look for internal contamination. A urine sample measured on a liquid scintillation counter can indicate whether the worker has taken some radioactive material internally. Nearly 100 percent of some beta emitters are excreted in the urine; for others it may be just a few percent. The excretion of the radionuclide into the urine is dependent upon the chemical form of the radionuclide, how it is metabolized, and the half-life of the radionuclide. Internal contamination with some gamma emitters can also be measured in this manner; however, the next two paragraphs discuss other techniques more commonly used for gamma emitters.

Thyroid

Thyroid counting is performed for determination of internal radioactive iodine uptake. This is a noninvasive test. Radioactive iodine, when taken into the body, seeks out the thyroid gland and deposits there. A thyroid count generally consists of the placement of a scintillation detector in front of the thyroid gland (the instrument is outside the body at the neck level) for one or more minutes with the resultant count indicating the presence or absence of radioactive iodine.

Whole-Body

Whole-body counting is performed to detect the presence of medium- to high-energy gamma-emitting radionuclides within the body. This is noninvasive. Whole-body counting can also be used to determine the distribution of a gamma emitter throughout the body. A whole-body counter may be a chair, bed, or standing type. In nearly all cases, individuals being counted have a series of detectors near them (usually scintillation detectors) that will detect the gamma photons being emitted from the radionuclide source in their body.

Radiation Metabolomics[6]

Gamma-radiation exposure of humans is a major public health concern as the threat of terrorism and potential hostile use of radiological devices increases worldwide. We report here the effects of sublethal γ-radiation exposure on the mouse urinary metabolome determined using ultra-performance liquid chromatography-coupled time-of-flight mass spectrometry-based metabolomics. Five urinary biomarkers of sublethal radiation exposure that were statistically significantly elevated during the first 24 h after exposure to doses ranging from 1 to 3 Gy were unequivocally identified by tandem mass spectrometry. These are deaminated purine and pyrimidine derivatives, namely, thymidine, 2'-deoxyuridine, 2'-deoxyxanthosine, xanthine and xanthosine. Furthermore, the aminopyrimidine 2'-deoxycytidine appeared to display reduced urinary excretion at 2 and 3 Gy. The elevated biomarkers displayed a time-dependent excretion, peaking in urine at 8–12 h but returning to baseline by 36 h after exposure. It is proposed that 2'-deoxyuridine and 2'-deoxyxanthosine arise as a result of γ irradiation by nitrosative deamination of 2'-deoxycytidine and 2'-deoxyguanosine, respectively, and that this further leads to increased synthesis of thymidine, xanthine and xanthosine. The urinary excretion of deaminated purines and pyrimidines, at the expense of aminopurines and aminopyrimidines, appears to form the core of the urinary radiation metabolomic signature of mice exposed to sublethal doses of ionizing radiation.

[5] https://www.radiationanswers.org/radiation-introduction/detecting-measuring/bioassays.html

[6] John B. Tyburski, Andrew D. Patterson, Kristopher W. Krausz, et al. Radiation Metabolomics. 2. Dose- and Time-Dependent Urinary Excretion of Deaminated Purines and Pyrimidines after Sublethal Gamma-Radiation Exposure in Mice. Radiat Res. 2009 Jul; 172(1): 42–57. doi: 10.1667/RR1703.1

In summary

In instances of suspected radiological exposure, a number of indicators and measures may be used to determine the likely absorbed dose of ionising radiation. Each provides an estimation of dose range with recognised limitations in sensitivity, specificity and accuracy. Collectively the multi-parameter approach is used to create the best statistical evaluation of dose.

Where overexposure is suspected:

- obtain a clinical and a location history
- observe and document all prodromal symptoms and signs, including erythema. Photograph cutaneous injuries
- obtain a full blood examination and differential cell count with absolute lymphocyte count immediately. Repeat every 6 hours for the first 48 hours, and 12 hourly for the subsequent 2 days
- perform measurement and bioassay, if appropriate, for internal contamination
- contact a qualified laboratory for dicentric assay. Seek guidance from the state or territory radiation safety unit with regard to assistance in arranging this.
- consider other opportunistic dosimetry approaches as available
- consider data entry into the Biodosimetry Assessment Tool

Dose assessments contribute, but should not be used alone to dictate life-saving medical treatment decisions. Factors such as dose rate and radiation quality can profoundly influence clinical outcome.

Update of REMM website

Dear REMM User,

We have just released a new update on the REMM website and the Mobile REMM app.

U.S. Department of Health & Human Services

REMM RADIATION EMERGENCY MEDICAL MANAGEMENT

What's new on REMM website, March, 2019

- Key detailed guidance document from HHS for senior leaders managing the medical complexities of a nuclear detonation: A Decision Makers Guide: Medical Planning and Response for a Nuclear Detonation
- Links to 2 documents that supplement the Planning Guidance for Response to a Nuclear Detonation, Second Edition, 2010
- Major update of the REMM template / prototype for hospital orders during a radiation emergency. There is one order set for adults and another for children.
- The radiation detectors page has been completely redone to include much more detailed information. A new table describes and illustrates various types of detectors and their optimal use. The key references section provides new information about radiation detection devices and estimating dose in large radiation incidents when adequate detection resources may be scarce.
- The myeloid cytokines page has significant new information, including mention that Leukine (sargramostim) has been approved by the FDA for use with radiation-induced myelosuppression.
- The 3 key algorithms for clinical management of radiation exposure and contamination, (exposure, contamination, exposure + contamination), have been updated with new content and design.
- REMM has aggregated and updated information about Personal Protective Equipment (PPE)
- New multimedia assets have been added to the multimedia carousel; they help explain radiation and response issues
- The Protection Actions page has several changes, including a table comparing references values for emergency responder radiation safety

- Printable wall poster for the EAST Tool: "Exposure and Symptom Triage" to assess patients with potential radiation exposure during a large mass casualty incident
- New publications about using CBCs to estimate dose from exposure and use this information for triage.
- Link on the RDD page to new excellent monograph, Radiological Dispersal Device (RDD) Response Guidance, Planning for the first 100 Minutes, (DHS, NUSTL, NNSA, FEMA, November 2017)
- Descriptions of a new radiation incident response specialist: Radiological Operations Support Specialist (ROSS)
- Update to the REMM page for Planners including new national documents about strategies, plans, and national assets
- Updates to REMM's Key Documents page
- Updates to REMM's Biodosimetry page
- Updates to REMM's Antiemetics page
- Updates to REMM's Fever and Neutropenia page

What's new on the Mobile REMM app

A new version of the Mobile REMM app, which contains selected pages from online REMM, was released in the App Store and Google Play Store. This new version reflects the content updates published on REMM online.

The REMM Team

Radioactive cylinder found on Lebanon coast: authority

Source: http://www.spacedaily.com/reports/Radioactive_cylinder_found_on_Lebanon_coast_authority_999.html

Feb 2018 – A metal cylinder containing a "radioactive substance" has been found next to a beach on Beirut's outskirts, Lebanese authorities said on Wednesday, ruling out any danger to the public.

The Lebanese Atomic Energy Commission (LAEC) said the cylinder was discovered on Tuesday at Ouzai just south of the capital, adding none of the substance escaped from the object.

"Tests conducted in the field showed the radioactive substance was still isolated in the cylinder and did not cause any radioactive pollution in the area it was found," the LAEC said in a statement.

The cylinder bore the inscription "USA DOT 7A TYPE A RADIOACTIVE MATERIAL".

It was transported by the LAEC and the Lebanese army before being stored according to international safety standards, the organisation said.

"Currently we do not have any information on the origin of this cylinder," said Lebanese Environment Minister Tarek el-Khatib.

"I asked the prosecutor yesterday to open an investigation about this which will be conducted by the military police," he told AFP.

"If this container has come from the sea, we will have to make sure there are no other similar cylinders."

Lebanon has struggled with a waste crisis that saw mountains of garbage pile up on streets in and around the capital in 2015.

The country has more than 150 illegal dump sites where waste is burned, according to Human Rights Watch.

"Lebanon's ongoing waste management crisis poses serious health risks for the country's residents," the New York-based HRW has said.

The waste crisis triggered mass protests, with many taking aim at politicians in a country that has suffered endemic corruption since the end of the 1975-1990 civil war.

EXPLOSIVE NEWS

Profit-Minded Suppliers: Convergence of IED Facilitation and WMD Proliferation Networks for Non-State Actors

By Stephen Hummel, F. John Burpo, and James Bonner

Sentinel February 2019 issue

Full text: https://ctc.usma.edu/app/uploads/2019/02/CTC-SENTINEL-022019.pdf

The elements that comprise a network that facilitates the development of improvised explosive devices (IED) are not dissimilar from the elements that lead to the proliferation of weapons of mass destruction (WMD). IED employment has burgeoned in recent years, with over 16,000 incidents worldwide in a 12-month period, while there have been over 500 WMD incidents by non-state actors in the last 26 years. The possibility of the profit-minded suppliers within vast, transnational IED networks expanding into WMD proliferation is high due to the opportunity for profits at relatively low additional risk. The convergence of these two seemingly separate networks does not mean that an IED facilitation network will suddenly market WMD, rather that non-state actors could employ these networks to gather the knowledge, people, materials, finances, and infrastructure required for WMD development and employment. This potential convergence of IED facilitation networks and WMD proliferation networks should be better understood in order to prevent greater proliferation of WMD.

***Major Stephen Hummel** serves as Deputy, Commander's Initiative Group (CIG) at the 20th CBRNE Command. Previously, he served in both Iraq and Afghanistan and as a USAREUR CBRN Plans Officer, an Assistant Professor in the Department of Chemistry and Life Science at the United States Military Academy, and a Nuclear Operations Officer on a Nuclear Disablement Team. He holds a B.A. in Political Science from Boston College, an M.S. in Free Radical and Radiation Biology from the University of Iowa, and an M.S. in Chemical and Physical Biology from Vanderbilt University.*

***Colonel F. John Burpo** is the Department Head of Chemistry and Life Science at West Point. COL Burpo commissioned as an artillery officer and served in airborne, armor, and Stryker units with humanitarian, peace-keeping, and combat operational deployments. He also served as the Deputy Commander-Transformation for the 20th Chemical, Biological, Radiological, Nuclear, and Explosives Command (CBRNE). He earned a B.S. in aerospace engineering from West Point, an M.S. in Chemical Engineering from Stanford University, and Sc.D. in Bioengineering from the Massachusetts Institute of Technology.*

Brigadier General James Bonner *is the Commanding General of the U.S. Army's 20th CBRNE Command in Aberdeen Proving Ground, MD. Previously, he was the 29th Chief of Chemical and CBRN School Commandant. Other key assignments include Plans and Policy Officer J-5 and as a Counterproliferation Planner J-3, Joint Special Operations Command (JSOC); and Special Assistant for Countering WMD Terrorism, Counterterrorism Division, Federal Bureau of Investigation (FBI). He holds master's degrees from Central Michigan University and the Naval War College.*

500 kilos of chemical used as IED ingredient seized in Zamboanga City

Source: https://mindanaoexaminer.com/500-kilos-of-chemical-used-as-ied-ingredient-seized-in-zamboanga-city/

Feb 24 – Police seized half a ton of ammonium nitrate, widely used by rebels and terrorists in the manufacture of explosives, following a sea chase that led to the capture of 5 men in the southern Philippine port city of Zamboanga.

A maritime police patrol spotted a suspicious boat off Taluksangay village on Saturday and gave chase after the vessel did not stop for security inspection. The boat was eventually apprehended and its passengers arrested after policemen discovered its cargo of **20 bags of ammonium nitrate.**

Each bag is weighing 25 kilos. The ammonium nitrate, made in South Korea by Huchems Fine Chemical Corporation, is a common ingredient in improvised explosives and is banned in the Philippines.

Baguio
Manila
Lucena
Naga
PHILIPPINES
Iloilo
Bacolod
Mandaue
Cebu
Puerto Princesa
Butuan
Zamboanga
Cotabato
Davao

Police were interrogating those arrested Ismol Malsani, Kadoh Kahamkam, Jinali Marosali, Makamil Malan and Mastal Malsani to determine whether if they are members of any rebel group or who was behind the foiled smuggling of the chemical to Zamboanga.

Just this month, a group of communist insurgents surrendered to the military and handed over 40 kilos of ammonium nitrate and 190 blasting caps they used in making homemade bombs in Compostela Valley's Monkayo town, also in the restive region.

Last year, police raided a house in Taluksangay village and seized two one-liter bottles containing ammonium nitrate and weapons from Samandi Imbas and Sagumbahar Akbar. **In August 2017, police here also confiscated 300 kilos of ammonium nitrate and dozens of blasting caps in a raid on a house in the coastal village of Arena Blanco.**

The house owner, Pagal Aliasan, 25, admitted purchasing the chemical from the black market in Tawi-Tawi, one of 5 provinces under the Muslim autonomous region, and sold homemade explosives to fishermen.

Stricter EU rules to prevent home-made bombs

Source: http://www.europarl.europa.eu/news/en/headlines/security/20190222STO28408/terrorism-stricter-eu-rules-to-prevent-home-made-bombs

Mar 01 – The EU has taken several measures to prevent terrorist attacks and is now updating rules regarding chemicals that can be used to create home-made bombs**.**

Home-made bombs

Home-made explosives have been used in the vast majority of terrorist attacks in the EU, including those in Paris in 2015, Brussels in 2016 as well as Manchester and Parsons Green in 2017. The chemicals to produce them, known as explosives precursors, can be found in a number of products, including detergents, fertilizers, special fuels, lubricants and water-treatment chemicals.

The EU is strengthening rules regulating who and how these substances can be purchased as part of the package of measures against terrorism and criminality. However, as these chemicals also have legitimate uses, it is this important to ensure that people such as farmers, miners and firework manufacturers can still use them.

Current rules date from 2013 and restrict sales of substances such as hydrogen peroxide and nitric acid. The rules have helped to decrease the availability of explosive precursors but have several weaknesses.

"Recent terrorist attacks have shown that no EU country can tackle terrorism unilaterally and I see it as a priority to regulate the availability of explosive substances at the Union level," said Latvian S&D member Andrejs Mamikins, who is the MEP responsible for steering the legislation through the Parliament.

What will change?

Currently, licensing and registration systems differ considerably between EU countries. The new regulation will set up common EU rules for the issue of licenses for those with legitimate interests. They will be subjected to a thorough security screening, including a criminal record check.

The new rules should introduce a clear definition of the "general public", who will not be able to buy these chemicals, and "professional users" who need them for their work.

As terrorists come up with new ways to create explosives, employing ingredients not covered by current rules, the European Commission is proposing to add new chemicals to the list of restricted substances, such as sulphuric acid.

The new rules will apply to both online and offline sales.

"It is particularly important to make sure that online platforms comply with the obligations under this regulation and guarantee that chemical substances that can be used for bomb-making are restricted," said Mamikins.

Next steps

Negotiators from the Parliament and the Council have already reached an agreement on what the final text of the legislation should be. Parliament's civil liberties committee voted in favor of the deal on 19 February. It will now be up to all MEPs vote on it during the plenary session in April.

EDITOR'S COMMENT: Recently the Greek gov is attempting to modify existing legislation related to possessing and using Molotov cocktails and explosives, from a felony to misdemeanor that will be punished with max 3 years in jail (instead of 20 yrs). And no penalty at all if bombs and related materials are delivered to authorities before the arrest! No, these are not fake news like the man who was hired in London to shoot down drones.

Jihadis turn a DONKEY into suicide bomber by strapping IED to it then detonating at checkpoint in Yemen

Source: https://www.thesun.co.uk/news/8619698/jihadis-suicide-bomber-donkey-yemen/

Mar 12 – Sick photos of the donkey bomb were published in recent extremist propaganda for Ansar al-Sharia, an al-Qaeda linked terror group operating in Yemen

The photos were published in recent extremist propaganda for Ansar al-Sharia, an al-Qaeda linked terror group operating in Yemen.

The unwitting suicide bomber was reportedly used to strike at a checkpoint manned by Houthi militants, though it's not known if anyone was killed.

Yemen is currently locked in a bitter civil war, with the Iran-backed Houthi fighters trying to topple the Saudi Arabia-backed government.

The photos were posted online by Martin Zabel, a lecturer on radicalisation and Islamic Studies. He stated they were published by the terror group's publication for last month, titled "Dust Battles".

They show shells being strapped onto the back of the poor donkey while its held still by masked fighters.

It is then seen being led down a road with straw tied to its back to hide the explosives.

Two additional distant photos then show what the jihadis claim is the donkey before and after it is detonated.

Mr Zabel said: "It features a despicable 'Donkey-Born-IED' targeting a #Houthi checkpoint.
"Haven't seen animals being misued for #IEDs in a while. #Iraq #insurgency comes to my mind first."
This incident is not the first-time donkeys are reported to have been used to carry IEDs.
In 2013, three US soldiers and an interpreter were reported to have been killed by a suicide bomber riding a donkey in Afghanistan.
In that instance, the attack was claimed by the Taliban.

Seddon..
BOMB DISPOSAL SQUAD
CARTOONSTOCK .com
Search ID: msen546
"...And then if the numbers in the column don't add up correctly, I have to start all over again! It really is quite a stressful job."

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C2BRNE DIARY

CYBER NEWS

A new world for hackers: Acoustic side-channel attack

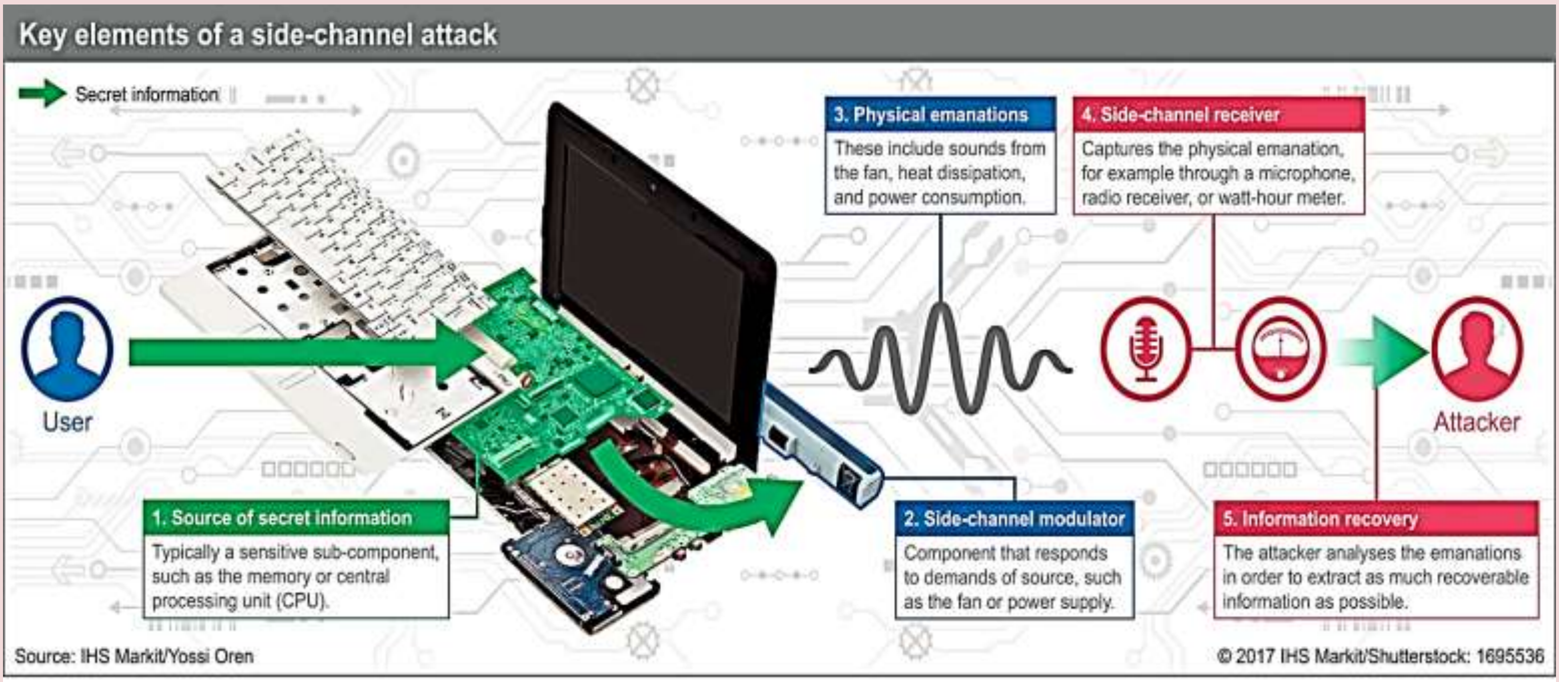
Source: http://www.homelandsecuritynewswire.com/dr20190311-a-new-world-for-hackers-acoustic-sidechannel-attack

Mar 11 – Researchers from the University of California, Irvine and the University of California, Riverside have uncovered the possibility of an acoustic side-channel attack on the DNA synthesis process, a vulnerability that could present a serious risk to biotechnology and pharmaceutical companies and academic research institutions.

“A few years ago, we published a study on a similar method for stealing blueprints of objects being fabricated in 3-D printers, but this attack on DNA synthesizers is potentially much more serious,” said Mohammad Al Faruque, UC Irvine associate professor of electrical engineering and computer science. “In the wrong hands, DNA synthesis capability could result in bioterrorists synthesizing, at will, harmful pathogens such as anthrax.”

Al Faruque said his lab’s discovery might also be used for a good cause: “Government agencies can employ the same technique as a monitoring tool to nullify the possibility of such activities.”

Key elements of a side-channel attack



1. Source of secret information
Typically a sensitive sub-component, such as the memory or central processing unit (CPU).

2. Side-channel modulator
Component that responds to demands of source, such as the fan or power supply.

3. Physical emanations
These include sounds from the fan, heat dissipation, and power consumption.

4. Side-channel receiver
Captures the physical emanation, for example through a microphone, radio receiver, or watt-hour meter.

5. Information recovery
The attacker analyses the emanations in order to extract as much recoverable information as possible.

Source: IHS Markit/Yossi Oren

© 2017 IHS Markit/Shutterstock: 1695536

Listening in

A DNA synthesizer is a complex machine with meandering pipes, fluid reservoirs, solenoid valves and electrical circuitry. Chemicals — which have their own unique acoustic signatures due to their varying densities — flow through tubes, creating distinct noises punctuated by the clicking of valves and the whirring of pressure pump motors.

“All of these inner workings of a DNA synthesizer result in the emission of subtle but distinguishable sound signatures that can give clues as to the specific genetic material being generated,” said Sina Faezi, a UC Irvine graduate student in electrical engineering and computer science, who will present a paper on the potential threat of an acoustic side attack on DNA synthesizers at the Network & Distributed System Security Symposium taking place Feb. 24-27 in San Diego.

He said that in many cases, variances in the sounds produced are so tiny that people can’t distinguish them. “But through careful feature engineering and a bespoke machine learning algorithm written in [Al Faruque’s] lab, we were able to pinpoint those differences,” he said.

Another factor that enables DNA synthesis information to be stolen is the design of the synthesizers themselves, according to Faezi. “Solenoid valves are placed asymmetrically inside the housing, so when a valve is working in one corner of the box, it makes a completely difference noise than one that’s working in the middle,” he said.

If hackers know which device model is in use, they'll have one more piece of the puzzle in place.
"Any active machine emits a trace of some form: physical residue, electromagnetic radiation, acoustic noise, etc.," said study collaborator Philip Brisk, UC Riverside associate professor of computer science & engineering. "The amount of information in these traces is immense, and we have only hit the tip of the iceberg in terms of what we can learn and reverse-engineer from it."

How your smartphone could be used for illicit listening

Al Faruque, head of UC Irvine's Advanced Integrated Cyber-Physical Systems Lab, added that the ubiquity of recording devices, such as smartphones, makes the problem even more pervasive.

"Let's say you're a good person who works in a lab. I can hack into your phone and essentially hijack it to record sound that I can eventually retrieve," he said. "Furthermore, some biological labs have acoustic sensors mounted on the walls, and more people are adopting technologies like Google Home or Alexa — all of these can be used to pilfer sounds."

With their side-channel attack methodology, the researchers said, they can predict each base in a DNA sequence with about 88 percent accuracy, and they're able to reconstruct short sequences with complete reliability. Their technique functions best when a recording device is placed within a couple feet of a DNA sequencing machine, they said, but the algorithm works even in the presence of noise from an air conditioner or peoples' voices.

Al Faruque stressed that this sort of attack is too sophisticated for a small-time criminal or terrorist to pull off but is not beyond the capability of state actors. The stakes are high: The global market for synthetic biological products is expected to reach almost $40 billion by 2020. And that market share is expected to grow, particularly in the area of DNA data storage, an application being pursued by heavy-hitting technology companies.

Faezi noted that there are some ways to prevent snooping attacks. Machine designers could arrange the pipes and valves in a way that mitigates the emission of distinct sounds, and the DNA synthesis process can be scrambled and randomized to block hackers from piecing together the intellectual property.

Iranian hackers stole terabytes of data from software giant Citrix

Source: https://www.engadget.com/2019/03/09/iranian-hackers-target-citrix/

Mar 11 – Citrix is best-known for software that runs behind the scenes, but a massive data breach is putting the company front and center. The FBI has warned Citrix that it believes reports of foreign hackers compromising the company's internal network, swiping business documents in an apparent "password spraying" attack where the intruders guessed weak passwords and then used that early foothold to launch more extensive attacks. While Citrix didn't shed more light on the incident, researchers at Resecurity provided more detail of what likely happened in a conversation with *NBC News*.

Resecurity understood that hackers from Iridium, an Iran-linked group, stole data in December 2018 and again on March 4th. They made off with at least 6TB of documents and as much as 10TB, and they seemed to be focused on project data for the aerospace industry, the FBI, NASA and Saudi Arabia's state-owned oil company. The intruders may have been lurking for a long time, too. Resecurity's Charles Yoo said that Iridium broke into Citrix's network roughly 10 years ago and had been hiding since then.

The researchers said they'd told Citrix about the first attack on December 28th. It's not clear if Citrix addressed the issue then, although it took a number of steps after the FBI got in touch on March 6th. The company said it launched a "forensic investigation" with the help of an unnamed security firm and took "actions" to lock down its network.

Citrix stressed there was "no indication" that the intruders compromised its products or services. However, that's not the major concern here. As a government contractor that focuses on networking and the cloud, Citrix could hold sensitive data on other companies. It may be aware of their network layouts and security measures, for instance. Like the OPM hack, the consequences could reach well beyond the initial target.

Triton is the world's most murderous malware, and it's spreading

Source: https://www.technologyreview.com/s/613054/cybersecurity-critical-infrastructure-triton-malware/

Mar 11 – In the summer of 2017, a petrochemical plant in Saudi Arabia experienced a worrisome security incident that cybersecurity experts consider to be the first-ever cyberattack carried out with "a blatant, flat-out intent to hurt people." The attack involved a highly sophisticated new malware strain called Triton, which was capable of remotely disabling safety systems inside the plant with potentially catastrophic consequences.

Luckily, a flaw in the Triton code triggered a safety system that responded by shutting down the plant. If it hadn't been for that flaw, the hackers could have released toxic hydrogen sulfide gas or caused explosions. As a result, employees of the plant and residents of the surrounding area could have been killed or injured.

Triton is almost certainly the work of state-backed hackers. While Iran was the initial suspect, later reports indicate that Russia may have been behind the attack.

Since Triton was first discovered, cybersecurity firms have uncovered more attacks involving malware with similar traits, designed to take over safety systems. Triton has not been spotted in other potentially destructive attacks, but cybersecurity experts believe it is only a matter of time before the murderous malware will rear its ugly head again.

Cyberwarfare: Competing National Perspectives the Threat of Cyberwarfare Is A Growing Fear Among All Intelligence Communities

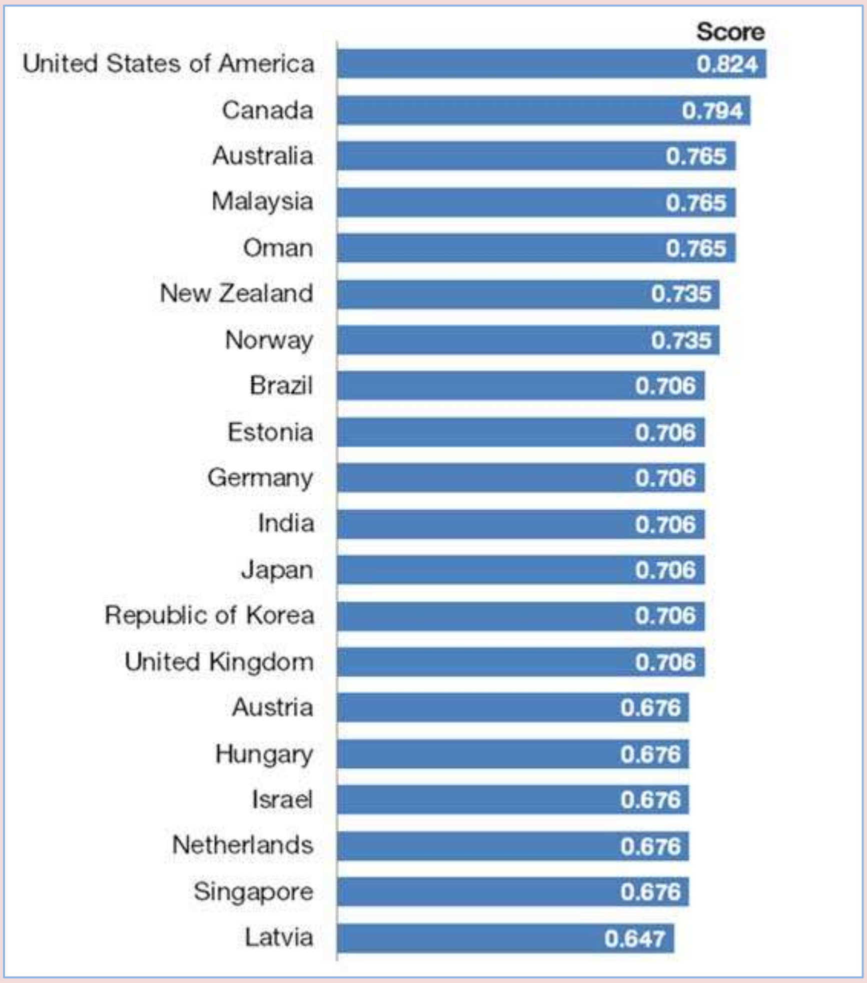
Source: https://moderndiploma cy.eu/2019/03/11/cyber-warfare-competing-national-perspectives/

Mar 11 – "In June 2009 the U.S. Cyber Command was created and in July of 2011 Deputy Secretary of Defense William J. Lynn III announced that as a matter of doctrine, cyberspace will be treated as an operational domain similar to land, air, sea, and space" (Colarik & Janczewski, 2012, 35). Cyber warfare is conducted by infiltrating the country's computer networks to cause damage and/or disruption to various infrastructures. This could be as minimal as spying on another nation or as in-depth as implementing acts of sabotage directed towards specific targets such as military operations or the power grid. The threat of cyber warfare is not specific to one country. This is a potential threat that effects each country across the globe. China is a dominant power within the global arena and is consistently evolving with potential threats especially cyber technology. Chinese colonels Liang and Xiangsui claimed advanced technol-ogy gave the country's adversaries a significant advantage, and proposed that China 'build the weapons to fit the fight. Recently, the Chinese People's Liberation Army (PLA) confirmed the exist-ence of its Online Blue Army (Colarik,& Janczewski, 2012, 35). China's fear of the impact and devas-tation that can be caused by the internet has forced them to implement strict policies governing the freedom and use of the internet within the country and creating strong security measures against infiltration by outside sources. In 2014, China implemented the Central Internet Security and Informatization Leading Group to oversee all internet security. "This leading group is to deepen reform, protect national security, safeguard national interests, and promote the development of information technology. The group will have complete authority over online activities, including economic, political, cultural, social, and military" (Iasiello, 2017, 5). This group disseminates and monitors all information found on the web to ensure that there are no security breaches and the people are not in violation of the law.

In 2015, China drafted a national cybersecurity law. "The chief goals of its 2015 draft national cybersecurity law are (1) ensure cybersecurity, (2) safeguard cyberspace sovereignty, national security, and the public interest, (3) protect the legitimate rights and interests of citizens, legal persons and other organizations, and (4) promote the healthy development of economic and social information" (Kolton, 2017, 126). Whereas the United States promotes a free internet, China's main focus is on establishing an internet that is secure from all potential threats both external and internal. In 2016, China passed the “Cyber Security Law” that focused on the security of the internet and information systems and extended the ability of the government to oversee the information that was being shared to determine if it was done within accordance of their strict cyber security laws. This law helps the government to monitor any potential breaches of security by outside or internal sources. By implementing a stronger grasp of control over the internet, the government is able to reduce the potential of an attack or intrusion. Within this law, government agencies would be able to implement more guidelines for network security within industries to include energy, transport, military, defense, and many more (Iasiello, 2017, 6). These restrictions increase the control of the government over cybersecurity but also limits the freedoms of its citizens to explore the internet. China has created new training for its military to be prepared against potential cyberwarfare attacks. It has “developed detailed procedures for internet warfare, including software for network scanning, obtaining passwords and breaking codes, and stealing data; information-paralyzing software, information-blocking software, information-deception software, and other malware; and software for effecting counter-measures” (Ball, 2011, 84). It has also increased its number of train-ing facilities to focus only on network attacks on cyber infrastructure and defense operations.

The amount of money China is investing in facilities and training of military personal increases its ability to remain secure within this global threat of cyber warfare. One fear for China is its dependence on Western technology. “China’s capabilities in cyber operations and emerging technologies such as artificial intelligence are becoming more sophisticated, the country still depends largely on Western technology. Beijing is hoping to break that dependency through the Made in China 2025 plan” (Bey, 2018, 33). This is a mutual fear for both the US and China as they both rely on each other’s manu-facturers with the fear that they will implement a trojan horse to intervene. Like China, Russia has increased its abilities in combating the potential threat of cyber warfare. However, Russia has taken a different approach to this threat by going on the offensive. Russia has focused on non-linear warfare within the cyber world, which is defined as “the collection of plans and policies that comprise the state’s deliberate effort to harness political, military, diplomatic, and economic tools together to advance that state’s national interest. Grand strategy is the art of reconciling ends and means” (Schnauffer, 2017, 22).

To assert its dominance in the global arena, Russia has been utilizing its own forms of cyber attacks to collect information and become a domi-nant cyber power. Russia began its experiments with cyber warfare in 2007 in the clash with Estonia. This was done to determine its cyber capabilities as well as create a stronger resilience against future attacks. “Russia’s cyber experiment effectively shut down day-to-day online operations in Estonia’s cyber infrastructure for weeks, from news outlets to government institutions” (Shuya, 2018, 4). After this successful movement, Russia began to expand its focus to Georgia and Ukraine in 2008 and then in 2015, to offset local initiatives there which it considered to be against Russian national security interests. Russia has “developed multiple capabilities for information warfare, such as computer network operations, electronic warfare, psychological operations, deception activities, and the weaponization of social media, to enhance its influence campaigns” (Ajir& Valliant, 2018, 75). Russia has had a strong focus on using the tool of propaganda to disseminate key information to its citizens with the hope that they will abide by it as the real truth. Russia’s investment into technology and the freedom of speech allotted by the West has made the West not only extremely vulnerable to Russia, but also has expanded the reach of the Russia globally. Ajir and Valliant (2018) highlight several key points of the Russian strategy: Direct lies for the purpose of disinformation both of the domestic population and foreign socie-ties; Concealing critically important information; Burying valuable information in a mass of infor-mation dross; Simplification, confirmation, and repetition (inculcation); Terminological substitution: use of concepts and terms whose meaning is unclear or has undergone qualitative change, which makes it harder to form a true picture of events, Introducing taboos on specific forms of infor-mation or categories of news; Image recognition: known politicians or celebrities can take part in political actions to order, thus exerting influence on the worldview of their followers; Providing negative information, which is more readily accepted by the audience than positive. This approach allows the Russian government to remain in control of information that is filtered to its citizens. The restriction of freedom reduces the capability of deciphering fact from fiction. Russia has also taken a defensive approach to cyber warfare by implementing strict laws that govern the use of the internet. The agency Roskomnadzor scans the internet for activity that is deemed illegal and detrimental to the Russian government. It has also implemented new laws to regulate internet activity. “The laws which came into force in November 2012 provided provisions for criminalizing slander, requiring nonprofits receiving funding from abroad to declare themselves “foreign agents,” and provide additional financial information and a final law sanctioning the block-ing of websites featuring content that “could threaten children’s lives, health, and develop-ment” (Cross, 2013, 14).



Many have deemed these laws as means to censor the internet, but the Russian government argues it is for the protection of its citizens. An opposite example of failing to employ measures to protect the country from a potential cyber warfare attack is Mexico. The main focus for Mexico has been on drug cartels and eliminating internal threats within their own government. Mexico has begun to implement its own version of cybersecurity due to its substantial growth in cyber-attacks over the years. However, its overall success has been limited due to a lack of understanding and outdated systems. “Incidents in cyberspace pose a challenge to Mexico due to a lack of institutional structures and there is a need to strengthen capabilities since it does not have any specialized government or public sector agencies certified under internationally recognized standard” (Kobek, 2017, 8). Without the establishment of a specific agency dedicated to cybersecurity, Mexico will continue to struggle against cyber warfare threats. Mexico must implement new security measures that are applicable to all main threats beyond the drug cartels. Currently, the government presence in Mexico is focused solely on actionable and tangible threats. There must be a reform to its current laws for “the armed forces require a law that re-frames and modernizes the concepts of public safety, internal security, and national defense; clarifies the role, conditions, terms, and limits of the armed forces’ engagement; and establishes mechanisms to hold them accountable” (Payan & Correa-Cabrera, 2016, 3). The lack of accountabil-ity and oversight by the government to control key aspects, such as the military, and impose a stronger presence in the more demanding field of cybersecurity opens up the potential for a catastrophic event to occur within Mexico.

China and Russia are prime examples of how strict policy governance of the internet will help to reduce the potential threat of an attack. They are micromanaging every aspect of the internet from restricting specific websites (social media) or establishing specific agencies to monitor and analyze all information that is being viewed from all sources. “With the United States and European democ-racies at one end and China and Russia at another, states disagree sharply over such issues as whether international laws of war and self-defense should apply to cyber-attacks, the right to block information from citizens, and the roles that private or quasi-private actors should play in Internet governance” (Forsyth, 2013, 94). The failure of this policy is the restriction of freedoms to citizens. As stated above, one of Russia’s main focuses is promoting propaganda that is anti-west and pro-Russia. The control over the internet does not allow their citizens to research the truth or have global interaction. This increases the risk of upheavals among the people, especially as technology continues to improve and loopholes are found to circumvent existing policies and hidden content is exposed. Another approach to cybersecurity is seen with the actions of NATO. It is focusing on improving its relationships with private security companies and “developing a Cyber Rapid Reaction Team (RRT)19 to protect its critical infrastructure, much like U.S. Cyber Command’s Cyber Protection Teams (CPTs)” (Ilves et al, 2016, 130).

One downside to this approach is NATO is only able to apply defensive measures. It does not have the ability to implement an offensive attack. Creating a part-nership with private companies provides it greater access and resources to potential cyber threats. Private companies have more funds available to pursue a stronger cyber security defense. A recom-mendation would be to create a joint European Union, United States, and NATO partnership against cyber warfare. Each has its own strengths that can be applied to a joint force against one common threat. A stronger partnership among key global powers will help to create a multifaceted approach to the threat of cyber warfare. The end goal of cyber warfare is the same for each country targeted. There is no specific adversary, but rather the substantial disruption or sabotage of key infrastruc-ture. Although facing intense criticism and skepticism, it would be beneficial for the US, China, and Russia to form a partnership against cyber warfare. As each country is already connected via their technology companies, they are each a global power that encompasses a vast majority of the world. A collaboration of information and resources would provide a stronger protection amongst common non-state threats. However, the chief obstacle is the ability to trust each country to act within the realm of security, instead of using it as an opportunity to gain substantial access to an inside look of the country. Since the US often accuses China and Russia of being the biggest state perpetrators of cyber actions, this criticism may be near impossible to overcome, despite the possible advantages. According to the World Economic Forum, the table (at the top) lists the top countries best prepared against cyber-attacks. The United States is ranked number one with a significant margin above Canada. China and Russia who h ave implemented a very strict cyber security policy are not listed within the top 20. This is determined by the Global Cybersecurity Index, a partnership between private industries and international organizations that analyze all aspects of cybersecurity. This argues that the approach by countries such as China and Russia is geared more to the control over its citizens rather than executing a strong cybersecurity policy focused on legitimate external threats. Although, the table above does show that the United States is ranked number one in being able to protect the nation from potential cyber threats, it is only ranked at 82.4% effective. Russia and China have employed a different approach to cyber security that could be utilized to increase the overall effectiveness globally if each side was able to work together towards common threats. Ideally, such partnership would not only create new channels of connection and collaboration between adversaries, but would also set the stage for the more heavy-handed and restrictive policies of China and Russia to be loosened to the benefit of its citizens’ virtual freedom.

Why tech companies failed to keep the New Zealand shooter’s extremism from going viral

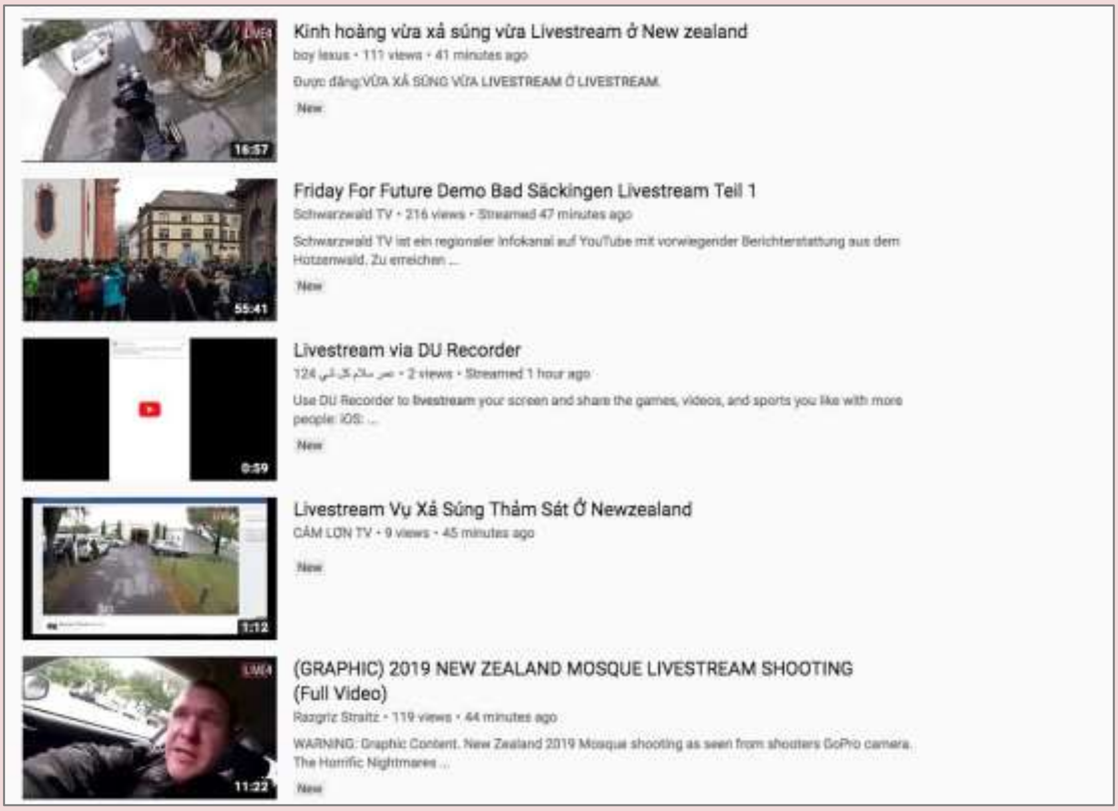
Source: https://www.vox.com/policy-and-politics/2019/3/17/18269617/new-zealand-shooting-mosque-online-extremism-tech

Mar 18 – The hate-filled terror rampage at two mosques in Christchurch, New Zealand, was meticulously designed to maximize the number of witnesses around the globe, highlighting the difficulty in putting a lid on extremist hate that spreads online.

The suspected gunman did everything he could to make his shooting spree go viral. He live-streamed the attack on social media, wearing a body camera to simulate a video game. He shared a rambling 74-page manifesto espousing white supremacy that was full of memes and easter eggs meant to invite attention from all corners of the internet and admiration from other extremists who live online. The shooter had laid a trap across the internet that exploited the newsworthiness of the attack and leaned into peoples’ inclination to gawk at horror and violence. Even professional journalistic institutions gave in to the temptation to air video of the massacre.

Scrubbing the video from the internet was like playing a game of whack-a-mole. Facebook quickly removed the alleged gunman’s Facebook and Instagram accounts — but not because its algorithm or moderators had flagged the violent content in real time. New Zealand authorities had to ask for the video to be taken down. Internet service providers in New Zealand rushed to "close off" websites that were distributing the video, but then a number of copy-cat sites immediately started popping up.

It soon didn't matter that the original video was removed. The clip had already been downloaded and re-upped online faster than tech companies could respond. Facebook alone says it removed 1.5 million videos within the first 24 hours of the attack. And those are just the clips they were able to catch.



Kinh hoàng vừa xả súng vừa Livestream ở New zealand
boy lexus • 111 views • 41 minutes ago
Được đăng:VỪA XẢ SÚNG VỪA LIVESTREAM Ở LIVESTREAM.
New

Friday For Future Demo Bad Säckingen Livestream Teil 1
Schwarzwald TV • 216 views • Streamed 47 minutes ago
Schwarzwald TV ist ein regionaler Infokanal auf YouTube mit vorwiegender Berichterstattung aus dem Hotzenwald. Zu erreichen ...
New

Livestream via DU Recorder
124 صر سلام كل لي • 2 views • Streamed 1 hour ago
Use DU Recorder to livestream your screen and share the games, videos, and sports you like with more people: iOS: ...
New

Livestream Vụ Xả Súng Thảm Sát Ở Newzealand
CẢM LƠN TV • 9 views • 45 minutes ago
New

(GRAPHIC) 2019 NEW ZEALAND MOSQUE LIVESTREAM SHOOTING (Full Video)
Razgriz Straitz • 119 views • 44 minutes ago
WARNING: Graphic Content. New Zealand 2019 Mosque shooting as seen from shooters GoPro camera. The Horrific Nightmares ...
New

Friday's massacre exemplified a larger problem that's plaguing the internet. Platforms are struggling to self-police problematic content created by its users, while the lawmakers who would ostensibly impose regulations are either too reluctant or ill-equipped to do so — and many in both camps are predisposed to treat far-right rhetoric less seriously than other forms of extremism, to boot.

As the death toll rises — now 50 lives have been taken since Friday's shooting, making it one of the deadliest terror attacks carried out by a far-right extremist in recent memory — the attack adds extra weight to the question that tech companies, policymakers, and social media users have been asking: How do you effectively police online hate?

The shooter's viral video outpaced social media company's content moderation

The world's largest tech companies were forced to scramble on Friday to keep the violent screed from spreading. Facebook said it was removing any praise or support of the shooting, and had a process to flag the digital fingerprint of disturbing materials. YouTube said it was "working vigilantly" to remove violent footage, while Twitter said it suspended the account that posted the original video. Reddit on Friday eventually resorted to taking down two infamous subreddits, r/watchpeopledie and r/gory.

Despite those efforts, videos of the attack were easy to find through simple searches online, even hours and days after the initial shooting spree. The swift dissemination highlights how ill-equipped tech companies remain in addressing the vile, racist, and excessively violent content that's being shared on their platforms.

Moderators already face an uphill battle in keeping offensive and violent content offline; the Christchurch terror attack shows the difficulty of catching deeply problematic video live-streams in real time.

For one, it's generally easier for software to scan text and offensive comments as opposed to moving images in a video. But even when the technical tools exist, policing-breaking news poses unique problems. YouTube, for example, does have a system for automatically removing copyrighted content or prohibited materials, and told the Verge's Julia Alexander that any exact re-uploads of the alleged shooter's videos would be automatically deleted. But the algorithm can't be used to tamp down on edited versions of the Christchurch shooting, because Youtube wants to "ensure that news videos that use a portion of the video for their segments aren't removed in the process":

YouTube's safety team thinks of it as a balancing act, according to sources familiar with their thinking. For major news events like yesterday's shooting, YouTube's team uses a system that's similar to its copyright tool, Content ID, but not exactly the same. It searches re-uploaded versions of the original video for similar metadata and imagery. If it's an unedited re-upload, it's removed. If it's edited, the tool flags it to a team of human moderators, both full-time employees at YouTube and contractors, who determine if the video violates the company's policies.

That process is not just traumatizing for the individual moderators who are forced to watch the horrific footage, it's also an imperfect system to limit its reach — particularly in a fast-moving event like Friday's tragedy.

Tech companies are expected to self-police. So far, they're falling short.

At this point, in theory, tech companies should be well-practiced in the art of blocking far-right hate speech and violence from their platforms. They've been having to deal with it for years.

After the 2017 Unite the Right rally of neo-Nazis and white supremacists in Charlottesville, Virginia — where a woman was mowed down and killed by an avowed Nazi sympathizer — tech companies faced intense public pressure to block prominent instigators of explicit far-right extremism. Twitter suspended a bunch of white supremacists and prominent provocateurs — including Milo Yiannoppolis, Alex Jones, and Gavin McInnes — but was hesitant to target other alt-right leaders like Richard Spencer. Gab and the Daily Stormer, two havens for neo-Nazis, were similarly banished to the darker recesses of the internet. Reddit quarantined hate-fueled subreddits, while other companies like PayPal, GoDaddy, and Squarespace blocked white supremacists from using their services.

In effect, individual leaders and groups were targeted in response to a high-profile flashpoint in American politics and culture. But for many critics, those actions were hollow in addressing the underlying proliferation of racist and white supremacist ideas that are peddled online.

And even minimal efforts at reform have come with costs for the social media giants — big ones. As Vox's Emily Stewart noted after Facebook's stock saw the biggest one-day drop in history last fall (with $119 billion wiped off of its value after the company reported slower-than-expected revenue growth), social media companies' efforts to address issues with their platforms garner "enormous backlash from Wall Street."

The message from investors is clear: They're nervous about what bad headlines and subsequent changes from social media platforms could do to their bottom lines. If Twitter and Facebook police their sites in a way that affects engagement or cracks down on content, or if privacy controls that ask users to opt in to their data being shared lead to more of them opting out, ad dollars could fall. And hiring workers to increase privacy protections and monitor activity is expensive.

... This week offers a lesson we don't necessarily want executives to take away: try to be better, and potentially be severely punished by investors.

Many companies only start to take action on long-standing issues when the financial risks of not doing anything become higher than the likely costs they'll encounter.

YouTube, for example, is under fire for failing to adequately combat conspiracies and prevent child exploitation from being circulated. Its algorithm has a troubling record of surfacing and recommending content that violates its own policies. Major advertisers —including Disney and Nestle — started to bolt earlier this year after finding that their ads were appearing in videos full of offensive and sexually explicit comments aimed at children. In response, YouTube purged hundreds of its users and said it would change the way new videos are elevated and surfaced, following up on a crackdown in 2017 from reports that videos full of predatory comments were being recommended to kids.

Some lawmakers are growing impatient with tech companies' self-regulation — but it's not clear they can do it any better

Even as platforms have tried to regulate themselves in recent years, some policymakers' patience for letting them do so is growing short. But the legislative solutions some of them have proposed — or lack thereof — also struggle to match the pace of change in internet culture and the communities that foster extremist ideas and behaviors.

Congress so far has struggled to grapple with — or even understand — the many tentacles of problems plaguing social networks, from tackling the spread of misinformation to regulating how sites handle user data and privacy.

Some members of Congress have been woefully ill-prepared to even talk about tech issues (during one hearing last year, a lawmaker asked the Google CEO questions about his iPhone). And even when they are interested and equipped to talk about regulating the internet, many US lawmakers have been "reticent to clamp down at the risk of harming growth," Stewart noted:

In a Senate hearing in April, Sen. Orrin Hatch (R-UT) asked Zuckerberg what "sorts of legislative changes" he thought should be enacted to prevent a Cambridge Analytica repeat. Sen. Lindsey Graham (R-SC), who also pressed Zuckerberg on whether Facebook is a monopoly, asked the executive to submit some proposed regulations to him.

Still, interest is growing. In the 2020 presidential primary race, Democratic candidates have vowed to take on Big Tech — Sen. Elizabeth Warren has gone as far as proposing to break up Google, Facebook, and Amazon, while Sen. Amy Klobuchar is expected to make tech reform a banner issue for her campaign.

There's a growing appetite for reform elsewhere in the world. The European Union took a stand on privacy concerns with General Data Protection Regulation Act, or GDPR, a law enacted last year to compel transparency around the data that companies collect and how it is used. And now some countries want to crack down on extremist content, too.

A British Parliamentary committee wants Facebook to be held legally liable for the content posted on the platform. The legislative body recently wrapped up an 18-month investigation into the social media site, finding that it violated data privacy and competition laws. And in the wake of the Christchurch terror attacks, British officials are threatening that tech companies be "prepared to face the force of the law" if they don't put a lid on the spread of hateful messages.

The response to Islamic extremism online is often treated much differently than white supremacy

It's well documented that social media has played an important role in helping fuel extremism and hate. Just look to the spread of ISIS, which notoriously leveraged and exploited platforms to recruit new members and promote propaganda. But more often than not, US authorities focus on Islamic extremism, even as homegrown right-wing terror has begun to have its moment.

That holds true for the tech companies as well. Even as they worked up solutions to combat ISIS online, they've been flat-footed in their response to white nationalism and white supremacy. Last year, Motherboard found that while YouTube was cracking down on videos of ISIS recruits, footage promoting neo-Nazi propaganda stayed online for months and even years.

And when researchers from Program on Extremism at George Washington University compared far-right extremism with ISIS online behavior, they found that the growth in white nationalist movements outpaced Islamic extremism by virtually every metric.

The white nationalist datasets examined outperformed ISIS in most current metrics and many historical metrics. White nationalists and Nazis had substantially higher follower counts than ISIS supporters, and tweeted more often. ISIS supporters had better discipline regarding consistent use of the movement's hashtags, but trailed in virtually every other respect. The clear advantage enjoyed by white nationalists was attributable in part to the effects of aggressive suspensions of accounts associated with ISIS networks.

Part of that could be the difficulty companies face in identifying offensive far-right content. As seen with the Christchurch manifesto, far-right extremism has a unique life online with its own language that's embedded in memes and "shitposts" and is difficult to decipher. As Vox's Aja Romano outlines in an rundown of the manifesto's underlying message, the alt-right has mastered the art of online trolling to "distort what their actual message is, so they can claim plausible deniability that their message is harmful or bad."

But leaving it unchecked has consequences: The surge in online activity coincides with a rise in real-world hate, particularly in the US. One study found that the number of far-right terror attacks in America more than quadrupled over the first year of Donald Trump's presidency.

In the last year alone, there have been a number of high-profile flare-ups of far-right violence. A US Coast Guard and self-proclaimed white nationalist had stockpiled weapons and ammunition with plans to stage an attack targeting Democratic politicians, journalists, and judges. Last fall's Pittsburgh shooting targeting Jews at the Tree of Life synagogue left 11 dead. In October, a man sent 13 pipe bombs to prominent Democrats and critics of Trump.

None of those incidents prompted major reform efforts on tech companies' parts. But in light of the graphic massacre in New Zealand, there's a chance the conversation around right-wing extremism may change. The staggering violence of ISIS's campaign helped define it as a terror-driven organization and made tech companies and governments alike get serious about combatting its propaganda online. Are they prepared to do the same with white supremacy?

The Mosque Shooter Exploited the Power of the Internet

By Paris Martineau

Source: https://www.wired.com/story/mosque-shooter-exploited-power-of-internet/

Mar 19 – After each new horrific mass shooting, an all-too-familiar cycle often plays out: Reporters (myself included) race to attempt to unpack an alleged shooter's possible motivations by piecing together clues from their social media accounts and online postings before it all gets scrubbed from the internet. We do this in the hopes that it will somehow provide a window into their mindset in the months leading up to the attack, or at least bring us somewhat closer to answering that ultimately unanswerable question: Why?

But this approach carries with it potentially dangerous unintended consequences. At least 49 people were killed on Friday during attacks on two mosques in Christchurch, New Zealand, and like clockwork the cycle began almost immediately. But this time it was a bit different. The alleged shooter himself had provided the world with more answers and possible motivations for his own actions than it seemed the internet knew how to handle.

Hours before the attack, the alleged shooter took to Twitter and 8chan—an online messaging board known for its distinct brand of toxicity—to announce his plans and share links to a Facebook account which later live-streamed 17 minutes of the massacre. He also linked to a 74-page document littered with awkwardly placed ironic memes and references to various toxic ideologies that many news outlets have since deemed his "manifesto." On 8chan, the links were accompanied by a request: "I have provided links to my [sic] my writings below, please do your part by spreading my message, making memes and shitposting as you usually do."

The internet largely did just that. The gory first-person Facebook video of the shooting quickly went viral, spreading across social media platforms like wildfire before platforms could take it down. Since then, pundits, analysts, and internet sleuths have been publicly dissecting and interpreting each line of his lengthy manifesto—along with his equally toxic social media presence—turning public discussion into something closer to a string of far-right rabbithole keywords.

There was no need for internet sleuths to track down his social media accounts and comb them for clues, as he broadcast their existence publicly: They were, predictably, filled with more made-to-provoke explanations for his actions. It was "a very clear instance of media manipulation," designed with the world's eye in mind, says Whitney Phillips, a Data and Society researcher who specializes in troll culture and the amplification of extremism online.

"The goal of media manipulation as an act is to generate the most amount of coverage possible, including intense focus on the perpetrator," says Phillips. "When journalists pore over motives and pore over all of the details of that person's life, even if the reporter is disgusted by their actions, that person still becomes the protagonist of the movie—and that's their goal: to be the central figure in this play."

When we talk about the actions of extremists—especially those with a hefty online presence—there's this tendency to take their statements and assertions at face value. It makes sense: If someone, say, regularly tweets out links to the Daily Stormer and predominantly interacts with neo-Nazis and white supremacists online, it's reasonable to assume they probably share those views. However, this approach fails to take into account the individual's proclivity towards media manipulation.

In the case of the Christchurch shooter, Phillips says, he displayed "a self-conscious awareness of" the internet at large's tendency to scour an alleged gunman's posting history for clues, "which is what makes choosing to jump at the manipulator's behest so incredibly dangerous."

Engaging with the toxic content produced by media manipulators makes it nearly impossible to avoid amplifying their views. The curse of the amplification game is that an idea or construct gets more powerful every time it's consumed, or rebroadcast.

To act more responsibly, Phillips recommends reframing the narrative so that it's no longer the manipulator's story. "The problem with so much of this coverage is that it falls into the trap of: It's their world and we're just living in it. Why does it get to be their story?" she added. "It just takes a lot of conscientious effort to figure out what are the bigger stories and how do we sidestep the stories that are ultimately just distractions."

Paris Martineau *is a staff writer at WIRED, where she covers social media manipulation, online extremism, and internet culture. Before WIRED, Martineau wrote about memes and conspiracy theories for New York Magazine's (now defunct) tech blog, Select All, and covered the future for The Outline. She's based in WIRED's New York office and spends far too much time online.*

750,000 Medtronic defibrillators vulnerable to hacking

Source: http://www.startribune.com/750-000-medtronic-defibrillators-vulnerable-to-hacking/507470932/

Mar 21 – As many as 750,000 heart devices made by Medtro nic PLC contain a serious cybersecurity vulnerability that could let an attacker with sophisticated insider knowledge harm a patient by altering programming on an implanted defibrillator, company and federal officials said Thursday.

The Homeland Security Department, which oversees security in critical U.S. infrastructure including medical devices, issued an alert Thursday describing two types of computer-hacking vulnerabilities in 16 different models of Medtronic implantable defibrillators sold around the world, including some still on the market today. The vulnerability also affects bedside monitors that read data from the devices in patients' homes and in-office programming computers used by doctors.

Medtronic recommends that patients use only bedside monitors obtained from a doctor or from Medtronic directly, to keep them plugged in so they can receive software updates, and that patients maintain "good physical control" over the monitor.

Implantable defibrillators are complex, battery-run computers implanted in patients' upper chests to monitor the heart and send electric pulses or high-voltage shocks to prevent sudden cardiac death and treat abnormal heart beats. The vulnerabilities announced Thursday do not affect Medtronic pacemakers.

Medtronic, run from offices in Fridley, says the risk of physical harm to defibrillator patients appears to be low, even though one of the two issues described by Homeland Security was assigned a CVSS base score of 9.3 out of 10. A higher CVSS base sore indicates a more severe vulnerability, but it assumes an attacker already has the knowledge and tools to mount the attack.

Although the vulnerabilities could be prevented by shutting off the devices' wireless communications, Medtronic is urging doctors and patients to keep the devices' wireless communications switched on. Remote patient monitoring can alert doctors to developing health or device problems and has been shown to improve outcomes in heart-device patients.

The vulnerabilities were discovered by two different teams of security researchers and reported to Medtronic, which reported it to authorities, Medtronic officials said.

Medtronic is now actively monitoring its network for signs that someone was trying to exploit the vulnerabilities. Medtronic officials say affected defibrillators contain a feature that shuts down wireless communications upon receiving unusual commands.

Dr. Robert Kowal, chief medical officer for Medtronic's cardiac rhythm and heart failure products, said in an interview that a hacker would have to be within 20 feet or so of the patient, would need detailed knowledge of the device's inner workings, and have possession of specialized technology to pull off the hack.

The Medtronic CareLink 2090 Programmer is a portable computer system used to program and manage cardiac devices in clinic and during implant. The device allows a doctor to set the exact parameters for when the defibrillator should send pulses or high-voltage shocks to the heart. It was among more than a dozen devices named in a March 2019 cybersecurity advisory.

"No. 1, this would be very hard to exploit to create harm," Kowal said. "No. 2, we know of no evidence that anyone's ever done this. And 3, we are working closely with FDA as this whole cyber issue evolves to make sure we are not only handling this problem but we're working on future devices to optimize security versus functionality."

The FDA is not expected to issue a recall. Rather, the vulnerabilities will likely be addressed through a future software patch, as happened last year with a widespread vulnerability in implantable defibrillators made by St. Jude Medical, which was acquired by Chicago's Abbott Laboratories in 2017.

Ben Ransford, CEO of medical-device security firm Virta Labs, said he agreed with the assessments of Medtronic and federal officials that the vulnerabilities in the Medtronic defibrillators were not serious enough to warrant replacement.

"If I had one of these devices, I would not be concerned that this meant an attack is coming, or anything like that," said Ransford, who was not involved in detecting or investigating the vulnerabilities.

A known weakness

But Ransford did say it was surprising that issues like the ones in Thursday's advisory continue to crop up in Medtronic defibrillators, since this variety of vulnerability has been known since 2008.

A decade ago Ransford was part of a team of researchers that tested a bacon-wrapped Medtronic Maximo defibrillator and came to the surprising conclusion that it could be hacked.

In the groundbreaking paper, the researchers reported that they could cause their compromised device to issue shocks on command, shut down its lifesaving features and change functionality so the battery would wear out.

"It looks like a manufacturer still has some work to do," Ransford said.

Ransford said the effects of the attack appeared to be essentially the same, regardless of the specific route used to attack the device. Medtronic officials said the vulnerabilities described in the 2008 paper involved a different communications protocol.

The Homeland Security advisory describes two specific vulnerabilities in the Medtronic defibrillators.

The more serious of the two is a vulnerability that could allow improper access to data sent between a defibrillator and an external device like an at-home monitor. The system doesn't use formal authentication or authorization protections, which means an attacker with short-range access to the device could inject or modify data and change device settings, the advisory says.

A second vulnerability allows an attacker to read sensitive data streaming out of the device, which could include the patient's name and past health data stored on their device. The system does not use data encryption, the advisory says. (Deploying encryption in medical devices is tricky because is increases computational complexity and therefore uses the battery faster.)

What to Know

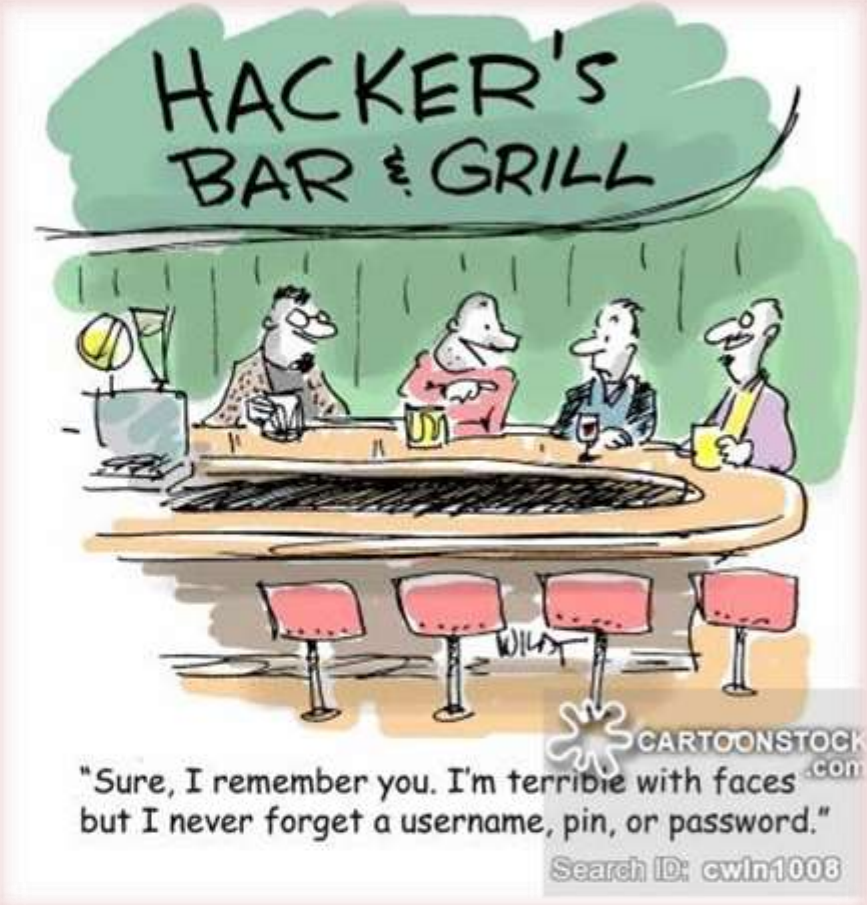
- Defibrillators do not need to be replaced. Medtronic says a software update is coming.
- Turning off the devices' wireless communication would prevent vulnerabilities but also beneficial features.
- Patients should use only bedside monitors provided by their doctor/the company.
- Patients should maintain physical control over their monitors, report concerns.

The common connection between all of the vulnerabilities and affected devices is Medtronic's proprietary Connexus "telemetry protocol" or communication system.

The FDA first approved a device with the Connexus protocol in 2006. At the time, the system was hailed as a breakthrough that would automatically be transmitted from an implanted device to an at-home monitor to the doctor's office via the internet.

However, Kowal noted that the vulnerabilities in Thursday's alert must be exploited in close physical proximity to the patient.

"Nothing about this issue is related to access via the internet," he said. Thursday's advisory affects two types of defibrillators: standard implantable cardioverter defibrillators (ICDs) as well as more complex cardiac resynchronization therapy defibrillators (CRT-Ds) that can deliver current to both sides of the heart. Some of the models are approved to be compatible with magnetic-resonance imaging, or MRI.


HACKER'S BAR & GRILL
WILEY
CARTOONSTOCK.com
"Sure, I remember you. I'm terrible with faces but I never forget a username, pin, or password."
Search ID: cwln1008

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter WMD

C2BRNE DIARY

DRONE NEWS

A New York man has been arrested after allegedly shooting down a Mavic drone

Source: https://www.digitaltrends.com/cool-tech/new-york-man-arrested-after-allegedly-shooting-down-a-mavic-drone/

Feb 24 – Cops on Long Island have arrested a man on suspicion of shooting a DJI quadcopter out of the sky.

The incident took place in the small community of St. James, about 50 miles east of Manhattan, on Saturday.

The drone — a Mavic 2 Zoom — was being used by a local volunteer group that specializes in searches for lost pets when it was allegedly shot down by 26-year-old Gerard Chasteen, according to the New York Post.

Chasteen reportedly fired three shots at the $1,249 drone, one of which knocked it clean out of the sky.

Lynn Fodale and Teddy Henn of pet-search group Missing Angels Long Island told the Post that when the signal went dead, they assumed a bird had attacked the drone.

But after making their way to the Mavic's last known location, someone nearby said Chasteen had used a shotgun to take down the drone before telling the pet-finding pair where the suspect lived.

Fodale and Henn said they confronted the alleged drone shooter, who reportedly told them that he fired at it because he didn't like it flying over his house. But the pair claim that flight records show that the Mavic was close by rather than directly overhead, and was being used to view a drainage ditch in search of the lost dog.

The police have since accused Chasteen of third-degree criminal mischief and prohibited use of a weapon. A court appearance is upcoming.

This isn't the first case of an irate property owner taking aim at a drone hovering close by, with more than a dozen cases reported in the U.S. alone in recent years. In 2015, a Kentucky man was arrested after blasting a drone out of the sky when he spotted it flying over his house.

Accounts of the event from the drone pilot and the accused didn't match up, but the subsequent court case saw the judge side with the suspect, prompting her to dismiss the first-degree criminal mischief charge against the shooter. Since that incident, the Federal Aviation Administration has said that it's a federal crime to shoot down a drone, citing the aircraft sabotage law.

The recent incident on Long Island comes as the government looks to gradually relax rules for commercial drone flights, with NASA's drone traffic control system likely to lead to more flight freedom in built-up areas in the near future. But opening up the skies to more drone flights in urban areas has the potential to upset more residents concerned about privacy, presenting a challenge for the authorities as well as companies like Amazon that want to use the machines to drop off customer orders.

Oh, and if you're wondering about the dog, the most recent reports suggest the mutt is still missing.

FAKE NEWS: The man was approached by Heathrow and Gatwick airport security officials in order to assist them with their drone threats. Free access to a variety of weapons and unlimited ammunition was offered along with a very appealing relocation package.

YouTube accused of making it too easy to build killer drones

Source: https://nypost.com/2019/02/27/youtube-accused-of-making-it-too-easy-to-build-killer-drones/

Feb 27 – It is "terrifyingly easy" to build a killer drone that can identify targets and make decisions to fire on its own, experts have warned.

Fears are growing that the snowballing production of deadly autonomous weapons could result in terrorist attacks and airports being held to ransom by individuals and extremist groups.

China is already "aggressively" exporting the most sophisticated killer drones and pilotless aircraft to Asia, Africa and combat zones in the Middle East.

But Pentagon defense expert and ex-US Army Ranger Paul Scharre pointed out that it takes just seconds for anyone to find all the software and pieces needed to build your own weaponized drone.

Hundreds of YouTube videos instruct viewers how to attach guns and AK-47s to drones — that can easily be bought online — from their own garage.

It is still completely legal to build and fly a weaponized drone on your property in the US.

You can even download trained neural networks for free that would enable the drone to identify targets and make decisions on its own.

Drones can "make decisions on their own"

Inspired by human brains, these computing systems are able to learn and operate using previous experience — with no human action required.

YouTube insists it removes content that provides instructional modification or transformation of a firearm in order to make it more dangerous or deadly.

But the ease at which autonomous drone technology is available for the masses is sparking fears among AI and defense experts across the world.

Especially since Gatwick Airport, near London, was disrupted for more than three days over Christmas last year due to unauthorized drone activity.

Scharre, the director of the national security program at the Center for a New American Security, told The Sun: "It's a terrifying reality that we're going to have to confront. People can build simple autonomous weapons and carrier weapons for terrorist attacks from their garage.

"We've already seen in the UK and US that drones are so ubiquitous that we have to be concerned about the threat from drones disrupting air travel."

"We need to prepare"

Scharre said the threat from drones is only going to "become more challenging as more people build autonomous drones and we need to prepare for that."

The defense expert, who wrote “Army of None: Autonomous Weapons and the Future of War,” said governments need to start thinking intelligently about countermeasures.

“It is a very real security challenge and we need to be about to defend effectively against these drones,” he said.

“We can’t live in a world where one individual can shut down airports or air traffic.

“We need to manage the possibility of threats in the third dimension — airports have great security on the ground, but drones just leap over that.”

Airports and arenas “vulnerable” to attack

Professor Noel Sharkey, who is co-founder of the Campaign to Stop Killer Robots and the International Committee for Robot Arms Control, shares this view.

He raised concerns that airports, concert venues, sports stadiums and government buildings in the UK are vulnerable to imminent attack from drone swarms and autonomous weapons.

The AI professor said experts have been warning the government about the “massive hole in our security” since 2007.

“This is what disturbed me about Gatwick — the absolute lack of preparedness,” he told The Sun.

“What I’m mainly concerned about is the possibility of a terror attack as ISIS already has this technology.

“We cannot be playing catch up like this. Our government security is not prepared.”

“No defense” against drone swarms

Perhaps most worryingly, he claims Britain has no effective defense against swarms of drones.

Both the US and China have been working on swarms of small aircraft (more than 100) that can be controlled by one or a few people or work in autonomous mode.

“You might be able to disrupt, or shoot down a few drones, but if there’s a whole swarm some of them will get through,” Sharkey said.

“There’s currently no way to block them.”

He also voiced fears that these drones could be used to attack arenas and football matches and they could even unleash chemicals.

Aviation Minister Liz Sugg said: “Flying drones illegally puts others at risk. The law is clear that these are serious criminal acts that hold lengthy prison sentences.

“The government is further strengthening the law by extending the no-fly zone around airports and from November all drone users must be registered and tested – which will help hold illegal drone users to account.”

“No-fly zones” widened

President Donald Trump signed an executive order earlier this month meant to spur the development and regulation of artificial intelligence.

The order aimed to improve access to the cloud computing services and data needed to build AI systems and promote cooperation with foreign powers.

It came amid warnings over China unleashing lethal fully autonomous drones that can carry out targeted military strikes.

US national security think tank Center for a New American Security (CNAS) said in a report that Chinese officials see this AI “arms race” as a threat to global peace.

Gregory C. Allen, the author of the report, said China is rushing to integrate ever more sophisticated artificial intelligence into weapons and military equipment.

One example is the Blowfish A2 drone, which China exports internationally and which Allen says is advertised as being capable of “full autonomy all the way up to targeted strikes.”

China unleashing sophisticated drones

The Blowfish A2 “autonomously performs complex combat missions, including fixed-point timing detection and fixed-range reconnaissance and targeted precision strikes.”

BLOWFISH A2

Depending on customer preferences, Chinese military drone manufacturer Ziyan offers to equip Blowfish A2 with either missiles or machine guns.

Allen wrote: “Though many current generation drones are primarily remotely operated, Chinese officials generally expect drones and military robotics to feature ever more extensive AI and autonomous capabilities in the future.

“Chinese weapons manufacturers already are selling armed drones with significant amounts of combat autonomy.”

Russia’s “kamikaze drone”

Russia has also unveiled a new and deadly kamikaze drone after it “successfully completed” trials.

The latest precision weapon from arms giant Kalashnikov “delivers explosives to any terrain, bypassing systems of air defense.”

The KYB (Cube) drone — with a maximum flying time of just 30 minutes — was showcased for the first time at the international IBEX arms exhibition in Dubai.

A video shows the unmanned military flying machine exploding as it reaches its target.

The Russian drone flies at speeds of between 50 and 80 mph and can carry a payload of explosives up to 6.6 pounds, say its manufacturers.

“This is an extremely precise and very effective weapon, incredibly hard to fight by traditional air defense systems,” said Sergey Chemezov, head of Rostec, a Russian state giant in charge of development strategic arms companies.

“The explosive can be delivered to target regardless of how well hidden it is.”

It operates “regardless of hidden terrains, at both high and low altitude,” he said.

Sensors, Drones and Artificial Intelligence at the Forefront at IWCE

Source: http://www.govtech.com/em/preparedness/Sensors-Drones-and-Artificial-Intelligence-at-the-Forefront-at-IWCE.html

Mar 08 – With all the new technology at our disposal, it seems counterintuitive that 911 dispatch times have increased by as much as 10 percent in some areas, but it's true.

Dispatching was traditionally a reactive task, but modern technology and all its sources of information has complicated that task, foisting on 911 call-takers streams of information, some of it accurate, some of it inaccurate and second- and third-hand and forcing call-takers to decide on its value.

With all this information cluttering up the system, what's needed is a process of curation to synthesize that information. That's the key to Next Gen 911, said Lawrence Hicks, vice president of engineering for *InterTalk Critical Information Systems*, in a keynote address at the International Wireless Communications Expo (IWCE) in Las Vegas Thursday.

"'911' is a motto for 'seconds count,'" Hicks said, but 911 dispatchers are suffering from information overload from a "fire hose" of information from different sources. The industry must provide tools for dispatchers to allow information to be curated into what's reliable, timely and accurate, he said.

Dispatchers have a "window to the world," with all the information available today, and being able to concentrate on what's relevant is the primary focus. That can be enhanced with tech solutions like artificial intelligence (AI) that can "coach" the information, providing insight such as how much stress the caller is under, or sensors that display on a GIS map and reveal how many firehoses are in a building.

Machine learning is another promising technology that records 911 events, analyzes the recordings, examines the outcomes and offers lessons learned in the future.

Hicks said the function of the human dispatcher is not going away, even with AI, but new technology will recreate the job into "dispatch as a service," a cloud solution. It all will amount to providing the right information at the right time in the right format.

System never blinked

In one of several short courses, RACOM President and CEO Mike Miller was able to provide first-hand lessons learned from a disaster — one that could have threatened the viability of

RACOM. He recalled July 19 of last year when an EF3 tornado, packing 144 mph winds, targeted Marshalltown, Iowa, and RACOM headquarters, a 25-year old building housing the public safety communications providers network and equipment.

Though the building sustained $7 million worth of damage, the network never went down and kept the town's 911 dispatching operational, as well as its EOC. In fact, 911 moved its dispatching operation into the RACOM building for more than three hours that afternoon, setting up card tables and a whiteboard for six dispatchers, until the dispatchers could return to their home base.

With the RACOM system still up and running after the tornado passed, Miller, acknowledging that he deals in reliability, reached out to his larger customers to assure them that the system was well. Having a backup generator and testing it weekly paid off for Miller. But it wasn't enough to have just one spare generator, and he ended up with three to assure things kept running until commercial power returned five days later.

There were other key calls made initially after the tornado, including calls for someone to come and quickly patch up the building before the rains came. "Rain and electronics don't mix," Miller said.

Another was to local hotels to book rooms for employees and another was to deal with the debris around the building. Miller also worked with local law enforcement, which provided escorts for key personnel coming and going.

Another course discussion involved drones and sensors, part of which involved outfitting drones with sensors to glean information about wildfires and floods. A drone, equipped with a sensor, can be sent out to determine where the hottest part of the fire is, instead of sending someone up the mountain. The difference is that the drone can assess the situation in a few minutes, much more quickly than it would take a human to hike the mountain or send an aircraft.

Drones can also be used for fatal vehicle accidents. In this case, law enforcement sometimes takes hours to collect all the information necessary to do the proper investigation, causing traffic jams for several hours. It would take a drone minutes to collect the same information.

Sensors, though expensive, can also save lives during floods. The most common cause of death during flooding is from people trying to drive vehicles through a flooded area. It takes just four inches of water to float a car, and there is no way of telling what's under the water — without a sensor. Modeling has been used to this point but can't be as accurate as a direct sensor.

And in another course, Department of Homeland Security Science and Technology Directorate personnel showcased an Information Sharing Assessment Tool that agencies can use free to assess and develop operability within an organization and interoperability with outside entities.

EDITOR'S COMMENT: Allow and encourage aerial solutions for emergencies, disasters' management, the military, S&R operations, border surveillance but DO NOT ALLOW selling drones to citizens just for fun. Once in a lifetime let global security prevail over profits.

Hands-Free Flight with EEGSmart's Mind-Controlled UDrone

Source: https://newatlas.com/udrone-mind-controlled-drone-umind-review/58791/

How much more fun could drones be if you got fiddly hand controllers out of the way and flew them with your mind? That's the question EEGSmart poses with its UDrone mini-quad, which responds to brainwaves and head movements instead of thumbsticks. It's not perfect, but it does give a glimpse of a mind-controlled future. The Udrone itself is fairly unremarkable; it's a lightweight mini-quadcopter with 2-inch props, nice plastic bumpers to save it from damage when it bumps into a wall, and an 8-megapixel, 1080p-capable camera. You can fly it using your mobile phone, in which case it works like most similar small quads, but also has some smarts under its belt with face tracking, subject tracking and gesture recognition. It flies for six or seven minutes on a battery, which is about right for this size of thing. The camera isn't anything to write home about, but it streams video back to your phone in real time as long as you're within Wi-Fi range. So far, so ordinary. In a second box, you get EEGSmart's UMind Lite headset, and here's where things get interesting. The headset has a number of sensors built in. There's an EEG, or electroen-cephalography sensor, which measures electrical activity in the brain. There's an EOG, or electro-oculography sensor that measures eye movements by monitoring the electrical potential between the front and back of the human eye. There's an EMG, or electromyog-raphy sensor, that measures electrical activity in response to a nerve's stimulation of muscles. It also has gyros and accelerometers, and patented gear built in to amplify signal and squash noise from the finicky brain and nerve sensors. It charges via USB, like the drone itself, and sits over the ears across your forehead,

just above your eyebrows. You pair it to your phone through the UDrone app, and then set the drone into "mind control mode" to activate it. To launch the thing, you have to attain a state of Jedi-like focus. Which is fine, I've been doing my Sam Harris meditation tapes. You can watch your mental focus activity summarized into a number in the UDrone app. If your thoughts are a little skittery, you might find that number hovering around 15 or 20. When you zen out into a space of relaxed focus, it rockets upward. I've seen as high as 400 or so, which made me feel like Yoda. To launch the drone, you pop it into mind control mode, then focus your way to 150 or more, and the drone lifts off to a chest-high hover. Focusing hard on the drone can con-vince it to rise, letting your mind wander makes it fall, in little stepped levels. To move it, you tilt your head. This feels extremely intuitive for right-to-left move-ments, and works really well; the drone tilts whichever way you tilt your head. EEGSmart has decided, however, to reverse things for forward and backward flight – probably thinking that you want to be looking up rather than down as your drone is flying forward. I thoroughly disagree with this assessment and would much rather the drone simply tilted whichever way I tilt my head. Yaw control is done by turning your head sideways then back again, and this happens in 45-degree increments. You blink twice to start the camera timer, and clench your jaw when it's time to land. After burning through half a dozen battery charges, I'm definitely getting the hang of it. Altitude control is by far the hardest and least responsive control, since it's difficult to know exactly when you're building or shedding focus, but the drone does eventually do what you want. The head tilt control works great – it'd be even better if the forward/backward inputs weren't reversed – and while the camera does fire off a lot of shots without me asking for it, I've done pretty well with the landing command. It's a pretty nifty feeling controlling a drone this way. It does suffer from being very digital – especially the stepped altitude changes and 45-degree turning implements, which are not a smooth way to fly. But it does give you a real sense of what hands-free flight could feel like, and as such we'd rate it a fun little toy to have around. It's quick enough to learn that you can pass it around for visitors to play with, and the prop guards do a good job stopping this thing from banging off the walls. You'll want to fly it indoors, too, because wind does blow it around a bit, and that can be hard to correct for without the rock solid thumbstick controls you'd normally be using. I do see a future in this kind of thing. I think UDrone should build some sort of training feature into the app, which lets you watch your control inputs in real time so you can make sure of exactly what signals you're sending. That'd make the learning curve quicker without burning battery on the drone. It's a pretty remarkable little gadget to play with, and I look forward to seeing where this kind of tech goes.

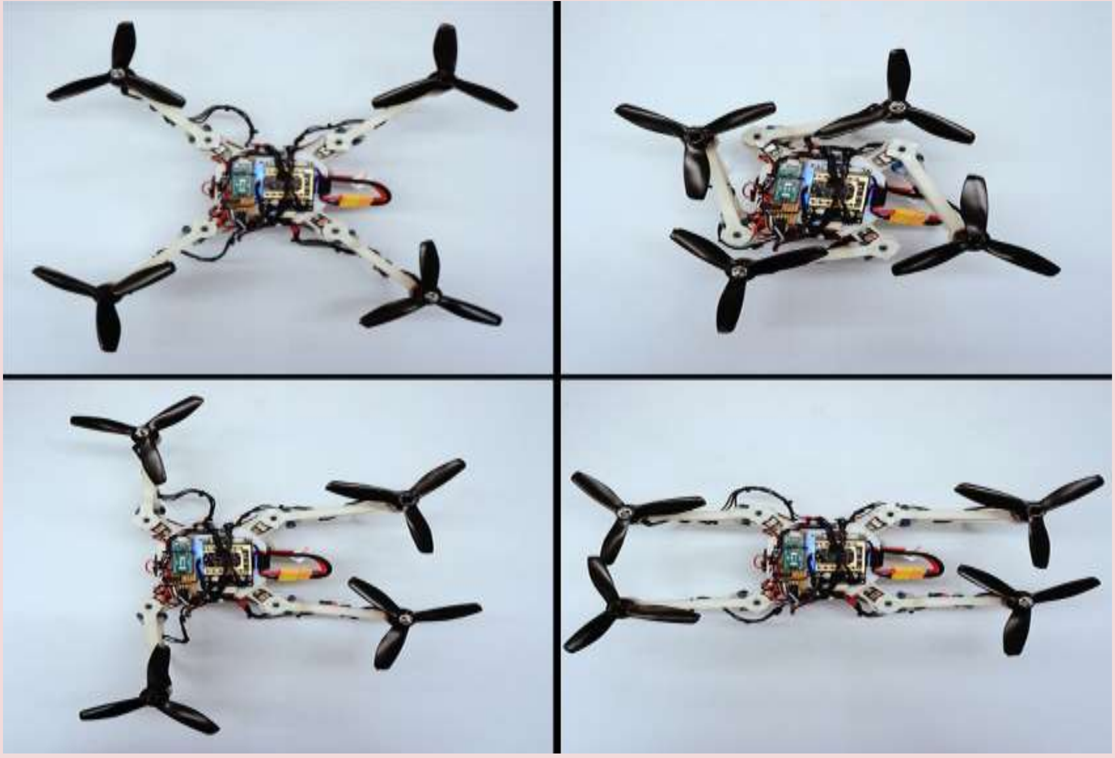
Swiss Development to Alter Rescue Capabilities Forever?

Source (+video): https://i-hls.com/archives/89869

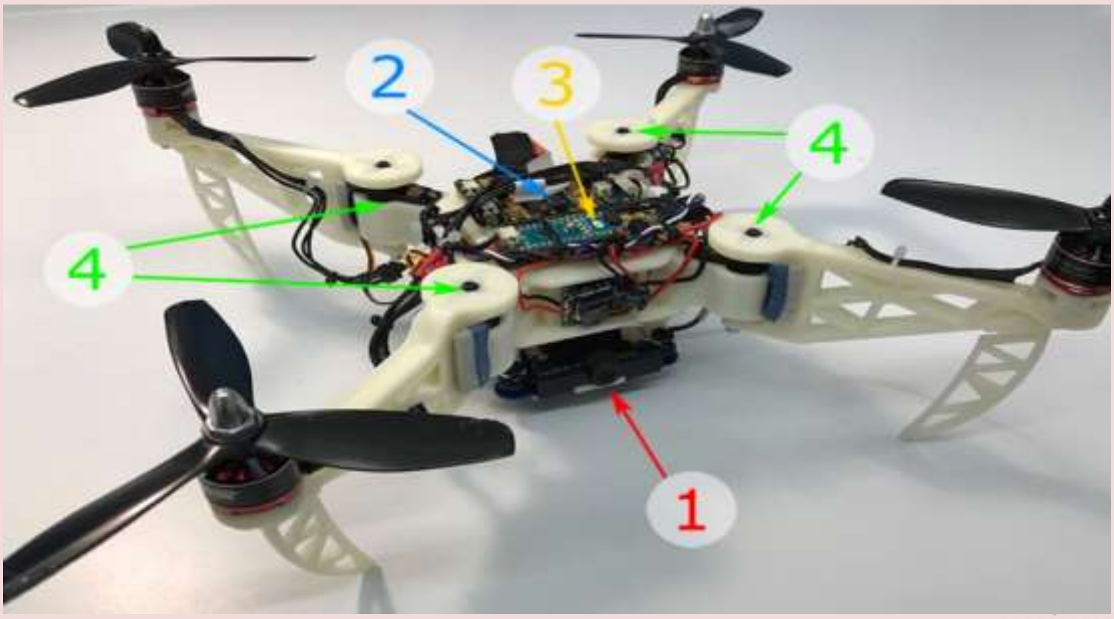
Mar 18 – **A team of researchers at the Zurich University has developed a drone that can change shape in flight.** The chief target of the drone is to assist with search and rescue missions. Able to contract and fold, the aircraft can enter small cracks and spaces to stream footage to rescue teams via its two integrated cameras. Its design is meant for use in disaster zones that become inaccessible to rescuers due to safety concerns or physical restrictions.

Davide Falanga, one of the developers, explained in an interview for CNBC that the drone could make rescue missions more efficient and effective. “This drone could have multiple impacts – it can go into areas that would otherwise be inaccessible and let rescuers enter and explore a collapsed building. It was crucial for us to use the most efficient and stable systems in order to let the device allow it to fly longer.”

Funded by the Swiss National Science Foundation, the project took six months to go from concept to prototype. However, as the drone is still in early development stages, its developers have no timescale for a wide rollout. According to the research paper written by the drone’s developers, their aircraft “could lead to a shift in the research community towards morphing aerial vehicles." However, they noted that there were still several unsolved research questions, such as "automatic morphology selection," which refers to the robot's ability to autonomously take the best shape for the task at hand.



Maria Kamargianni, lecturer in transport and energy at University College London, told CNBC that privacy concerns would need to be addressed before the drone could be commercialized. "This is a very promising technology for search and rescue projects, and it's much more economically viable than existing options. In circumstances where a helicopter or a drone could be used, a drone would be much cheaper to deploy," she said.



Close-up of the foldable drone and its components: (1) Qualcomm Snapdragon Flight onboard computer, equipped with a quad-core ARM processor, 2 GB of RAM, an IMU, and two cameras. (2) Qualcomm Snapdragon flight electronic speed controller. (3) Arduino Nano microcontroller. (4) Servo motors used to fold the arms.

"The technology has lots of other applications as well — for example, it could be used to examine the quality of materials on a collapsed bridge. But technologies must be developed in line with public acceptance of them, so these drones should be designed in a way that notifies the public they are being used by the authorities — this could be done by using distinctive colors. In rolling them out companies would also have to make sure they are not violating personal data regulations."

Frankfurt Airport mayhem as all planes grounded after drone spotted flying near runway

Source: https://www.thesun.co.uk/news/8699996/drone-frankfurt-airport-chaos/

Mar 22 – Flights were grounded at Frankfurt airport today after a drone was spotted near a runway.

It brought chaos to one of the world's busiest air hubs as planes were diverted to other airports and passengers left stranded.

The airport wrote on Twitter: "A drone was sighted today at Frankfurt Airport. Our priority is Safety First. Flight operations were suspended for 30 min. until the Police cleared the situation. Flight operations are back to normal."

It also claimed there was "no chaos".

The incident is said to have occurred in the southern part of the airport, according to a spokesperson.

Flights were grounded from around 5.15pm until around 5.45pm, local time.

It was initially thought two drones had been sighted but it was later clarified that only one had been seen.

The airport is operated by Fraport and serves as the main hub for Lufthansa.

It is the world's eighth busiest airport, serving over 57million international passengers a year.

Unconfirmed reports had previously said flights had been due to "software issues".

The body that oversees European air traffic management Eurocontrol said there had been "significant" delays at the airport.

Eurocontrol has yet to respond to a request for information by The Sun Online.

The delayed flights caused problems for travellers.

Mike on Twitter wrote: "What's going on with Frankfurt airport? Something serious? My flight is cancelled but dunno why."

Just before Christmas last year Gatwick Airport was hit by travel chaos after a drone was sighted amid the festive getaway.

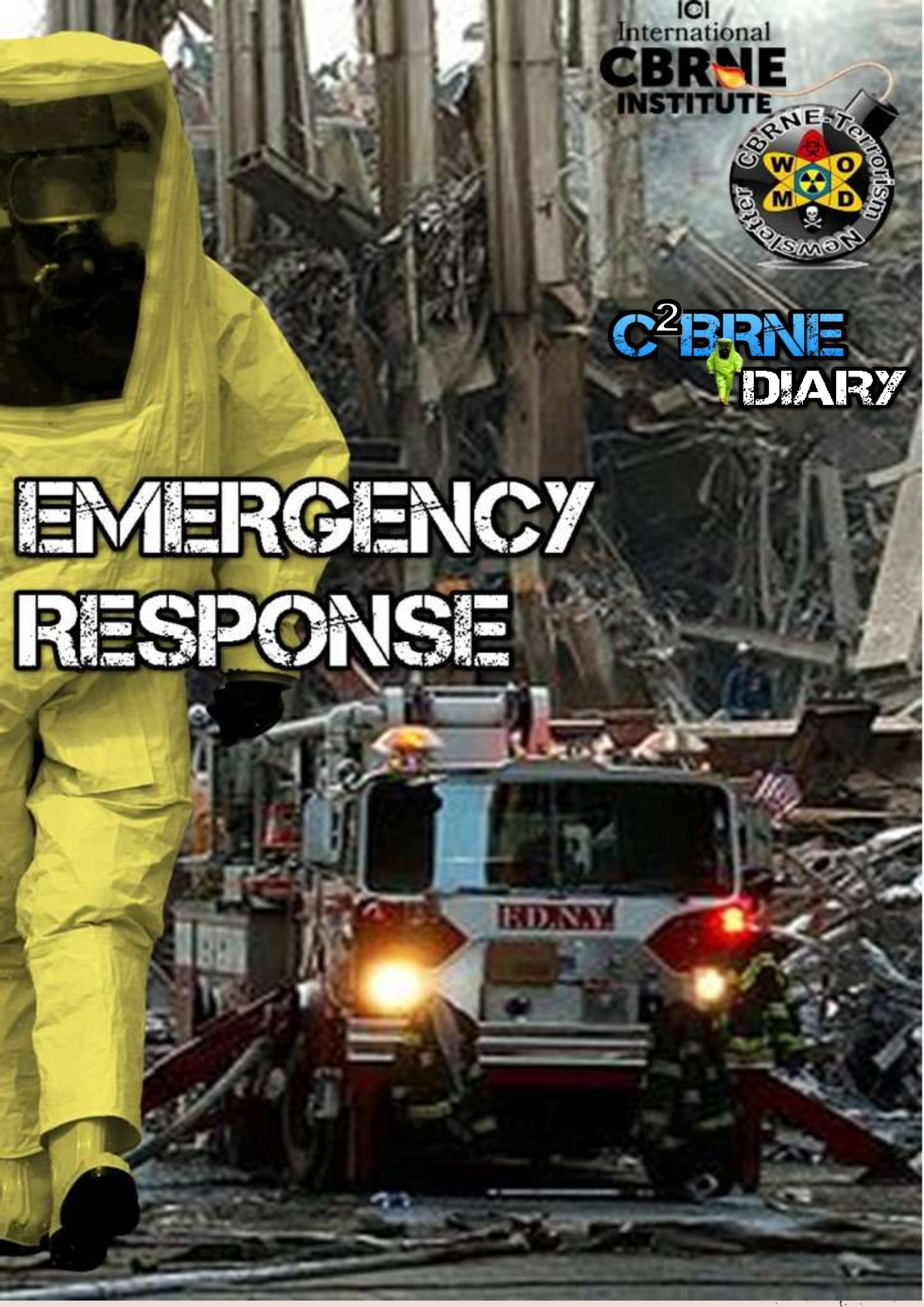
The London airport was brought to a stand-still for almost three days and 1,000 flights were cancelled or diverted, affecting 140,000 passengers.

Another drone was also spotted in February this year flying over a runway at Dublin airport.

Flights were grounded for 30 minutes.

And a third was spotted over Heathrow airport in early January this year, causing flights to be suspended for almost an hour.

EDITOR'S COMMENT: I am starting to think that maybe it is an organized campaign by companies offering anti-drone technologies 😉



International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C²BRNE DIARY

EMERGENCY RESPONSE

Report: We've Failed Miserably at Preparedness

Source: http://www.govtech.com/em/preparedness/Report-Weve-Failed-Miserably-at-Preparedness.html

Mar 01 – A review of the last couple of decades of the federal government's approach to developing more disaster-resilient communities yielded the stark affirmation that those efforts have failed because of a top-down, one-size-fits-all approach that doesn't reach most communities.

A better approach, a new FEMA Higher Education Program report says, is to develop individual cultures of preparedness from the bottom up that could eventually lead to a more resilient nation.

The *report* was the result of a two-day workshop that convened 39 expert scholars and practitioners at Georgetown University to discuss how to build a culture of preparedness. The theme of the report is that to build a culture of preparedness, the efforts from the past that have been mostly ineffective should be abandoned in favor of efforts that encourage local engagement through "culture brokers" with individual communities.

"We've achieved our national preparedness goals when it comes to first responders [as per Presidential Policy Directive 8] but when it comes to preparedness of individual households and communities, we've failed," said Laura Olson, a lead author of the report. "To say we've failed it putting it mildly. We really haven't been able to achieve any of our goals for two decades at least, which is the amount of time we've been tracking this."

The report suggests that it's time to change strategies and discontinue the same top-down approaches like, "Buy a kit" and "Go to the Ready.gov website" because people aren't paying attention. The problems with those approaches are that they don't understand and articulate individual community needs, values and sense of identities, and they generalize the message.

The typical message has portrayed the family in a way that reaches just a portion of the population and misses big portions of the population. Plans should instead acknowledge different livelihoods, family structures, ethnic backgrounds, religious practices and so forth.

"Shift the lens from looking from the ground up, a radical shift to reframe how we go about this and understand what we're doing," said Kate Browne, a lead author of the report. "To reach a unified culture of preparedness is probably possible, but only if the inherent variabilities of those communities are engaged with directly."

The key difficulty with past approaches is that communities across the country lost trust in the government and therefore, the report says, government is not the best entity to reach out to communities with a message of preparedness.

There must be recognition that there is going to be a cultural difference in communication, whether it be communication between emergency managers and communities or any other entities, and to eliminate assumptions.

An example she put forth was working with indigenous tribes in Alaska and the fact that the first person to speak shouldn't be a government person but an elder from the tribe, according to customs and norms.

"It's recognizing that the party you're speaking to has its own way of communicating in their own styles and understanding of the world and what the risks are and how to deal with them," Olson said.

It's an acknowledgement that preparedness is not something that is delivered from the outside, but that people may already be working on as best they can with a variety of limitations that may be hampering their efforts.

"So many of these communities that are so vulnerable are dealing with a set of difficulties on a daily basis that make it difficult to put preparedness for something unseen, at the top of the to-do list," Olson said.

That's where culture brokers need to be developed that understand the community and its needs and what is already being done in that community to develop preparedness and enhancing that. Emergency managers can facilitate community preparedness through these culture brokers.

The report says that rather than immerse emergency managers in all kinds of impossible forms of cultural awareness and education there is a better solution, and that is to locate people who are steeped in this knowledge who are in the community.

And rather than go into a community and tell community leaders what they should be doing, emergency managers should work with those communities to enhance their efforts.

It will take resources and a suggested solution was to change how grants are awarded to encourage a bottom-up approach. Funding could be used for using researchers who could be trained in this type preparedness methodology who could in turn teach their knowledge to others and create a cascading effect.

Forecasters use Iron Dome science to handle disasters

By Abigail Klein Leichman

Source: http://www.homelandsecuritynewswire.com/dr20190307-forecasters-use-iron-dome-science-to-handle-disasters

Mar 07 – Typhoons, floods, droughts, earthquakes, hurricanes, wildfires — the frequency and intensity of natural disasters across the globe are worsening, and these deadly events could continue plaguing the planet as a result of climate change.

Hoping to minimize disruption of essential services in disaster zones, government and utility officials are seeking better solutions for preparation and management of catastrophic weather events.

One new solution is a sophisticated product from mPrest Systems, the private Israeli company that famously developed the command-and-control software inside Israel's Iron Dome missile-defense system.

Natan Barak, founder and CEO of mPrest, explains that the Major Event Management Application (MEMA) automatically forecasts the extent, location and progress of damage via a network of sensors and systems that jointly gather and analyze current weather and other relevant data using advanced algorithms.

"It is based on the same 'system of systems' architecture we developed for the Iron Dome," he tells ISRAEL21c. "We are now applying rocket science, which was originally designed to save lives, to improve quality of life."

How does that work?

"The Iron Dome is, in essence, a real-time distributed asset analytics and management system," he explains. "The system accumulates data from tens of thousands of sensors to detect when a missile is launched, calculate its path, and decide if, when and where to intercept so that citizens and communities remain safe."

That same technology can be integrated into, say, smart-grids and cloud-based irrigation systems. And in the case of MEMA, it helps utilities handle disasters.

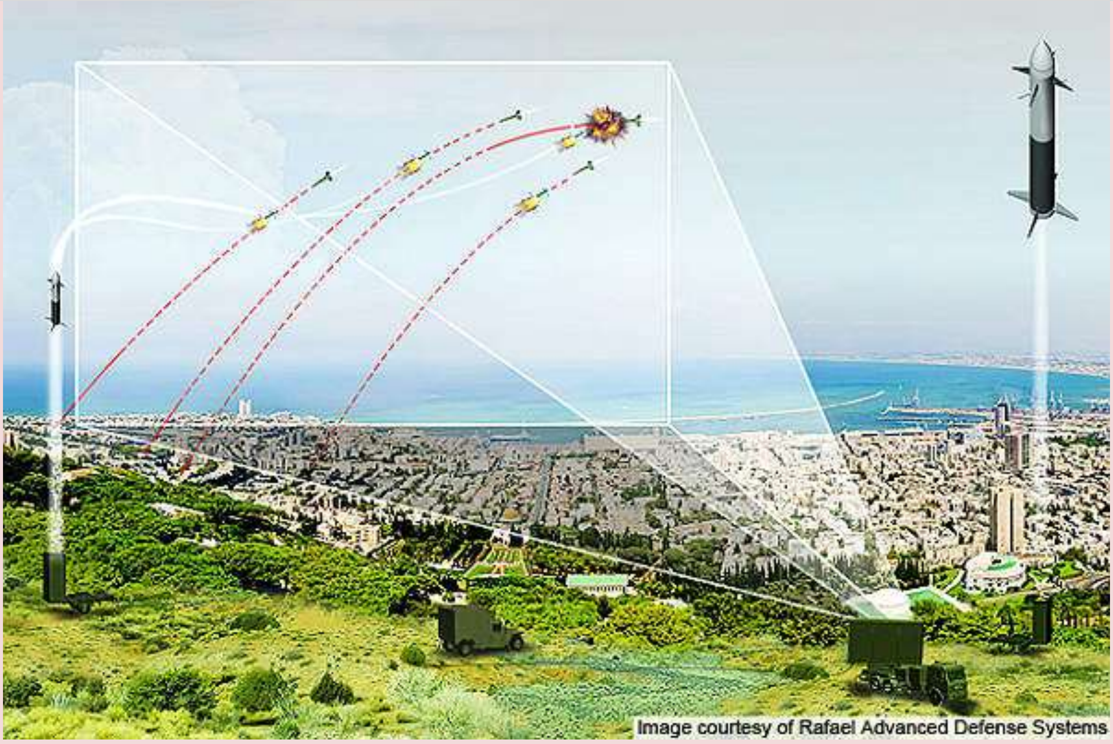


Image courtesy of Rafael Advanced Defense Systems

Earthquake scenario

Let's imagine, for example, that an earthquake is anticipated in a city like San Francisco.

First of all, MEMA would enable local utilities to develop simulation tools for a disaster plan by leveraging historical data from previous disasters.

Then, based on data from hundreds of thousands of sensors, the application would pinpoint high-risk areas where resources should concentrate in order to mitigate potential damage.

Once the quake hits, MEMA would automatically notify the utility, in real time, of incidents and continuously gather data from its sensors and systems — including satellite and drone imagery – to provide information on rising temperatures, rising wind levels, unusual ground motion, and more.

Barak says the application's sensors can also do a "health check" of critical assets such as power lines and electrical transformers so that utility and other officials can make informed real-time decisions.

"Based on the earthquake's epicenter, ground movement and more, the application can help identify power and utility infrastructure — lines, transformers, breakers, etc. — as well as critical facilities — schools, hospitals, etc. — that are in the event's path," Barak tells ISRAEL21c.

With this information in hand, officials could assign restoration crews and materials based on location and damage assessment.

"The 'system-of-systems' application can then combine both real-time and filed data to create an optimal restoration plan that accelerates recovery times and reduces restoration costs," explains Barak. Prest is in discussions with potential utility clients for MEMA, many in the United States.

Smart cities

Barak says this latest product is part of mPrest's increasing focus on the distributed energy resource management system (DERMS) market.

Based in Petah Tikva, mPrest was founded in 2003 by command-and-control technology experts originally from the defense industry. Today the company has 240 employees and additional offices in the US, UK and Australia.

In partnership with system integrators and organizations, mPrest develops monitoring and control solutions that serve defense and security organizations, electric and water utilities, smart cities, fleet management companies, and other enterprises worldwide.

Two years ago, the New York Power Authority deployed mPrest's Asset Health Management application at its

Niagara Power Plant, one of the largest renewable energy sources in the US. The application enhances the reliability and cost effectiveness of its transformer system by accurately diagnosing and predicting potential failures.

In January, mPrest and Atlanta-based Southern Company energy company received a BIRD Energy grant to develop and implement a solution to enhance the resiliency, efficiency and flexibility of Southern Company's distribution system in the face of "rapidly decentralizing networks, sharp changes in energy demand, extreme weather events and cyber security threats."

Energy utilities are also one of the main clients for mPrest's mCity platform, which helps municipalities optimize resource consumption, improve decision-making and planning, engage residents and improve overall quality of life and services.

Flexible implementation options for mCity are designed to cut the typically expensive and lengthy time it takes to get smart-city infrastructure installed; it can start out small and grow as needed.

Barak says mCity offers several unique features that set it apart from monitoring, control and analytics products and platforms offered by major multinationals such as GE and Siemens: for instance, the ability to integrate quickly with a client city's existing and future third-party platforms and sensors of any brand; and the ability to include smart energy in the package.

"We offer everything under a single platform," says Barak. "None of our competitors offers all these capabilities in one overarching 'system of systems.'"

Just as the market for mPrest's Major Event Management Application may expand due to natural disasters influenced by climate change, Barak predicts that mCity will be in greater demand as cities seek ways to provide efficient and reliable digital infrastructure serving the increasing population shift to urban areas.

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

Next Gen TV Could Be Another Tool in Public Safety Arsenal

Source: http://www.govtech.com/em/preparedness/Next-Gen-TV-Could-Be-Another-Tool-in-Public-Safety-Arsenal.html

Mar 05 – In this era of highly advanced technology, some fire and EMS agencies still use paging systems to communicate about incidents. The communication is often sequential in nature and not the best avenue for sharing urgent information.

That's what prompted the North Carolina Department of Information Technology (NC DIT) in partnership with the Wireless Research Center of North Carolina and UNC-TV Public Media, have embarked on a project they hope will change that.

With the advent of ATSC 3.0/Next Gen TV, which is based on Internet protocol and merges broadcast TV with the Internet, researchers hope they can channel more information simultaneously through broadcast television to give first responders more real-time data, video and other information, including alerts, more efficiently.

In the late 1990s, there was a transition from analog broadcasting to digital, and all analog broadcasts ended in 2009 with the transition to digital television using the Advanced Television Systems Committee (ATSC) standard. ATSC 3.0 is an evolution of that standard.

"Next Gen TV is kind of the digital evolution of broadcast TV," said Gerry Hayes, CEO and founder of the Wireless Research Center. "ATSC 3.0 will provide content in less bandwidth, so not only will standard-definition TV broadcast be made to be HD, the bandwidth footprint will be smaller and will be able to have the same content in a smaller part of the pipe."

Hayes said one of the first applications of Next Gen TV could be replacing the pagers that some first responders use, or enhancing their efficiency. With Next Gen TV, the transmission is simultaneous, and specific data, including weather mapping and video content, could be targeted to certain receivers.

"Like in an emergency response situation, a lot of high-data content can be pushed out and targeted to specific people and large groups of people if needed," Hayes said.

Red Grasso is a former firefighter who is now director of the First Responder Emerging Technologies Program for NC DIT. He explained the pager system as 60-year-old technology, usually 100 watts coming from a 200-to-300-foot tower, covering maybe a county or two and operated on the local level.

"Broadcast television is hundreds or thousands or a million times greater in power with 10 times greater height that is going to have a bigger footprint and much better building penetration and better overall coverage than today's public safety analog paging systems," Grasso said.

For the concept to work, there has to be a robust connection between the 911 call center and the paging system and the television station that will be transmitting it. It won't go over the Internet. It might be virtual private network, or a direct data connection, but it ends up being delivered to a device such as a pager or a chip or smartphone.

Grasso said there are three or four experimental ATSC 3.0 licenses on the air and one happens to be in North Carolina and thus the ability to experiment. So far, that's what this project is.

"Right now, it's not ready to be sold," he said.

"I can describe to you what the vision might be, but that will be influenced by the for-profit company that picks it up to market it."

Dealing with disaster

By Peter Reuell

Source: http://www.homelandsecuritynewswire.com/dr20190311-dealing-with-disaster

Must Read

Mar 11 – It took less than 90 minutes before students in Miaki Ishii's first-year seminar started to talk openly about revolt.

The unrest, however, wasn't due to any political issue currently making headlines, but to a small room in Harvard's Geological Museum and a handful of their classmates.

As part of the class "GeoSciFi Movies: Real vs. Fiction," students took part in a role-playing game that saw them acting as citizens of the island of Montserrat, the tiny country's government, and a group of scientists monitoring the island's volcano.

Over the game's five 15-minute rounds, each group requested funding for various projects — a new water treatment plant for the community, volcano monitoring instruments for scientists, or new ambulances for the hospital — which had to be balanced against the government's limited budget. Complicating matters, the island also faced devastating natural disasters over the course of the game, including a powerful hurricane and a massive volcanic eruption.

It wasn't long before things started to go sideways.

The "community" swiftly grew skeptical of the government's ability to quickly and effectively respond to pressing environmental concerns.

"The community group was constantly questioning the government's ability to protect its citizens from natural hazards," said Varun Tekur, who played a community member. "We expected our needs to be served regardless of the government's budget, and this did not happen."

When the funding for the promised water treatment plant failed to materialize at the start of the second round, community trust in the government plummeted and protests began to break out. By the next round, an uprising seemed inevitable.

“Can we just revolt against the government?” asked Charlotte Berry. “Can we start a coup?”

Before the end of the game, it actually happened — community members seceded and formed the Montserrat People’s Front, rejecting the existing government as illegitimate.

Students in the government group, meanwhile, grew frustrated with the short news items produced by the community, which featured headlines like “LIES and Lack of Concern from the Government” and “Possible Embezzlement and Fraud in the Highest Level of the Government.”

In the face of such turmoil, the warnings from students portraying scientists seemed to fall on deaf ears.

By the fourth round, all three groups came together to make one final decision — with scientists warning of an imminent eruption of the island’s volcano, they needed to formulate a plan.

Chaos ensued. Shouts, accusations, and arguments filled the room.

In the end, the students playing the government chose to evacuate to the northern tip of the island in an effort to avoid the pyroclastic flows — deadly masses of hot ash, rocks, and gases traveling at the speed of a train — produced by the eruption.

That decision paid off in the end: When the students’ score was tabulated, the class got an impressive 12 out of 25 — the best score of any of the four classes Ishii has led through the game.

In addition to providing an enjoyable hands-on experience for the students, the game also taught them a sobering lesson when, afterward, Ishii played a handful of video clips that showed some of the effects of the 1995 Soufrière Hills volcanic eruption, which left most of Montserrat uninhabitable.

“I could not believe that all that was left was a church tower peeking out of the ground,” said Oliver Hollo. “All these people’s livelihoods were altered, destroyed, and forever different. They had to start a new life because of this disaster.”

“The video at the end hit really hard,” added Jania Tumey, “and there was a real sense of immediacy with this game.”

“For me, the biggest thing as a student was that growing up we see all these natural disasters, and we wonder why there isn’t a plan for relief or more resources allocated to a particular source,” said Nadine Lee. “But after this you realize that even if you can allocate resources, there are repercussions, economic and otherwise, we may not think about.”

As their generation struggles to deal with the impacts of climate change, Berry said, it may be important for more people to understand the complex considerations that go into preparing for and dealing with disasters.

“This will definitely impact our generation,” she said. “So I think it’s important for young people to do things like this and learn more about what goes on behind the scenes, and how hard it is to coordinate disaster relief between multiple groups of people.”

Drew Kelner, a member of the scientists’ group, agreed.

“It amazed me how hard it was to get funding for projects I, as a scientist, knew would clearly benefit the safety of the whole island,” he said.

***Peter Reuell** is a Harvard staff writer.*

Keeping first responders, high-risk workers safer

Source: http://www.homelandsecuritynewswire.com/dr20190313-keeping-first-responders-highrisk-workers-safer

Mar 13 – Researchers, working with partners at other universities, have created a motion-powered, fireproof sensor that can track the movements of firefighters, steelworkers, miners and others who work in high-risk environments where they cannot always be seen.

The low-cost sensor is about the size of a button-cell watch battery and can easily be incorporated into the sole of a boot or under the arm of a jacket – wherever motion creates a pattern of constant contact and release to generate the power the sensor needs to operate.

McMaster says that the sensor uses triboelectric, or friction-generated, charging, harvesting electricity from movement in much the same way that a person in socks picks up static electricity walking across a carpet.

The sensor can track the movement and location of a person in a burning building, a mineshaft or other hazardous environment, alerting someone outside if the movement ceases.

The key material in the sensor, a new carbon aerogel nanocomposite, is fireproof, and the device never needs charging from a power source.

"If somebody is unconscious and you are unable to find them, this could be very useful," says Ravi Selvaganapathy, a professor of mechanical engineering who oversaw the project. "The nice thing is that because it is self-powered, you don't have to do anything. It scavenges power from the environment."

The research team – from McMaster, UCLA and University of Chemistry and Technology Prague – describes the new sensor in a paper published today in the journal *Nano Energy*.

The researchers explain that previously developed self-powered sensors have allowed similar tracking, but their materials break down at high temperatures, rendering them useless,

A self-powered sensor is necessary in extreme heat because most batteries also break down in high temperatures. The researchers have successfully tested the new technology at temperatures up to 300C – the temperature where most types of wood start to burn – without any loss of function.

"It's exciting to develop something that could save someone's life in the future," said co-author Islam Hassan, a McMaster PhD student in mechanical engineering. "If firefighters use our technology and we can save someone's life, that would be great."

The researchers hope to work with a commercial partner to get the technology to market.

— Read more in Abdelsalam Ahmed et al., "Fire-retardant, self-extinguishing triboelectric nanogenerators," Nano Energy 59 (May 2019).

Greater Responsibilities, More Recognition for Hospital Emergency Managers

By Theodore Tully

Source: https://www.domesticpreparedness.com/healthcare/greater-responsibilities-more-recognition-for-hospital-emergency-managers/

March 2008 – If the 9/11 terrorist attacks were the watershed moment for the nation's emergency-management profession in general, the defining moment for *hospital* emergency management, particularly in the planning stages, was Hurricane Katrina. That single event shattered what little confidence the public previously had in all emergency plans, especially those for hospitals.

For the emergency managers actually on the scene in Louisiana, and elsewhere on the Gulf Coast, it was disappointing, and somewhat disturbing, that their fellow citizens seemed either unable or unwilling to recognize the incredible sacrifices that so many responders, especially those outstanding healthcare providers who stayed with their patients at considerable risk to their own lives, made during and after that cataclysmic "once in a century" event. All but buried in the chaos and confusion that followed the hurricane were the facts that only the United States could have responded to such a disaster so quickly, that a great deal of incident-response planning *did* go right, and that probably *no* major U.S. institution, public or private, could have been fully prepared to respond to a catastrophic event of such unprecedented magnitude.

Nonetheless, and despite all the things that did go right during Katrina and its overlong aftermath, the nation's hospitals and other healthcare facilities should and must focus greater attention on the many aspects of their emergency-management plans and operational capabilities that obviously do require improvement.

If nothing else, Katrina focused the attention of administrators and lawmakers alike on what must be admitted were inadequate assumptions and, therefore, poor emergency planning on the part of most if not all of the hospitals directly affected by the monster hurricane. Prior to Katrina, most decision makers in the U.S. healthcare industry believed – erroneously, as it turned out – that a federal government response to an emergency, although perhaps not immediate, would follow in a few hours, not days.

One of Several Weak Links in the Chain

Most hospital administrators in New Orleans and surrounding areas, it seems safe to say, also believed that "sheltering in place" until help would arrive was a more advisable alternative than immediate (and potentially very dangerous) evacuation. These same officials, however, failed to see (among other things) the weakness of a hospital supply chain that sets a healthcare facility up for failure if reliable plans are not in place to ensure the re-supply of medicines, pharmaceuticals, and other medical consumables in a relatively short period of time – anywhere from 24 to 72 hours, for most practical purposes.

In the context of their previous professional experience – and/or the lack thereof – **clinical personnel also probably never believed that "the triage color," black, would ever have to be used outside of a battlefield,** or that physicians would be required to make some extremely difficult ethical decisions about the limited resources available to them – sacrificing some very seriously injured patients, for example, to save the lives of others who seemed more likely to survive.

Looking back at the many reasons *why* emergency planning could and should have been better – but was not – during Katrina and the flooding that followed, the first and most obvious questions asked by hospital administrators, and by legislators as well as the print and broadcast media, were: (1) "Who were the hospital leaders?" (2) "Who did the healthcare institutions put in charge of the important task of preparing hospitals for emergencies?"

The answers received were and are not surprising: Prior to Katrina, most U.S. hospitals and other healthcare facilities delegated those important planning roles and responsibilities to some of their best people. But almost all of those same people, understandably but unfortunately, had a huge number of other responsibilities as well. Until Katrina struck, and for some time after, most if not all U.S. hospital officials responsible for emergency planning usually had other full-time responsibilities as well, mostly in the provision of day-to-day healthcare for their hospital. **In short, prior to Katrina, hospital leadership during an emergency situation was at best a part-time responsibility.**

The Beginning of a Much-Needed Upgrading

Today's emergency planning requirements for hospitals have been significantly elevated over the past several years, thanks in large part to Hurricane Katrina. The detailed new planning requirements mandated by the Joint Commission (JC) and/or by local state healthcare regulators, for example, now require hospitals to greatly increase their institutional preparedness efforts. Additional funding resources, although still limited, also are being provided, though, and those hospitals that avail themselves of the funding available through federal grant programs are finding that some incredible deliverables accompany the grants.

Funding is possibly the most difficult problem facing most of the nation's healthcare facilities. The average citizen, or legislator, who knows what hospitals now are being asked to plan for probably would judge the long list of requirements to be both appropriate and reasonable. But very few if any emergency planners and hospital administrators believe that the funding currently available is adequate for the numerous tasks assigned. That economic fact of life does not, of course, diminish the responsibility of healthcare institutions to plan for what *can* happen in even a worst-case scenario, to schedule and carry out drills and exercises on the more realistic planning assumptions that are, in fact, now in place, and to use those drills to significantly improve the hospital's emergency planning and capabilities.

Although the JC's current requirements do not specifically spell out the need for a full-time or even part-time emergency manager, it seems clear that the job of emergency manager is now at least an FTE (full-time equivalent) position for most U.S. hospitals. The JC has said in briefings with hospitals and trade associations that it will hold hospital senior leadership responsible, under the leadership standards, if they do not allocate enough resources to their planning efforts. And

the Joint Commission itself plans to put even greater emphasis on emergency management in the future, so the standards may receive yet another upward revision.

In 2007, the Health Research Institute (HRI) commissioned a new study of hospital preparedness by Pricewater Coopers. In that study – *Closing the Seam: Developing an Integrated Approach to Health System Disaster Preparedness* – HRI clearly identified leadership as a crucial need and encouraged the industry to select, train, and both develop and encourage what the institute calls “Disaster Masters” – i.e., a new and, it would seem, higher level of emergency-management professionals.

HRI also recommended, not incidentally, that hospitals: (a) Develop a standard curriculum and establish certification requirements for their future emergency leaders; (b) redefine the roles of all hospital staff personnel during emergencies; and (c) finally allocate the funding needed to support the development and maintenance of the on-going leadership skills required of emergency leaders.

Clearly, the time of the Hospital Emergency Manager has arrived. Now all that the hospitals have to do is find them.

***Theodore Tully** has been director of Trauma and Emergency Services at the Westchester Medical Center (WMC) in Westchester County, N.Y., since 1994. Prior to assuming that post he served as a police paramedic/detective and as the Westchester County EMS (emergency medical services) coordinator. He also helped create and administer the WMC Regional Resource Center, which is responsible for coordinating the emergency plans of 32 hospitals in the greater Westchester County area.*

EDITOR’S COMMENT: Why we always need a “Katrina” to shape our plans and boost our preparedness? Do we really a CBRN Katrina to decide to have a hospital CBRN response unite ready, equipped and trained? Do we need a catastrophe to incorporate a CBRN Medicine module into the curricula of universities’ medical and nursing schools? I m sorry to say, but – 11 years after this article and 14 years after the hurricane with 1,833 fatalities – it seems that is what we really need – another massive disruption only to persuade hospitals administrations that the unexpected might happen in their shift, TOMORROW!

The Seven and a Half Traits of the Ultimate Emergency Manager

By Chas Eby

Source: https://www.domesticpreparedness.com/commentary/the-seven-and-a-half-traits-of-the-ultimate-emergency-manager/

Mar 13 – Emergency management is an evolving discipline that requires a progressive emergency manager to fulfill new and expanding requirements for success. Successful leaders in this field follow a systematic problem-solving process and excel at coordinating multiple agencies and information sources rather than simply being experts in one subject matter. The seven and a half traits discussed here describe the ultimate emergency manager.

The Federal Emergency Management Agency’s (FEMA) 2018-2022 Strategic Plan provides an updated “framework for supporting the United States before, during, and after disasters” and highlights new focal points for emergency management. The three strategic goals are as follows: to build a culture of preparedness; to ready the nation for catastrophic disasters; and to reduce the complexity of FEMA. Each of these goals requires different skillsets, capabilities, and objectives in order to be completed. Changing a collective culture requires social listening, understanding, and teaching. Readying a workforce to “enhance a collective readiness,” as FEMA states, requires facilitation and coordination skills and focusing on common problem solving across organizations within the emergency management system. Reducing complexity requires FEMA to be mission-focused and carry out processes in a simpler, systematic way.

The emergency management workforce must also adapt to meet changing strategies and requirements. The workforce may already be changing organically. Terry Hastings noted in a 2017 DomPrep article:

The discipline of emergency management is poised to benefit from three converging factors: an increasing number of millennials joining the workforce; the proliferation of emergency management related degree programs; and greater visibility and relevance of the discipline itself.

As both the field and the workforce evolve, the traits, characteristics, and capabilities of successful emergency managers also have changed.

The following seven and a half traits encompass the best characteristics of the ultimate emergency manager:

1. Recognize problems before they become disasters;
2. Operate proactively;
3. Focus on enabling;
4. Differentiate between simple, complicated, and complex problems, and act accordingly;
5. Know the audience;
6. Understand the importance of messaging;
7. Identify and seek the best people; and

7.5. Perhaps have direct experience in emergency management.

Recognize Problems Before They Become Disasters

If risk is a function of threat, vulnerability, and consequence, disasters are a function of incident magnitude, capability/capacity, and resilience. Good emergency managers reduce the negative impacts of incidents in order to avoid a disaster – or at least decrease the effects of a disaster. This is accomplished through recognizing problems before or as they occur and then identifying solutions. The best emergency managers do not necessarily know all of the answers. Rather, they enthusiastically ask questions and relay concerns to partner agencies while using emergency management's coordination role to identify the most efficient, multidisciplinary response.

Operate Proactively

In a 1799 letter, U.S. President George Washington wrote that "offensive operations, often times, is the surest, if not the only (in some cases) means of defence [*sic*]." State and local emergency management agencies typically have few physical resources to conduct tactical response operations. Emergency managers' "offense" is being proactive. Specifically, facilitating resource support and information needs based on a given circumstance in order to ensure that first responders and tactical operators can continue to function. Anticipating future needs and conducting future planning, while difficult, is an excellent trait for an emergency manager.

Focus on Enabling

Strong emergency managers focus on enabling personnel and partner organizations, even at the cost of strictly following plans and processes. Following Hurricane Katrina, Colonel Terry Ebert determined that the most effective organizations and people were those that were mission-driven versus compliance-driven. He wrote in a 2014 opinion article, "mission-driven organizations can be given an assignment in two or three sentences and then can deploy millions of dollars of equipment and thousands of people" based on the understanding of the overarching mission. Pre-disaster planning is essential for formulating relationships, outlining roles and responsibilities, and developing a general playbook. The best emergency managers may use plans as a guide, but also are driven by agency mission in order to find methods to meet incident objectives.

Differentiate Between Simple, Complicated, and Complex Problems, and Act Accordingly

David Snowden (chief scientific officer of Cognitive Edge) and Mary Boone (president of Boone Associates) authored a 2007 article in the *Harvard Business Review* on the Cynefin leadership framework, which was developed to "allow executives to see things from new viewpoints, assimilate complex concepts, and address real-world problems and opportunities." The framework usually places problems in four domains: simple, complicated, complex, and chaotic. The problems within each domain necessitate a different approach to solving them. Strong emergency managers intuitively understand which incidents, emergencies, or problems can be solved using a simple solution versus which ones require a complicated or complex-style solution. Within the disaster realm, a simple solution may be a checklist that dictates actions that would mitigate an incident. A complicated solution usually entails identifying good practice based on known best practices. According to Snowden and Boone "complicated context calls for investigating several options – many of which may be excellent – good practice, as opposed to best practice, is more appropriate." Complex problems are unpredictable and constantly changing, and usually involve multiple, intertwined systems. Emergency managers take a set of given circumstances, understand what resources they have at hand, can identify a complex situation, and then work together and with other disciplines to identify the best solution.

Know the Audience

Identifying solutions to complicated and complex problems that occur during disasters usually necessitates a multidisciplinary approach. Each involved agency and organization would have different, and perhaps even competing, motivations and priorities. Emergency managers must be able to understand their audience and empathize with their partners. Although consensus among different agencies may be beneficial, often the best actions are not simple compromises. Instead, they are multifaceted solutions that address all partners' priorities.

Understand the Importance of Messaging

The best emergency managers understand that effectively communicating to and with the public are important components of any disaster response. All emergency managers, not solely public information officers, should understand how their activities and operations during an emergency relate to effective risk communications to the public. A 2014 study from Sara Rubin et al. of the National Association of County & City Health Officials found that "local health departments' ability to more quickly communicate preparedness information to their communities could minimize adverse effects of disasters." One of the government's most essential roles during a disaster is to relay transparent information and direction to the public. Working with the traditional media and interacting directly with the public through social media and other platforms is an essential function and is at the forefront of the ultimate emergency manager's mind.

Identify and Seeks the Best People

Emergency management is a discipline that requires both external and internal collaboration. The best emergency managers identify colleagues who can excel in high-pressure situations and have many of the traits listed above. Furthermore, they empower and promote the best people in order to enable them to solve problems before, during, and after disasters.

Perhaps Have Direct Experience in Emergency Management

Experience in emergency management and related disciplines can be useful, especially for senior leadership positions. However, it is not essential for most staff-level positions. Agencies and organizations should focus on capability-based hiring practices. New staff can be trained and learn emergency management. Other capabilities, such as project management, problem solving, and active facilitation, are paramount for burgeoning emergency managers.

Conclusion

Emergency management is an evolving discipline with a broadening scope. In order to be successful, strong emergency managers must follow systematic processes and excel at coordinating multiple agencies and information sources while interacting well with partner organizations and the public. Anyone who exhibits most or all of the traits outlined in this article would likely be an excellent emergency manager.

This article is dedicated to Donald "Doc" Lumpkins, who exhibited the traits outlined above.

__Chas Eby__ is the deputy executive director of the Maryland Emergency Management Agency (MEMA), where he oversees all operations, administration, and programs at the Agency. Previously, he held the positions of director of disaster risk reduction and external outreach branch manager at MEMA. These roles included developing strategy and overseeing disaster recovery, public information and outreach, individual assistance, hazard mitigation, and community and private sector preparedness. Prior to joining MEMA, he was the chief planner for emergency preparedness at the Maryland Department of Health. He received a Master of Arts degree in Security Studies from the Naval Postgraduate School. He previously graduated from Boston College. He has completed the National Emergency Management Executive Academy and is an adjunct professor teaching both public health preparedness and homeland security planning and policy at Towson University.

I THINK WE MAY NEED TO UPDATE OUR DISASTER RECOVERY PLAN. THIS ONE SUGGESTS WE ALL RUN AROUND IN CIRCLES SHOUTING 'WHAT DO WE DO?!!' 'WHAT DO WE DO?!!'

ICI International CBRNE INSTITUTE

C2BRNE DIARY

ASYMMETRIC THREATS

Evidence for man-made global warming hits 'gold standard'

Source: https://uk.reuters.com/article/us-climatechange-temperatures/evidence-for-man-made-global-warming-hits-gold-standard-scientists-idUKKCN1QE1ZU

Feb 25 – Evidence for man-made global warming has reached a "gold standard" level of certainty, adding pressure for cuts in greenhouse gases to limit rising temperatures, scientists said on Monday.

"Humanity cannot afford to ignore such clear signals," the U.S.-led team wrote in the journal Nature Climate Change of satellite measurements of rising temperatures over the past 40 years.

They said confidence that human activities were raising the heat at the Earth's surface had reached a "five-sigma" level, a statistical gauge meaning there is only a one-in-a-million chance that the signal would appear if there was no warming.

Such a "gold standard" was applied in 2012, for instance, to confirm the discovery of the Higgs boson subatomic particle, a basic building block of the universe.

Benjamin Santer, lead author of Monday's study at the Lawrence Livermore National Laboratory in California, said he hoped the findings would win over skeptics and spur action.

"The narrative out there that scientists don't know the cause of climate change is wrong," he told Reuters. "We do."

Mainstream scientists say the burning of fossil fuels is causing more floods, droughts, heat waves and rising sea levels.

U.S. President Donald Trump has often cast doubt on global warming and plans to pull out of the 197-nation Paris climate agreement which seeks to end the fossil fuel era this century by shifting to cleaner energies such as wind and solar power.

Sixty-two percent of Americans polled in 2018 believed that climate change has a human cause, up from 47 percent in 2013, according to the Yale Program on Climate Change Communication.

Satellite data

Monday's findings, by researchers in the United States, Canada and Scotland, said evidence for global warming reached the five-sigma level by 2005 in two of three sets of satellite data widely used by researchers, and in 2016 in the third.

Professor John Christy, of the University of Alabama in Huntsville which runs the third set of data, said there were still many gaps in understanding climate change. His data show a slower pace of warming than the other two sets.

"You may see a certain fingerprint that indicates human influence, but that the actual intensity of the influence is minor (as our satellite data indicate)," he told Reuters.

Separately in 2013, the United Nations' Intergovernmental Panel on Climate Change (IPCC) concluded that it is "extremely likely", or at least 95 percent probable, that human activities have been the main cause of climate change since the 1950s.

Peter Stott of the British Met Office, who was among the scientists drawing that conclusion and was not involved in Monday's study, said he would favor raising the probability one notch to "virtually certain", or 99-100 percent.

"The alternative explanation of natural factors dominating has got even less likely," he told Reuters.

The last four years have been the hottest since records began in the 19th century.

The IPCC will next publish a formal assessment of the probabilities in 2021.

"I would be reluctant to raise to 99-100 percent, but there is no doubt there is more evidence of change in the global signals over a wider suite of ocean indices and atmospheric indices," said Professor Nathan Bindoff, a climate scientist at the University of Tasmania.