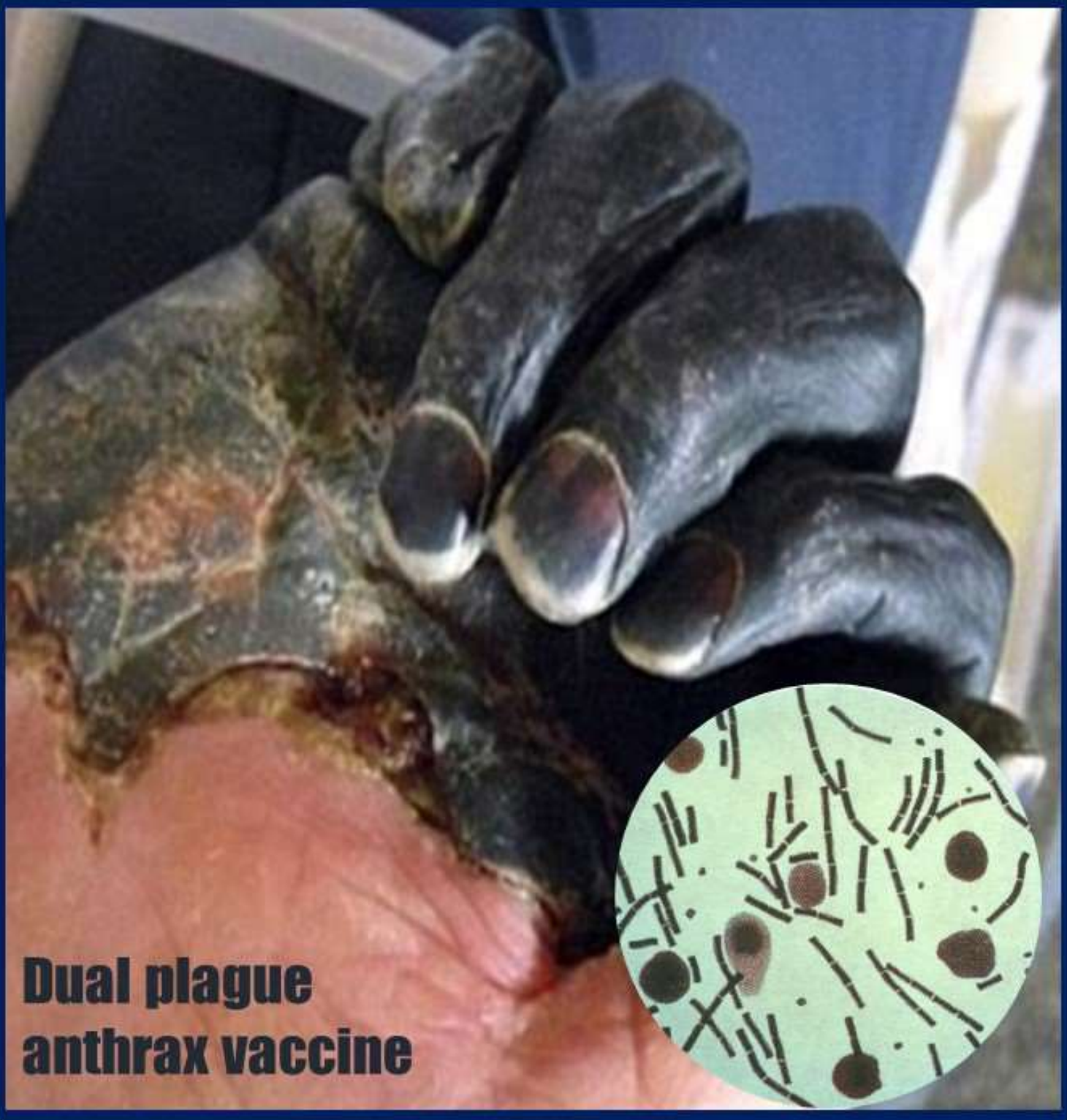
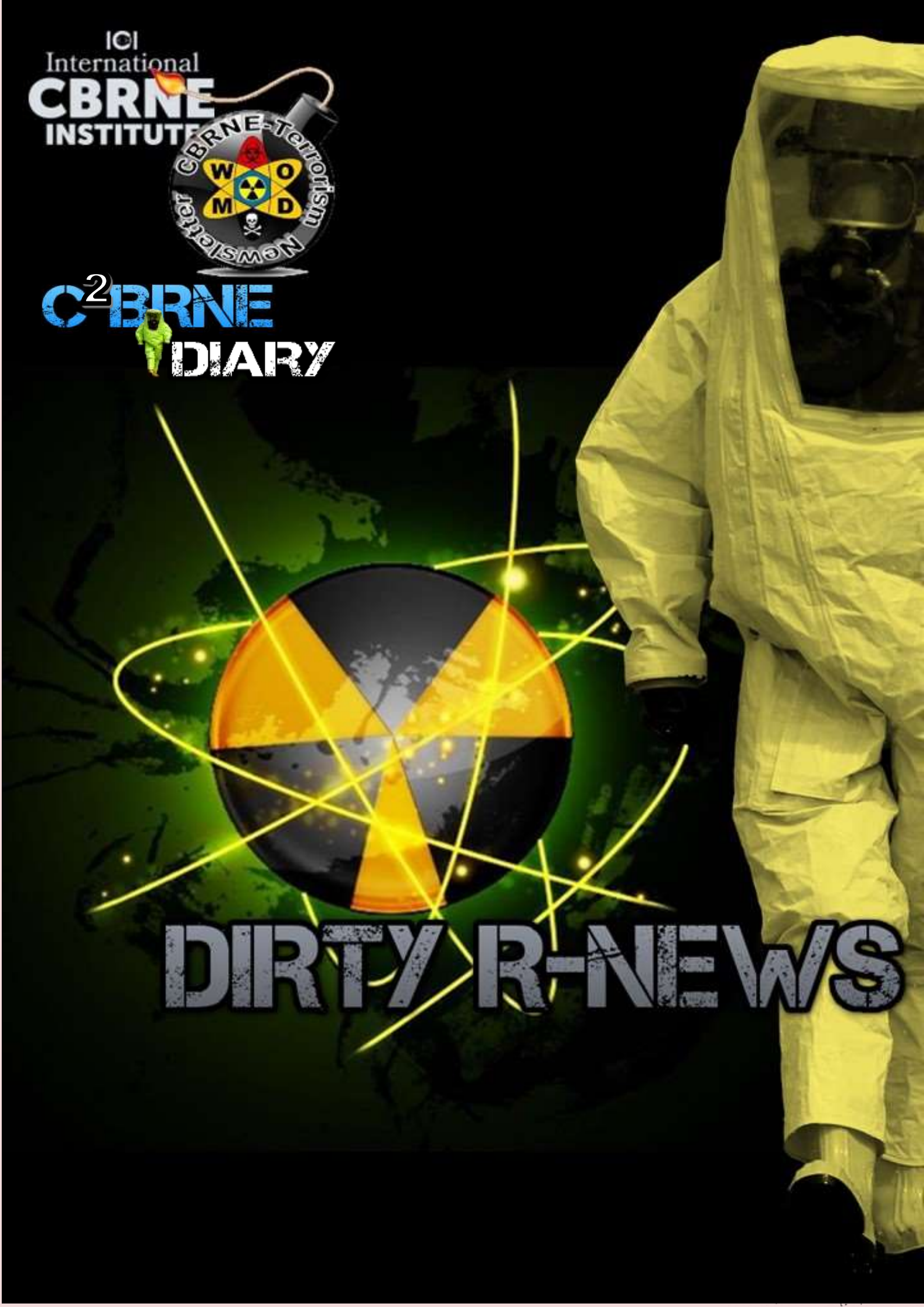
2 CBRNE DIARY

Dedicated to Global First Responders

October 2018



www.cbrne-terrorism-newsletter.com


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

Explosion, collapse, earthquakes: North Korea's 2017 nuclear test

Source: http://www.homelandsecuritynewswire.com/dr20180928-explosion-collapse-earthquakes-north-korea-s-2017-nuclear-test

Sept 28 – The epicenter of the 3 September 2017 nuclear test explosion in North Korea occurred about 3.6 kilometers northwest of the country's first nuclear test in October 2006, according to a new high-precision analysis of the explosion and its aftermath.

The study published in *Seismological Research Letters* by Lian-Feng Zhao of the Chinese Academy of Sciences and colleagues used regional seismic data collected from a number of sources to locate the 2017 test, and to confirm that subsequent seismic events were not also nuclear explosions.

Their paper is published as part of the journal's special focus section on the September 2017 North Korean explosion. The body-wave magnitude 6.1 underground test by the Democratic People's Republic of Korea (DPRK) is the largest such test in more than 20 years, and is the sixth declared nuclear test by the DPRK since 2006. The September explosion is an order of magnitude larger than the next largest test by the country, which occurred in September 2016.

SSA says that Zhao and colleagues used seismic wave data from 255 seismograph stations in the China National Digital Seismic Network, Global Seismic Network, International Federation of Digital Seismograph Networks and Full Range Seismograph Network in Japan to investigate the explosion and three other seismic events that occurred in the minutes and days after.

Punggye-ri nuclear test site, DPRK. / USGS Earthquake Hazard Program

Although global seismic networks may pick up the signal of underground nuclear tests, the signals they detect are often too weak to be to be used in the kind of location analysis performed by Zhao and colleagues. "The closer to the sources the better," said Zhao. "However, seismometers cannot be deployed in the North Korean test site due to political issues. Thus, seismologists have developed methods that can be applied to regional seismic data to investigate seismic characteristics of the underground nuclear explosions."

The researchers used seismic data from the first DPRK nuclear test as the "master event" to calibrate their location analysis, since the epicenter of that small explosion could be visually located using satellite images of localized ground surface damage. The much larger September 2017 explosion produced surface damage over an area about nine square kilometers, however, in ground that was already disturbed by previous nuclear tests. "For

example, after the sixth North Korean nuclear test, large displacements occurred on the west and south flank [of the test site] and debris flows were localized in pre-existing channels," Zhao explained. "These spatially distributing phenomena made it difficult for us to directly determine the epicenter of the explosion."

Zhao and colleagues used regional seismic data instead to calculate that the epicenter of the September 2017 explosion was at 41.3018°N and 129.0696°E. A seismic event that took place about eight minutes after the explosion occurred very close to the explosion epicenter—less than 200 meters away—and probably represents the seismic signature of the collapse of a cavity left by the underground explosion, the researchers suggested.

Two subsequent seismic events, one on 23 September and one on 12 October, were located about eight kilometers northeast of the nuclear test site. Zhao and colleagues said that the seismic signatures of these two events indicate that they are not explosions, but may have resulted from mechanisms such as landslide or ground collapse. They may also be very shallow natural earthquakes that were triggered by the explosion, they noted, a possibility that will require more research on the pre- and post-explosion stresses on the faults where the events occurred.

Careful analysis of data collected after the 3 September 2017 North Korean declared nuclear test explosion has allowed seismologists to distinguish the separate seismic signatures of the explosion, the collapse of the explosion cavity and even several small earthquakes that occurred after the collapse.

The data, compared with those collected from 20th-century Nevada nuclear test sites, can help refine seismologists' methods of identifying nuclear test explosions around the world, write William R. Walter and his colleagues at Lawrence Livermore National Laboratory in the SRL focus section.

The researchers used a method that compares the ratio between regional P- and S-wave amplitudes to distinguish the seismic signature of an explosion compared to an earthquake, at distances about 200 to 1500 kilometers away from the seismic wave source. (P-waves compress rock in the same direction as the seismic wave's movement, while S-waves move rock perpendicular to the direction of the wave.) "In the P/S ratio discriminant we use to identify explosions, it is the lack of S-waves at high frequency that is distinctive of the explosions," Walter explained.

Walter and colleagues showed that the ratio could separate the six North Korean declared nuclear tests from natural earthquakes in the region, and that the same method could be used to successfully distinguish between historic Nevada Test Site nuclear explosions and earthquakes in the western United States.

However, there was another unusual seismic event, occurring about eight and half minutes after the explosion, which also drew the attention of the seismologists. Models of seismic waveforms of the event led the scientists to conclude that the event may have been the ground collapsing around an underground cavity left by the explosion.

Although collapses similar to this were sometimes seen after Nevada Test Site explosions, "this is the first time, to my knowledge, that we have remotely observed seismic waves from a collapse with modern instrumentation at a foreign test site," said Walter. "It is important to be able to determine this collapse was not another nuclear test."

Several features of the post-explosion event's waveforms mark it as a collapse rather than an explosion, the researchers say, including the relative lack of high frequency energy compared to explosion waveforms.

"Identifying the event as a collapse is another indicator the 3 September 2017 event was a nuclear test that generated a large vaporization cavity that collapsed eight and half minutes later," said Walter. "But we want to continue to develop methods to identify collapses to distinguish them from both explosions and earthquakes."

Researchers studying the September 2017 nuclear test data also noted two smaller seismic events occurring after the explosion, of magnitudes 2.6 and 3.4, that appear from the P- to S-wave ratios to be small earthquakes located four to eight kilometers north of the explosion site.

"We had not remotely observed any aftershocks from the prior DPRK declared nuclear tests, so the earthquakes following the explosion got people's attention," Walter said. "Again, we wanted to determine they were not additional smaller nuclear tests. Alternatively, we wanted to determine they were not associated with the collapse event." Upon careful re-analysis of the continuous data the researchers found a number of additional small earthquakes, including some that occurred before the 3 September 2017 declared nuclear test.

Given the timing these earthquakes do not appear to be true "aftershocks" of the nuclear test, Walter and colleagues concluded, though they may be related and possibly induced by the explosion. "The fact that apparent tectonic earthquakes are occurring near the DPRK test site reveals information about the state of [seismic] stress in the region, which may help us better understand the explosion seismic signatures," said Walter.

— Read more in Xi He et al., "High-Precision Relocation and Event Discrimination for the 3 September 2017 Underground Nuclear Explosion and Subsequent Seismic Events at the North Korean Test Site," Seismological Research Letters (2018).

Israel accuses Iran of having "secret atomic warehouse" near Tehran

Source: http://www.homelandsecuritynewswire.com/dr20180928-israel-accuses-iran-of-having-secret-atomic-warehouse-near-tehran

Sept 28 – Israeli Prime Minister Benjamin Netanyahu has accused Iran of having a secret atomic warehouse near Tehran in a UN speech that was dismissed as false by Iranian officials.

Addressing the United Nations General Assembly on 27 September, Netanyahu displayed an aerial photograph of the Iranian capital with a red arrow pointing to what he said was an undisclosed warehouse holding nuclear-related material.

He contended that the discovery shows Iran is still seeking to develop nuclear weapons, despite its 2015 agreement with world powers to curb its nuclear program in exchange for the lifting of global economic sanctions.

Netanyahu claimed the site near a rug-cleaning plant in the Turquzabad district contained as much as 300 kilograms of radioactive material, some of which has been moved recently. He called on the UN atomic agency to inspect the location immediately with Geiger counters — a demand echoed later on 27 September by the U.S. State Department.

Iranian officials dismissed the allegations.

"The world will only laugh loudly at this type of false, meaningless, and unnecessary speech and false shows," Iranian Foreign Ministry spokesman Bahram Qassemi was quoted as saying by Iran's Fars news agency.

Iranian Foreign Minister Mohammad Javad Zarif said that there should be more scrutiny of Israel's nuclear program.

"No arts & craft show will ever obfuscate that Israel is the only regime in our region with a 'secret' and 'undeclared' nuclear weapons program — including an 'actual atomic arsenal.' Time for Israel to fess up and open its illegal nuclear weapons program to international inspectors," Zarif said on Twitter.

"Farcical Claims"

The spokesman of Iran's Foreign Ministry, Bahram Ghasemi, said Netanyahu's accusation was "not worth talking about."

"These farcical claims and the show by the prime minister of the occupying regime [Israel)] were not unexpected," Ghasemi said on 28 September.

Iran's deputy foreign minister, Abbas Araghchi, mocked Netanyahu, saying the Israeli leader must have been badly advised by some people.

Netanyahu did not identify the material he claimed was in the warehouse nor did he specifically say that Iran had violated the nuclear deal.

The Israeli leader regards Iran as the biggest enemy of the Jewish state and has previously made allegations about Tehran's nuclear activities that are difficult to verify.

In 2012 in a speech to the UN assembly, Netanyahu held up a cartoon drawing of a bomb to dramatize his claim that Tehran was producing a nuclear bomb at the time.

In April, Netanyahu touted what he said was evidence of a large secret archive of documents related to Iran's clandestine nuclear weapons program at a different site in Tehran.

He said Israeli agents removed vast amounts of documents from that site. At the time, Iran said the documents were fake.

In his latest UN speech, Netanyahu claimed Iran had begun moving items out of the alleged secret warehouse and spreading them around Tehran to hide the evidence.

He said the warehouse still contains some 15 shipping containers full of nuclear-related equipment and materials, however.

Under the nuclear deal, the UN's atomic watchdog agency has the authority to inspect any site that allegedly houses nuclear materials.

But the International Atomic Agency has repeatedly said its inspections have found Iran was abiding by the restrictions in the deal. It did not immediately comment on Netanyahu's latest allegations.

While the United States withdrew from the deal in May, France, Britain, Germany, China, and Russia have continued to honor the agreement and have been seeking to provide legal procedures and protections so their businesses can continue to operate in Iran despite U.S. sanctions.

That drew harsh criticism from Netanyahu, who accused Europe of "appeasing Iran."

"Instead of coddling Iran's dictators," other countries should support the sanctions, he said to applause.

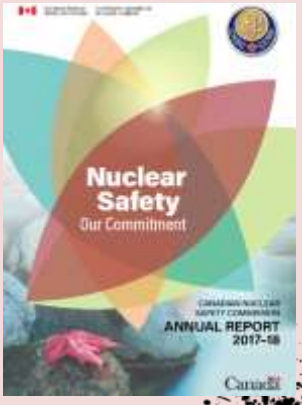
A U.S. official, speaking on condition of anonymity, told Reuters that the United States is aware of the facility Netanyahu mentioned and described it as a "warehouse" used to store "records and archives" from Iran's nuclear program.

Under the terms of the deal, Iran is allowed to keep documents and other research, but the deal puts strict limits on nuclear equipment and materials such as enriched uranium which can be used to make bombs.

The Israeli leader also lambasted Iran's ballistic missile activity, identifying three locations near Beirut airport where he claimed Iran's ally, the Lebanese Hizballah militia, is developing precision missiles that could be used to hit Israel.

Canadian Nuclear Safety Commission 2017–18 Annual Report

Source: http://www.nuclearsafety.gc.ca/eng/resources/publications/reports/annual-reports/ar2017-2018/index.cfm



On October 5, 2018, the Honourable Amarjeet Sohi, Minister of Natural Resources, tabled the Canadian Nuclear Safety Commission 2017–18 Annual Report in Parliament.

The report highlights many of the CNSC's accomplishments over the last fiscal year. It is a great reflection of the CNSC's commitment to safety as its first priority at every level and in every regulatory decision it makes.

This year's report includes detailed information about how the CNSC has:

- provided regulatory oversight for major nuclear and uranium mining facilities in Canada; this oversight activity included several licence renewals

- continued environmental assessments of Canadian Nuclear Laboratories' proposed major projects
- continued its growing work in vendor design reviews for new reactor concepts from vendors who have expressed an interest in obtaining feedback on how their designs are addressing Canadian regulatory requirements

In all its work to ensure the effective regulatory oversight of Canada's nuclear industry, CNSC staff are, and will continue to be, fully committed to safety first!

Strategy for protecting and preparing the Homeland against threats of electromagnetic pulse and geomagnetic disturbances

Source: https://www.dhs.gov/sites/default/files/publications/18_1009_EMP_GMD_Strategy-Non-Embargoed.pdf

Oct 11 – DHS earlier this week announced the release of the Strategy for Protecting and Preparing the Homeland against Threats from Electromagnetic Pulse (EMP) and Geomagnetic Disturbance (GMD).
The new strategy outlines an approach for DHS to take to protect critical infrastructure and prepare to cope with, respond to, and recover from potentially catastrophic electromagnetic pulse incidents. The strategy reflects the consensus assessment of the intelligence community about the threat EMP posed by adversaries of the United States.
Electromagnetic incidents, caused by either an intentional EMP attack or naturally occurring GMD events, are unlikely, but they could cause serious damage to the U.S critical infrastructure, including the electrical grid, communications equipment, financial services, and transportation capabilities.
The new DHS strategy primarily focuses on DHS activities, but it recognizes the importance of close collaboration with federal, state, and local decision-makers, sector-specific agencies, and private sector critical infrastructure owner-operators. DHS says that this partnership is essential to help critical infrastructure owners and operators to manage EMP and GMD risk.
DHS is currently developing an accompanying Implementation Plan, which will include measures that enable DHS to evaluate progress toward addressing identified capability gaps. Together, the strategy and its companion Implementation Plan will improve DHS's management oversight and optimize resource utilization for a national EMP/GMD protection, response, and recovery activities.
DHS says it intends to review and update the EMP/GMD strategy, as needed, and regularly assess the department's progress on the Implementation Plan

Blast tube tests at Sandia simulate shock wave conditions nuclear weapons could face

Source: http://www.homelandsecuritynewswire.com/dr20181011-blast-tube-tests-at-sandia-simulate-shock-wave-conditions-nuclear-weapons-could-face

Oct 11 – You can learn a lot from a blast tube. You can learn more when you couple blast experiments with computer modeling.
Sandia National Laboratories researchers are using a blast tube configurable to 120 feet to demonstrate how well nuclear weapons could survive the shock wave of a blast from an enemy weapon and to help validate the modeling.
Sandia recently completed a two-year series of blast tube tests for one nuclear weapon program and started tests for another. Each series requires instrumentation, explosives, high-speed cameras and computer modeling.
Tests simulate part of the environment a weapon re-entering the Earth's atmosphere would face if another nuclear weapon went off nearby, said test director Nathan Glenn.
Each series starts with calibration shots that allow team members to verify blast wave parameters and at the same time validate the computer model. The team hangs an explosive

charge at one end of the 6-foot diameter tube and places pressure transducers along its length. Transducers sense the strength of the blast pressure moving through the tube — higher pressure closer to the charge, falling off farther away.

Modeler Greg Tipton, who helped design the series, said tests validate the computer models of the structural dynamics of the system. "We can then use the models to simulate real environments we can't actually test to," he said.

Figuring out how to conduct testing

It's complex just to analyze how to conduct a test, Tipton said. The pressure drives how big a charge is needed and how the test article is positioned in the tube, and that determines the loading, or the amount of force applied to the test unit. In turn, the loading determines the structural response of the test article. "So, the team does end-to-end calculations to simulate the explosive going off, the shock wave through the tube, the shock propagation over the test unit and then the structural response to the shock wave. All of that data is used to determine the right orientation, the right shock level, to validate the models," Tipton said.

Sandia says that one software program simulates the explosive going off and the shock wave moving through the tube. A second calculates the shock moving over the test unit. A third computes the unit's response to shock and vibration. The fourth simulates how the unit will fly from the tube so the team can estimate where it's going, how fast it's moving and how they're going to catch it safely. Each software package has the dual purpose of computing the response of the system to validate the models and of helping design the test, Tipton said.

Software that simulates the explosive going off, for example, helps determine the size of the charge. "They do a number of shots in the tube to calibrate that. You know a charge weight and a pressure at some target location," he said. "As you up the charge weight, you're going to up the pressure, and if you do a handful of those tests and a whole bunch of simulations to fill in the blanks, you establish a calibration curve that tells you how much explosive you need to achieve a target pressure."

Wil Holzmann, who helps analyze test data, said more than a hundred channels of data might be collected on pressures, strains and acceleration responses. Analysts process experimental data using embedded information and use identical signal processing methods to the experimental and analysis data and compare responses to assess the credibility of the model.

"The objective is to develop validated analytic models for predicting responses to blast loads with a high degree of confidence," Holzmann said. Researchers can use the validated model to help qualify a weapon to withstand harsh conditions, such as a nuclear blast, that cannot be directly simulated with ground-level blast tube tests.

Planning takes much longer than test itself

Instrumentation is critical. Tests that last mere milliseconds require months of planning. "Communication and technical excellence is crucial to success," and there's only one chance at getting data from the extreme environment of a blast, said John Griffin of Measurement

Science and Engineering. "Simplicity in the design, protection of the hardware, redundancy of critical elements and thorough verification of connections are key to ensuring that we get the data in that one opportunity."
Over the past three years, Sandia developed a new mobile instrumentation unit, a large-data acquisition system designed to self-check the accuracy and "health" of connections before and after testing.
A hardened trailer encloses the system so it can be placed near a blast test. The system can store up to 16 million samples per channel and record about 1 gigabyte per second at the maximum sample rate, Griffin said. For comparison, he said, this equates to more than 70 hours of digital music or about 1,100 songs.
Glenn said it's more of an art than a science to measure pressure pulses. "If you don't have it set up right and mounted right, the data is worthless," he said. "There are racks and racks of instrumentation with wires coming at you. It makes your head dizzy just looking at it."

Specialty high-speed imaging employed
High-speed imaging that measures pressure changes also helps assess a shock wave's impact. In the past, researchers used streak cameras that viewed images through a quarter-inch by 6-inch slit. Streak cameras are similar to document scanners, imaging a column of pixels and generating an image by the object moving rapidly past the scan.
Now, a photographic technique called synthetic schlieren, implemented for harsh environments by optical engineer Anthony Tanbakuchi, enables a much larger view. Synthetic schlieren detects changes in optical index induced by changes in pressure, temperature and density. The schlieren effect is comparable to seeing ripples from heat on a road. Regular schlieren (a German word that means streak in the singular) techniques require large optics, special lighting and other complex, sensitive optical configurations that aren't practical for large-scale tests, Tanbakuchi said. Synthetic schlieren doesn't require any special setup other than an optional background and has no size limit because it looks for subpixel shifts in the background to detect optical index changes.
The team combines synthetic imaging algorithms with image stabilization codes Tanbakuchi developed to image a blast wave front. Sandia's 50-year history of extreme testing means it has a huge code base to solve these problems.
Synthetic schlieren can be used for everything from pressure to temperature imaging. "But the most value comes when we also combine it with the data fusion techniques we've developed so you can see the pressure wave fronts with instrumentation data and model data," Tanbakuchi said. "That's when the full picture really emerges."

France sued for "crimes against humanity" South Pacific nuclear tests

Source: http://www.homelandsecuritynewswire.com/dr20181011-france-sued-for-crimes-against-humanity-south-pacific-nuclear-tests

Oct 11 – French Polynesia is taking France to the International Criminal Court (ICC) for carrying out nuclear weapons tests in French Polynesia, a Polynesian opposition leader said on Tuesday.
Oscar Temaru, the archipelago's former president and now leader of the Tavini Huiraatira Party, announced the move during a United Nations committee dealing with decolonization.
Temaru accused France of "crimes against humanity" and said that he hopes to hold French presidents accountable for the nuclear tests with the ICC complaint.
"We owe it to all the people who died from the consequences of nuclear colonialism," he told the UN committee.

Maxime Chan from Te Ora Naho, an association for the protection of the environment in French Polynesia, told the UN that there had been 368 instances of radioactive fallout from the tests and that radioactive waste had also been discharged into the ocean — violating international rules.
DW reports that the former French territory, currently home to 290,000 people, is home to the popular tourist island of Tahiti, but its atolls of Mururoa and Fangataufa were used for decades for nuclear tests.
France carried out 193 nuclear weapons tests on islands in the archipelago between 1960 and 1996 until French President Jacques Chirac ended nuclear testing.
Around 150,000 military and civilian personnel were involved in France's nuclear tests, with thousands of them later developing serious health problems.
France has denied responsibility for the detrimental health and environmental impacts of the tests, fearing that it would weaken the country's nuclear program during the Cold War.
In 2010, France passed a law allowing military veterans and civilians to be compensated if their cancer could be attributed to the nuclear tests – which France conducted not only in the Pacific, but also in the Sahara Desert in southern Algiria.
Out of about 1,000 veterans who have filed complaints against France, only 20 have been deemed eligible for compensation.

Japan is poised to FLOOD the Pacific with one million tons of radioactive water contaminated by the Fukushima nuclear plant

Source: https://www.dailymail.co.uk/sciencetech/article-5753411/Japan-poised-flood-Pacific-one-million-tons-radioactive-water-Fukushima.html

Aug 2018 – Japan is poised to flood the Pacific Ocean with one million tons of radioactive water contaminated by the Fukushima nuclear plant.
Storage space at the abandoned facility is running dangerously low as officials race to secure the nearly 160 tons of contaminated water produced at the plant per day.
As space for tanks dwindles the Japanese government and the plant's owner Tokyo Electric Power Company (Tepco) may decide to dump treated water into the ocean.
Tepco plans to secure 1.37 million tons of storage capacity by the end of 2020, but it has not yet decided on a plan for after 2021.
At a Fukushima committee meeting on Friday, Akira Ono, chief decommissioning officer of Tepco, said: 'It is impossible to continue to store [treated water] forever.'

At the safety meeting an expert committee set up by the industry ministry discussed dumping the contaminated waste into the Pacific.

Japan News reports that one committee member said: 'While the fishery industry [in Fukushima and other prefectures] is in the process of revival, should we dispose of [the treated water] now?

Another said: 'In order to advance the decommissioning, the number of tanks should be decreased at an early date.'

The number of storage tanks for contaminated water and other materials has steadily risen at the Fukushima plant on Japan's east coast.

Meltdowns following a 10-metre-high (33ft) tsunami in the region in 2011 released harmful radioactive fuel rods and debris from contained areas.

Groundwater continues to enter the leaking reactor buildings, producing around 160 tons of radioactive water per day that must be collected and safely stored.

While most contaminants can be removed through purification devices, tritium - a radioactive isotope of hydrogen - cannot be removed for technical reasons.

As the amount of treated or 'tritium' water continues to rise officials have struggled to come to an agreement on what should be done with the waste.

Storage tanks at Fukushima currently have a capacity of around 1.13 million tons, with about 80 per cent - 1.13 million tons - of space designated for treated water.

Space for tanks has been expanded by clearing forest and debris, leaving around 230,000 square metres (2.4 million sq ft) of space, but there is now almost none left.

Tritium is found in tap water and exists naturally in sea beds and rivers.

The isotope is produced as part of normal operations at nuclear plants and is often diluted and released into the ocean or elsewhere as part of waste management.

Currently the Tritium water produced at Fukushima is ten times the national standard for ocean dumping of treated waste.

Further dilutions to the stored water could make it suitable for ocean deposits.

Other ideas discussed during Friday's meeting include release by evaporation, release following electrolysis treatment and burial ungerground.

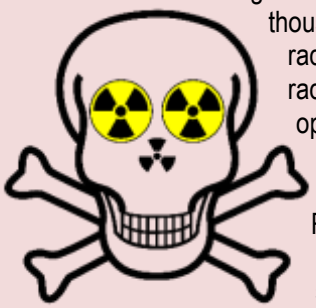
The meeting was the committee's seventh since it was set up 18 months ago, but the group is yet to reach a conclusion on what to do with the treated water.

Members plan to hold public meetings to gather citizens' views on the matter later this year.

Sheltering Against the Ultimate - A Nuclear Detonation in a U.S. City

By Kirk Paradise

Source: https://www.domesticpreparedness.com/healthcare/sheltering-against-the-ultimate-a-nuclear-detonation-in-a-u.s-city/



August 2007 – Should terrorists detonate a nuclear weapon in a major city, tens, perhaps hundreds, of thousands of people might die from the direct effects of heat, blast, and the initial nuclear radiation. Beyond Ground Zero, thousands of others could be at risk of death from *fallout* radiation. In the chaotic aftermath of such an event, in fact, there would be only two survival options for those not killed immediately: get out of town as quickly as possible, or take shelter – but it is unlikely that all could flee. For those in the fallout area, it is imperative that action must be taken almost immediately – within a matter of minutes, preferably.

Regardless of how much (or how little) time is available, taking shelter from fallout radiation is essential; fortunately, such action is known to be extremely effective in preventing injury, specifically including long-term debilitating illness, from radiation. But, to be effective, fallout shelters must be prepared beforehand and, of equal if not greater importance, shelter management teams must be created, and trained.

Fallout lofted into the atmosphere may reach as high as 30,000 feet, and could be carried off in two or three directions, at different strata and at different speeds. Moreover, exposure rates – where twice the median lethal dose may be received in just a single hour – may extend over several hundred square miles within a few hours. Intense radiation could cover a thousand square miles within 24 hours. The lethal exposure of literally hundreds of thousands of people, perhaps a million or more, is possible in the East or West Coast urban corridors of the United States.

Invisible Assets Are Already in Place

Fortunately, and surprisingly as well, in these same areas and within easy driving (and/or walking, in downtown areas) distances are large numbers of fallout shelters, previously built, which range in size from a 50-person capacity upward. Many if not most are government buildings – schools and courthouses, for example – but a fairly high percentage are owned by private-sector businesses or agencies, or by individual citizens. These so-called "relics of the Cold War" still exist in almost every county in the country, in fact, and in most if not all areas of the country their protective capabilities remain intact. Although not currently part of the DHS (Department of Homeland Security) strategy to protect people, they could be revitalized in short order and be used to attenuate radiation intensity.

To test this hypothesis, Huntsville, Alabama, started a revitalization of its fallout shelter program in 2005 under a Metropolitan Medical Response System grant provided by the Department of Homeland Security (DHS). Using a list of fallout shelters compiled by FEMA (the Federal Emergency Management Agency) several years ago, a number of shelters providing the best protection were selected, in 2005 and 2006, by the Huntsville-Madison County Emergency Management Agency for further evaluation. Using such criteria as building capacity and the quality of protection that could be provided, as expressed by a numeric "Protection Factor" scale developed by FEMA, then contacted the owners of a number of the buildings evaluated and asked them if the buildings could be further evaluated for use as public fallout shelters. Over 100 owners agreed; only about 10 declined.

Most of the owners also agreed to send representatives to participate in a fallout-shelter management course. This was a significant step forward, because successful sheltering is more than just bricks and concrete. It means taking frightened people – rudely gathered together under the worst of circumstances and confronted by fears of the unknown – and organizing them into teams capable of group survival. In that context, the shelter is just a tool; the main task of the shelter manager is to gain psychological control of people, reassure them of the shelter's protective qualities, and organize them into self-help teams.

Following the Huntsville Example

To accomplish that important goal, a fallout shelter management course and a fallout shelter managers' guide were developed by the Huntsville-Madison County EMA. The course informs people about the dangers of fallout radiation and explains how shelters protect

people, and how to organize and direct people to survive. In January 2007, 78 persons completed the eight-hour course. Four sessions were held in Huntsville under the auspices of the Huntsville-Madison County EMA.
Thirty new shelters were added to the list in 2006 to accommodate areas of Madison County where the population has grown significantly in recent years. A civil engineer from the University of Alabama in Huntsville, using FEMA methods developed in the 1970s,entified the protective space that could be used in buildings not available when the original inventory of fallout shelters was developed.
Other cities and counties can revitalize their own fallout-shelter programs – and would be well advised to do so. The lists of fallout shelters, last published by FEMA in 1992, still exist and are available on request to state and local authorities. Those other cities and counties can follow the same process used in Huntsville: identify potential shelters; obtain signed agreements from the current owners of the shelters; recruit shelter managers and shelter management teams, and train them; and make fallout shelter management courses available to the general public as well.

Links for additional information:
The Fallout Shelter Managers' Guide, the Fallout Shelter Management Course as Micro Soft Power Point slides, and related information http://www.madisoncountyema.com/Fallout.html
Nuclear Detonations
https://www.fema.gov/media-library-data/20130726-1549-20490-0802/terrorism.pdf
Particularly recommended is the section titled "Before a Nuclear Blast"
https://www.usfa.fema.gov/data/library/research/topics/top_civil_defense.html
Sheltering and Evacuation
https://www.ready.gov/nuclear-explosion

Kirk Paradise *serves as the emergency plans coordinator for the Huntsville-Madison County, Alabama, Emergency Management Agency. His primary task is to track all of the plans and procedures the agency is involved with and to ensure they are updated and distributed to the using agencies. He also is the county radiological officer and shelter officer, and assists in training as a radiological monitor instructor. He has worked for the agency since 1979 and has prior experience as a disaster preparedness officer in the U.S. Air Force. His education and training includes a Bachelor's degree from Virginia Polytechnic Institute and a Master of Science degree from University of Alabama Huntsville plus numerous training courses conducted by the Federal Emergency Management Agency.*


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

IEDs and the First Responder

By Glen Rudner

Source: https://www.domesticpreparedness.com/preparedness/ieds-and-the-first-responder/

Oct 08 – Today's first responder has had to adapt to an ever-changing threat that affects all U.S. citizens. The individual responder himself has to some extent become a human "tool box" that must be able to operate in many different venues. From apprehending a criminal to fighting a fire, to transporting sick or injured victims, first responders today must be able to carry out a multitude of tasks – at times, more or less simultaneously.

Many if not all of those tasks are inherently dangerous in themselves, and they may become much more dangerous within the foreseeable future. As American troops in Iraq have found out, there is an invisible enemy that, without warning, has already killed or wounded literally thousands of U.S. military personnel. That enemy is the improvised explosive device, better known as an IED.

IED bombings are one of the most challenging types of terrorist attack to prevent. Terrorist groups reap several advantages from such attacks, which require relatively little in material resources and training, provide flexibility in both timing and targeting, and, as proven, have a high rate of success. In addition, al Qaeda and other terrorist groups have become rather adept at adjusting their tactics to defeat new defenses against IEDs. There already have been several under-publicized incidents in the United States itself involving IEDs – but those attacks have caused only minimal damage so far. However, the psychological impact is starting to show, and a growing number of experts in the fields of terrorism and counterterrorism predict that more, and more destructive, IED attacks on U.S. soil may be just over the horizon. Whether that prediction becomes a reality or not, it seems clear that the nation's response community must be much better prepared than it now is to protect their communities and fellow citizen from such attacks.

Needed: Clear Thinking, and Decisive Action

Because of the inherent complexity of an IED attack, the individual responder is faced with the need to make several decisions – immediately in many cases, and sometimes simultaneously. The most complex decision involves the identification of potential hazards, a complex task that involves, among other factors, the recognition and assessment of various "indicators" that may (or may not) provide helpful clues that indicate the possible presence of an IED. Among those indicators are the receipt of a written or oral threat and the presence of unidentified and/or seemingly non-threatening packages. The responder also must be aware of unidentified people in a potential target area who seem out of place, and ensure that the appropriate law-enforcement agencies have been notified.

When arriving at the scene of a potential IED attack, responders should first establish a staging area at a safe distance from the reported address. They also should keep a close and continuing surveillance of the surrounding area, noting potential points of both egress and access, and keeping a particularly close lookout for suspicious-looking packages as well as people. They also must set up a protective perimeter to protect themselves as well as others in the area.

If in fact one or more strong indicators is found – e.g., an unidentified package or suspicious-looking device – the responders' exit strategy is simple: They should stop whatever else they are doing, mark the area clearly, and retreat to a safe distance until trained EOD (explosive ordnance disposal) personnel have arrived and are ready to take over. EOD personnel are better trained today than ever before, fortunately, to handle suspicious packages.

To summarize: The IED threat is already causing increased concern to the nation's first-responder community, and for good reason. When emergency commanders receive a call for assistance, they should gather as much information as possible before sending a response unit to the scene of a suspected IED. In addition, first-responder agencies and emergency-management officials should already be carefully reviewing their plans for responding to suspicious incidents, and should ensure that those plans include the eventuality of an IED incident. These same agencies need to train *all* of their personnel, not just the response units, but anyone who may become involved in any way with an IED incident. In short,

not only the federal government but the individual states and cities must move much more quickly to prepare and plan to cope with what could become a wave of IED incidents before such incidents take place on a scale that today can only be imagined in a worst-case scenario.

__Glen D. Rudner__ is the Hazardous Materials Response Officer for the Virginia Department of Emergency Management; he has been assigned to the Northern Virginia Region for the last nine years. During the past 25 years he has been closely involved in the development, management, and delivery of numerous local, state, federal, and international programs in his areas of expertise for several organizations and public agencies.

Autonomous IED Detection System to Save Soldiers' Lives

Source: https://i-hls.com/archives/85937

Oct 08 – Israel Aerospace Industries (IAI) has completed the development of an autonomous improvised explosive device detection (IED's) system that will eliminate risk to human teams. The system is a robotic engineering scout, installed on a robotic platform made by IAI, and integrates a combination of multiple sensors, for detecting improvised explosive devices. The system is detecting IEDs placed and hidden in complex areas, engage and remove them as necessary using the blade installed on the vehicle. The system operation, maneuver and detection are done autonomously without danger to human life. The system is scheduled to be transferred for trial and evaluation purposes.

The system is part of the SAHAR family, which includes a number of platforms that have explosive detection device and route clearing capabilities. Each system is adapted to customer needs, and includes the robotic platform, the control system and the relevant detection payloads. The system is based on IAI's robotic kit, enabling faster, more efficient execution of missions and safe operation of the system without risk to human life. The system may operate in any terrain and has a precision operation system that generates a real image of the arena. The system combines a number of payloads of different types for detection of explosive devices on and under the surface and engineering capabilities for neutralizing them, according to the company's announcement.

Meir Shabtai, General Manager, Robotic Systems Division: "The completion of the development of the autonomous IED's detection system of the SAHAR family and its delivery to operational trails is another significant quantum leap in the field of unmanned vehicles. Israel Aerospace Industries is operating intensively and is adapting its products to the future battlefield needs. The SAHAR system integrates and uses the advanced technologies in the terms of detection sensors capabilities, and Autonomous Navigation."

First of Its Kind App Developed for IDF Training Base in the Israeli Negev

Source: https://i-hls.com/archives/85899

Oct 10 – The IDF's training camp in the Negev, "Ir Habahadim" (the "City of Training Bases"), is known for its magnitude and innovation. The wide array of services and activities in the IDF's first smart city, as well as the large number of soldiers active in it, necessitate a means for the soldiers to attain quick accessibility of current and precise information.

The "Pocket Notepad" app, recently developed in the training campus and won the Personnel Management Head Officer's Shield award for development of an innovative solution for the soldier, provides every official in the training campus access to vital information.

Ever since its launch in April 2017, 55,000 downloads of the app have been recorded, with an average of 2,000-2,500 downloads each month.

In an interview to i-HLS, Major Chaim Chana, Head of Information Systems in the IDF Teleprocessing Corps, presented the unique app, which centers around the average soldier. The app is tailored to a unique target audience – trainees and new recruits in the training base.

The idea for the development of the app arose with the completion of soldier transfers to the Negev campus, when the need for a means of updating the arriving soldiers and providing them access to the relevant information and services peaked.

The app covers all information vital for the incoming soldier from the moment of arrival – from emergency

numbers and emergency buttons to the infirmary and operations room, through soldiers rights, classroom locator, food and catering, health services (Medical Corps service center, pharmacy, experts clinic, lab services etc.), options for approaching commanders, details on the commercial center (prices, sales, opening hours), transportation (including special lines and rides, frequency), hairdressing services, laundry etc. (all including relevant contacts and the option of setting appointments), Women's Affairs advisor (contacts for requests), personal affairs and rabbinate, lost and found and even convictions through the digital enlisted person ID, push notifications and updates.

The app is available for both Android and iOS for every soldier in the IDF, as well as interested citizens.

Advanced search options enable finding information related to any field in an intuitive manner.

The app offers navigation within the camp – arriving at a classroom in a certain building is done through the building's specific number, operating via Waze and Google Maps.

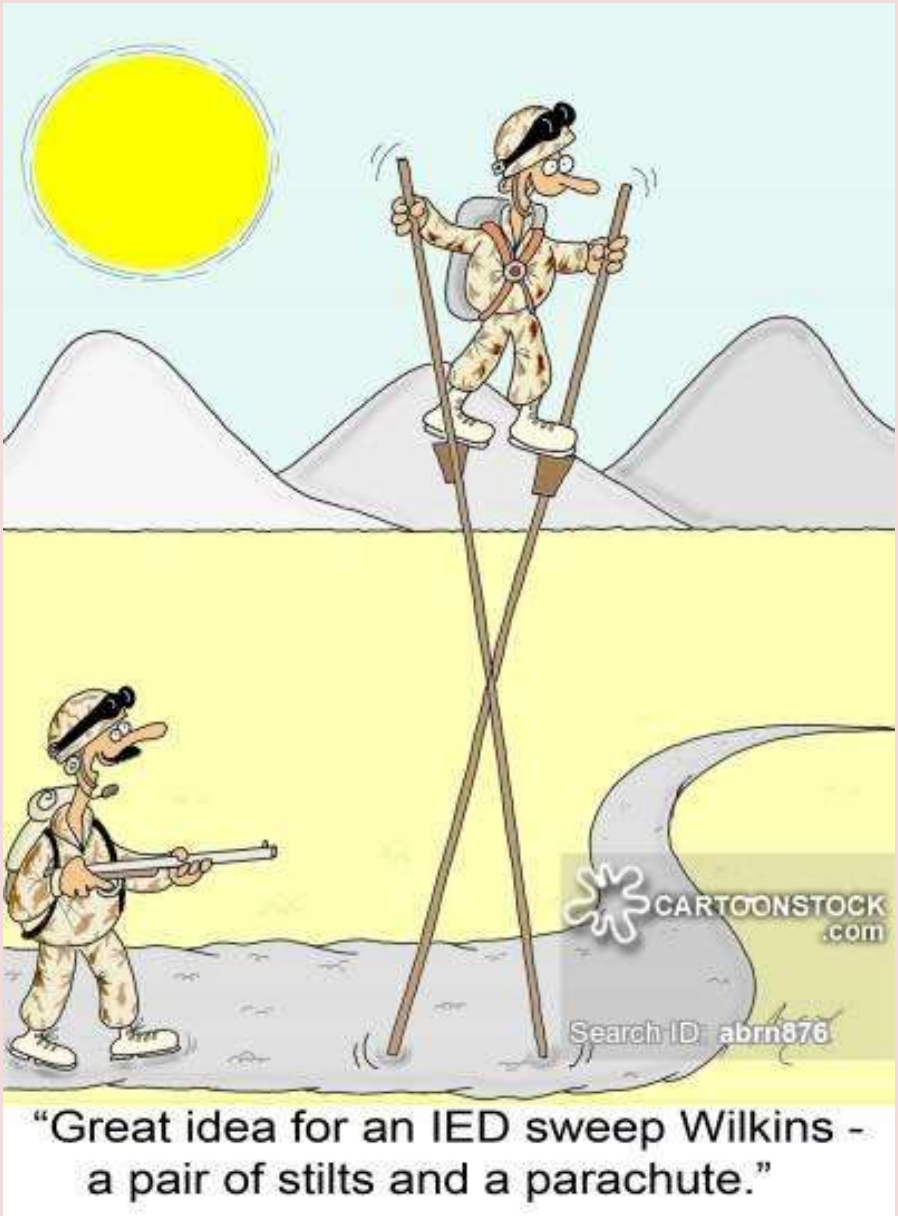
How does the app work? according to Major Chana, the development of the app was based on survey questionnaires that were distributed among the soldiers in order to better understand their needs, as well as research into existing apps aimed at enhancing commercial accessibility of information in college and university campuses. The app was developed by soldiers in their regular service.

A daily update is registered at the center, regarding the phone numbers of every soldier scheduled to arrive at the camp. The center sends every soldier a link to download the app.

Information regarding transportation, food etc., automatically flows to the center and updates. At the same time, initiated requests are made to the different authorities for the purpose of monthly updates. The app's content, additionally, goes through quality control.

Every six months, the app's version is improved based on feedback from soldiers and statistics regarding usage of the different features. The version currently in use is the third one.

The app is approved according to information security standards, although it includes no classified information nor is it implemented operationally.
The developers of the app are currently working on additional applications for the smart city in the realms of security, building maintenance and more.
According to the head of the Training and Doctrine branch at the Personnel Management Corps, Lieutenant Colonel Yair Levi, "the Personnel Management Head Officer's Shield award is awarded to projects in the different units, that focus on demonstrating initiatives, innovation and creativity in the entire handling of personnel management with an emphasis on enhancing expertise and providing a learning culture.
In an era in which the challenge of maintaining quality personnel in the permanent service is increasingly complex, alongside the challenge of the technological development – the award encourages creative thinking and productive action among the personnel, and for those who participate we must show appreciation."



ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C²BRNE DIARY

CYBER NEWS

Chemical weapons watchdog says target of growing cyber activities

Source: https://www.i24news.tv/en/news/international/europe/185593-181004-dutch-expel-four-russians-over-operation-targeting-chemical-weapons-watchdog

Oct 04 – Dutch intelligence thwarted a Russian cyber attack targeting the global chemical weapons watchdog in April and expelled four Russian agents, the government said Thursday.
The Russians set up a car full of electronic equipment in the car park of a hotel next to the Organisation for the Prohibition for Chemical Weapons in The Hague in a bid to hack into its computer system, it said.
"The OPCW takes very seriously the security of its information systems and networks. Since early 2018, the Organization has observed increased cyber-related activities," the watchdog group said in a statement following a press conference from the defense minister.

A man tries on an air permeable charcoal impregnated suit during a simulation at the OPCW (The Organisation for the Prohibition of Chemical Weapons) headquarters in The Hague – JOHN THYS (AFP/File)

As the implementing body for the Chemical Weapons Convention, the OPCW, with its 193 Member States, oversees the global endeavour to permanently eliminate chemical weapons. Since the Convention's entry into force in 1997, it is the most successful disarmament treaty eliminating an entire class of weapons of mass destruction.
Over 96% of all chemical weapon stockpiles declared by possessor States have been destroyed under OPCW verification.
For its extensive efforts in eliminating chemical weapons, the OPCW received the 2013 Nobel Peace Prize.
"The Dutch government finds the involvement of these intelligence operatives extremely worrisome," Dutch Defense Minister Ank Bijleveld told a news conference.
"Normally we don't reveal this type of counter-intelligence operation."
The Netherlands publicly identified the alleged Russian agents and said the operation was carried out by Russia's GRU military intelligence agency, Dutch officials said.
Britain helped the Netherlands with the operation, they added.

A laptop belonging to one of the four was linked to Brazil, Switzerland and Malaysia. The activities in Malaysia were related to the investigation into the 2014 shooting down of flight MH17 over Ukraine, Bijleveld added.

At the time of the attack the OPCW was investigating the nerve agent poisoning of former Russian spy Sergei Skripal and his daughter in Salisbury, England. Dutch officials said it was not clear if the cyber operation was linked to that.

The head of the Dutch MIVD intelligence service, Major-General Onno Eichelsheim, told the news conference that the men travelled to Amsterdam's Schiphol Airport on April 4 on Russian diplomatic passports.

An official from the Russian embassy escorted them to The Hague, he said.

On April 11 they then hired a Citroen C3 and scouted the area around the OPCW -- all the time being watched by Dutch intelligence.

"They were trying to commit a close access hack operation," he said.

'Clearly not on holiday'

The Russians set up in the Marriott Hotel next door to the OPCW and took photos, while parking the car at the hotel with the boot facing the OPCW, he said.

In the boot was electronic equipment to intercept the OPCW's WiFfi as will as log in codes at the organisation, with the antenna hidden in the back of the car facing the OPCW.

"We intercepted it and expelled the four men from the country. It was a successful operation."

The Dutch spy chief said the Russians had originally taken a taxi from a GRU base in Moscow to the airport, and some of their mobile phones were activated in Moscow near the agency's headquarters.

When leaving The Hague, the men took all the rubbish from their room in a further bid to cover their tracks.

"They were clearly not here on holiday," said Eichelsheim.

News of the Dutch operation came a day after Britain and Australia blamed the GRU for some of the biggest cyber attacks of recent years -- including one on the Democratic National Committee during the 2016 US presidential campaign.

They said the Russian military intelligence service could have only been conducting operations of such scale on Kremlin orders.

Russian President Vladimir Putin has repeatedly and angrily rejected similar charges. He told US President Donald Trump during a July summit in Helsinki that talk of Russia meddling in the 2016 election was "nonsense".

Five Leading Airport Security Technologies by 2030

Source: https://i-hls.com/archives/85794

Oct 07 – The protection of passengers, staff, and aircraft in the airport and its vicinities from crime, terror and other threats has always been on high priority of law enforcement and government agencies worldwide. Technological innovation supplies new approaches to this challenging task.

As reported by passengerterminaltoday.com, over the next decade, all areas of airport security will be impacted equally by technological advancements: screening, communications, surveillance, command and control, access control, cybersecurity and perimeter security.

According to Diogenis Papiomytis, global program director, commercial aviation, aerospace, defense and security in Frost & Sullivan, the technologies with the most substantial impact on airport security by 2030 will be:

Artificial Intelligence

Airports are procuring IT solutions with embedded AI, aiming to predict performance and potential operational disruptions. AI is also a key element of intelligent video analytics and automation of passenger screening processes. AI-enabled risk-based screening will eventually replace risk-based screening by observational techniques (SPOT) employed by security agencies worldwide but championed by the TSA.

Biometrics

Biometrics technology, now primarily used for border control, has numerous applications across the passenger journey. First and foremost it is an enabler for tunnel screening, which will eventually replace the security touchpoint. As airports and airlines invest in digitization of all passenger touchpoints and implement self-service systems (check-in, bag drop, security, boarding), biometrics will become the preferred technology for identity management.

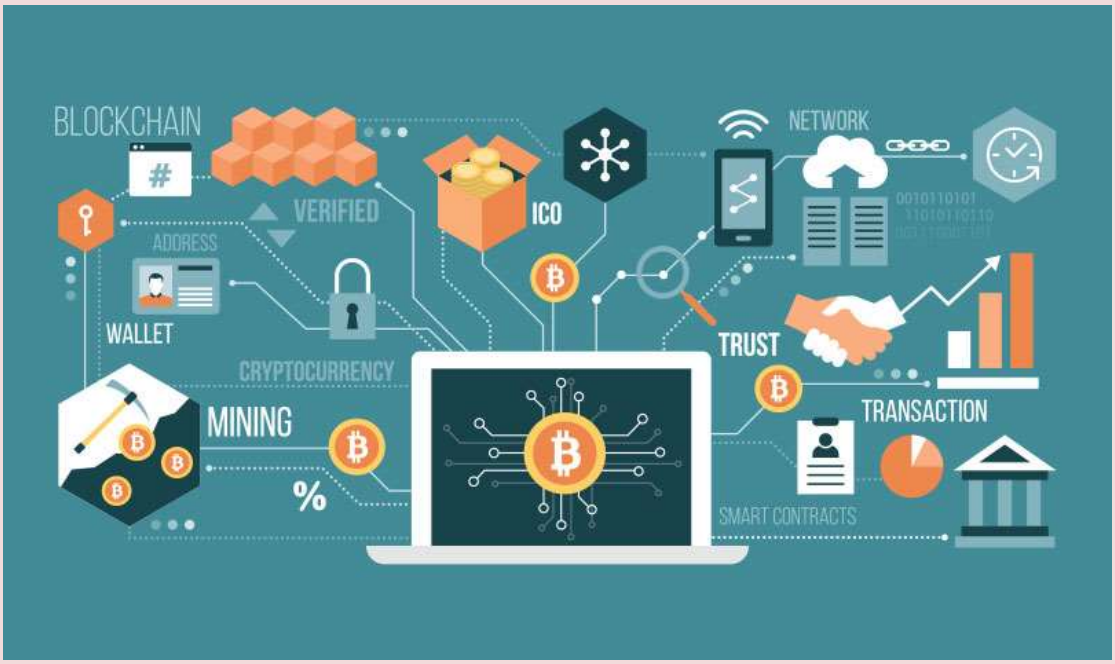
Biometric data, when linked with boarding pass data, is of immense value to airport operators. These data sets will allow a transformation of airport business models, as airports learn more about passengers and can develop personalized products and services.

Cybersecurity

With increased digitization, sensorization and cloud use, airports become targets for cyber criminals. Almost all airport IT suppliers are investing in their cybersecurity capabilities.

Blockchain

Blockchain, a technology that links records using cryptography (secured communication), has been already tried in airline and airport operations. Perhaps the most important application of blockchain is in



storing passenger biometric data and enabling seamless passenger journeys. In the airport environment, the technology holds immense potential in enabling collaboration projects and real-time data sharing among airport stakeholders.

Sensorization and data analytics

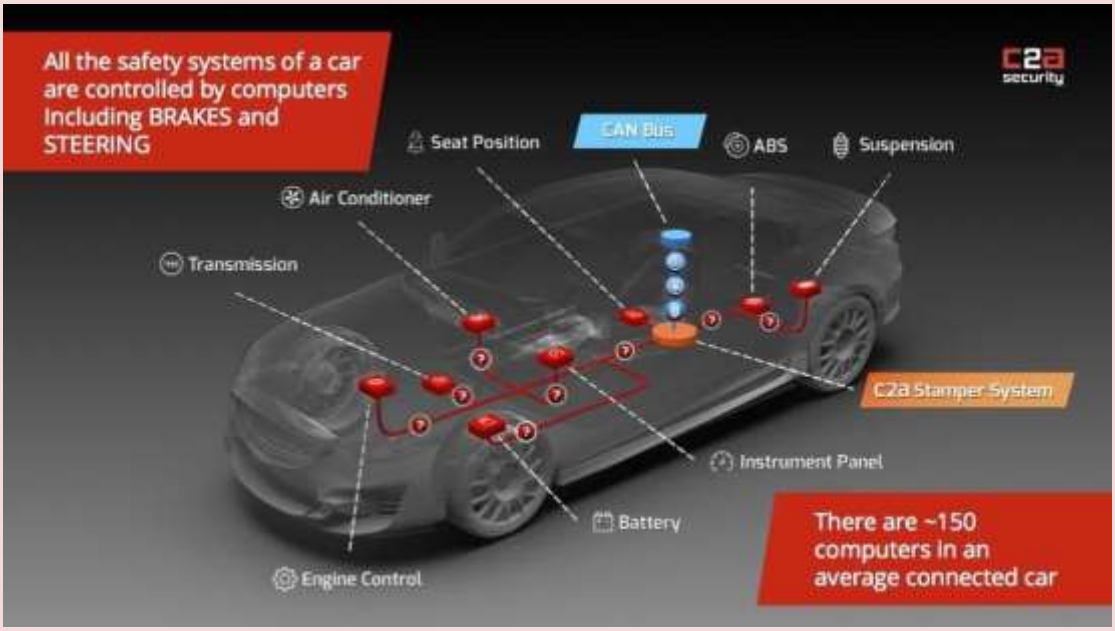
Passenger screening is expanding beyond the security checkpoint and will take place across the terminal (and beyond, linking to the Safe City vision). The goal is to enable a decentralized security model, with sensors performing analysis of numerous data sets over the passenger journey.

Mitigating cyberthreats in vehicles

Source: http://www.homelandsecuritynewswire.com/dr20181012-mitigating-cyberthreats-in-vehicles

Oct 12 – In acts of terrorism, vehicles have been deployed as killing machines. These incidents involved human operators, but another sinister possibility looms: a vehicle cyber hack intended to cause human harm. While this kind of terrorist attack has not yet occurred, in the realm of security research, it's been demonstrated how hackers could gain control over car systems like the brakes, steering and engine.

Using machine learning techniques, American University Computer Science Professor Nathalie Japkowicz and her co-authors, Adrian Taylor of Defence R&D Canada and Sylvain Leblanc of the Royal Military College of Canada, designed a way to **detect unusual activity in a car's computer system**. **Unusual activity could signal a cyberattack, so the findings have implications for the search for tools to respond to cybersecurity threats in vehicles.**



"We are catching abnormal activity on the network which needs to be analyzed further. We just know that it is different from usual and may lead to a dangerous situation," said Japkowicz. At AU, where it concerns cybersecurity research, the current focus of the computer science department is on "vulnerability management," or detecting attacks during normal system operations. Computer science research into cybersecurity threats and vehicles plays an important role in informing how the automotive industry and national governments will address cyberattacks.

American notes that car computer network systems have many vulnerabilities. They are made up of many small, linked computer units, (or electronic control units) that communicate with each other. Newer car models can be hacked through wireless and cellular connections. Even USB and iPod ports provide access points for a potential hack. Newer vehicles, especially, are vulnerable because they are constantly connected to the internet.

A cyberattack will disrupt the normal patterns of a car. Japkowicz and her co-authors' focused on detecting anomalies on the computer network system and the point at which a car, having been hacked, is made to do things differently from what it's programmed to do. For example, a change in a message in the computer network system from "steer right" to "steer left," Japkowicz explains.

To detect unusual activity, the researchers experimented with **two machine learning techniques**, called **Long Short-Term Memory and Gated Recurrent Units**, to learn normal data patterns in a car, Japkowicz explains. In particular, they used that technology to analyze network data on a 2012 Subaru Impreza for vehicle traffic and driving in various conditions.

Both techniques involved a "neural network" trained on normal traffic patterns so that it could recognize anomalies. A neural network is an important part of machine learning. Neural networks are computer algorithms built on data inputs. Neural networks proceed in a way analogous to how humans learn through neural processes. Japkowicz explains how an

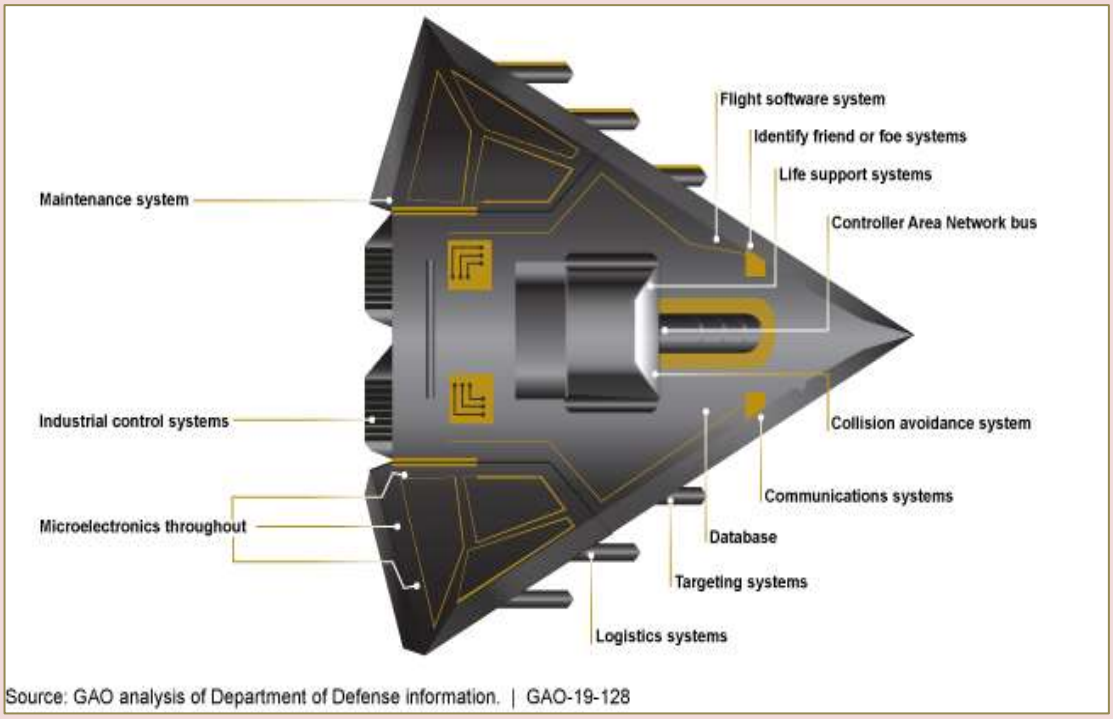
artificial neural network works: information gets transmitted from artificial neuron to artificial neuron through highly parallel connections that get stronger and stronger as similar patterns are observed.
The researchers created an attack framework that allowed them to test a wide range of cyberattacks representative of real ones. They did so by reviewing every example they could find of published cyberattacks in vehicles and integrating these examples and their generalizations into their framework. In doing so, not only did they create a robust framework within which to test their own work, but they believe that the research community involved in the same kind of research can also benefit from it, Japkowicz said.
Although cars are unique, the research findings should apply to other car models because cyberattacks on car models are similar, Japkowicz said. In the future, she will test the detection system in other cars and refine the technique, making the neural network smarter with more varied data inputs.
The research has published in a special issue on data mining and cybersecurity in *IEEE Intelligent Systems*.

GAO: Defense Dept. Just Beginning to Grapple with Scale of Weapon-Systems Cybersecurity Vulnerabilities

Source: https://www.hstoday.us/federal-pages/government-reports-and-summaries/gao-defense-dept-just-beginning-to-grapple-with-scale-of-weapon-systems-cybersecurity-vulnerabilities/

Oct 14 – The Defense Department plans to spend about $1.66 trillion to develop its current portfolio of major weapon systems. Potential adversaries have developed advanced cyber-espionage and cyber-attack capabilities that target DOD systems. Effectively protecting information and information systems can reduce the likelihood that attackers are able to access systems and limit the damage if they do.
The Government Accountability Office was asked to review the state of DOD weapon systems cybersecurity. Its report addresses factors that contribute to the current state of DOD weapon systems' cybersecurity, the vulnerabilities in weapons that are under development, and the steps DOD is taking to develop more cyber resilient weapon systems.
To undertake this work, GAO analyzed weapon systems cybersecurity test reports, policies, and guidance. GAO interviewed officials from key defense organizations with weapon systems cybersecurity responsibilities as well as program officials from a non-generalizable sample of nine major defense acquisition program offices.

DOD's weapons are more computerized and networked than ever before, unsurprisingly there are more opportunities for attacks. Yet until relatively recently, DOD did not make weapon cybersecurity a priority.



Source: GAO analysis of Department of Defense information. | GAO-19-128

Over the past few years, DOD has taken steps towards improvement, like updating policies and increasing testing.

The Department of Defense (DOD) faces mounting challenges in protecting its weapon systems from increasingly sophisticated cyber threats. As well as the aforementioned computerized nature of weapon systems, DOD's late start in prioritizing weapon systems cybersecurity and DOD's nascent understanding of how to develop more secure weapon systems has presented a precarious situation. DOD weapon systems are more software dependent and more networked than ever before. Systems that could potentially fall foul to cyber attacks include targeting systems, friend or foe identification systems, flight software, communications, and microelectronics used throughout the weapon system.

GAO has warned of the cyber risks for decades, but until recently, the agency said, DOD did not prioritize weapon systems cybersecurity. In fact, DOD is still determining how best to address weapon systems cybersecurity.

GAO found that in operational testing, DOD routinely detected mission-critical cyber vulnerabilities in systems that were under development, yet program officials GAO met with believed their systems were secure and discounted some test results as unrealistic. Using relatively simple tools and techniques, testers were able to take control of systems and largely operate undetected, due in part to basic issues such as poor password management and unencrypted communications. In addition, GAO says the vulnerabilities that DOD is aware of likely represent a fraction of total vulnerabilities due to testing limitations. For example, not all programs have been tested and tests do not reflect the full range of threats.

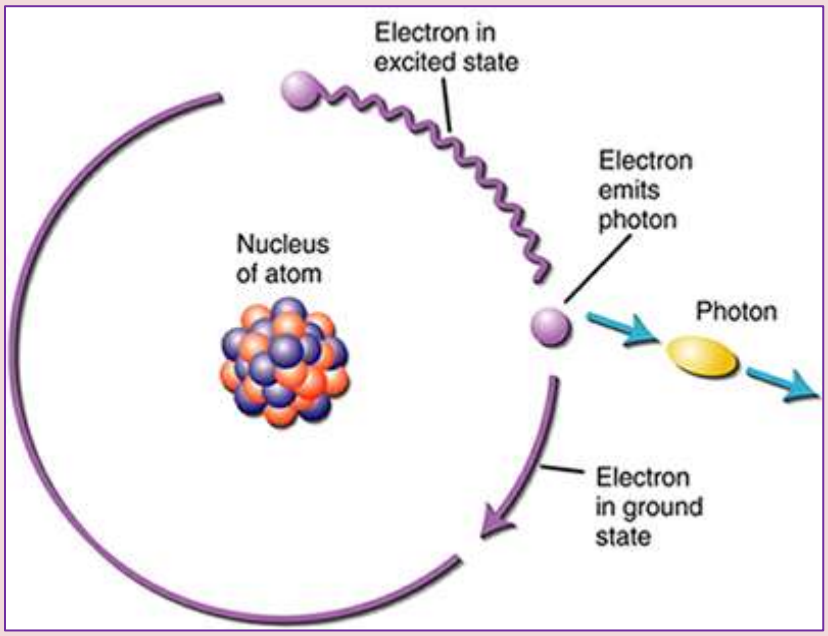
DOD has however recently taken several steps to improve weapon systems cybersecurity, including issuing and revising policies and guidance to better incorporate cybersecurity considerations. DOD, as directed by Congress, has also begun initiatives to better understand and address cyber vulnerabilities. However, DOD faces barriers that could limit the effectiveness of these steps, such as cybersecurity workforce challenges and difficulties sharing information and lessons about vulnerabilities. To address these challenges and improve the state of weapon systems cybersecurity, GAO says it is essential that DOD sustain its momentum in developing and implementing key initiatives. GAO plans to continue evaluating key aspects of DOD's weapon systems cybersecurity efforts.

Read the full report

Unhackable communication: Single particles of light could bring the "quantum internet"

Source: http://www.homelandsecuritynewswire.com/dr20181019-unhackable-communication-single-particles-of-light-could-bring-the-quantum-internet

Oct 19 – Hacker attacks on everything from social media accounts to government files could be largely prevented by the advent of **quantum communication, which would use particles of light called "photons" to secure information rather than a crackable code.**



The problem is that quantum communication is currently limited by how much information single photons can help send securely, called a "secret bit rate." Purdue says that Purdue University researchers created a new technique that would increase the secret bit rate 100-fold, to over 35 million photons per second.

"Increasing the bit rate allows us to use single photons for sending not just a sentence a second, but rather a relatively large piece of information with extreme security, like a megabyte-sized file," said Simeon Bogdanov, a Purdue postdoctoral researcher in electrical and computer engineering.

Eventually, a high bit rate will enable an ultra-secure "quantum internet," a network of channels called "waveguides" that will transmit single photons between devices, chips, places or parties capable of processing quantum information.

"No matter how computationally advanced a hacker is, it would be basically impossible by the laws of physics to interfere with these quantum communication channels without being detected, since at the quantum level, light and matter are so sensitive to disturbances," Bogdanov said.

The work was first published in *Nano Letters*.

Using light to send information is a game of probability: Transmitting one bit of information can take multiple attempts. The more photons a light source can generate per second, the faster the rate of successful information transmission.

"A source might generate a lot of photons per second, but only a few of them may actually be used to transmit information, which strongly limits the speed of quantum communication," Bogdanov said.

For faster quantum communication, Purdue researchers modified the way in which a light pulse from a laser beam excites electrons in a man-made "defect," or local disturbance in a crystal lattice, and then how this defect emits one photon at a time.

The researchers sped up these processes by creating a new light source that includes a tiny diamond only 10 nanometers big, sandwiched between a silver cube and silver film. Within the nanodiamond, they identified a single defect, resulting from one atom of carbon being replaced by nitrogen and a vacancy left by a missing adjacent carbon atom.

The nitrogen and the missing atom together formed a so-called "nitrogen-vacancy center" in a diamond with electrons orbiting around it.

A metallic antenna coupled to this defect facilitated the interaction of photons with the orbiting electrons of the nitrogen-vacancy center, through hybrid light-matter particles called "plasmons." By the center absorbing and emitting one plasmon at a time, and the nanoantenna converting the plasmons into photons, the rate of generating photons for quantum communication became dramatically faster.

"We have demonstrated the brightest single-photon source at room temperature. Usually sources with comparable brightness only operate at very low temperatures, which is impractical for implementing on computer chips that we would use at room temperature,"

said Vlad Shalaev, the Bob and Anne Burnett Distinguished Professor of Electrical and Computer Engineering.
Next, the researchers will be adapting this system for on-chip circuitry. This would mean connecting the plasmonic antenna with waveguides so that photons could be routed to different parts of the chip rather than radiating in all directions.

— Read more in Simeon I. Bogdanov et al., "Ultrabright Room-Temperature Sub-Nanosecond Emission from Single Nitrogen-Vacancy Centers Coupled to Nanopatch Antennas," Nano Letters 18, no. 8 (3 July 2018).

Where Do Terrorists Go When They Are Kicked Off Social Media Platforms?

By Nikita Malik
Source: ttps://www.forbes.com/sites/mitsubishiheavyindustries/2018/10/18/industry-2050-how-clean-manufacturing-is-a-win-win-proposition/#4694bfed7f35

Oct 18 – A few weeks ago, I published a piece on the social media platforms exploited – by terrorists.
Using information released by the Crown Prosecution Service on terrorism in the United Kingdom in 2018, I found that people convicted for spreading hate from the Far Right tended to use only two platforms to do this – Twitter and Facebook. The majority of offenders (75%) disseminated material on Facebook.
Unlike the Far Right, Islamist related content was spread on a variety of platforms, indicating that perpetrators were getting better at hiding and spreading their messages. 33% used encryption – the process of encoding a message or information in such a way that only authorized parties can access it – to communicate.
Recently, I have expanded this search to include convictions from 2016, 2017, and 2018. Most of these offenders have used social media to prepare for terrorist attacks, collect and disseminate information, and encourage and support terrorism.
The question we need to ask ourselves, however, is what happens when technology companies identify these individuals, and ban them from continuing to use (and exploit) their platforms.
The first technique is to create a new account to continue to disseminate a terrorist message. As we know, a social media account is usually verified using a mobile phone number. In one court case in 2018, however, Rabar Mala – later sentenced to eight years in prison – would help re-open a messaging channel or account that had been blocked by the provider. To do this, he would obtain a SIM card and use it in one of his UK mobile phones, and send the third party (who was often based outside the UK) the mobile telephone number. The third party would then use this telephone number to open a social media or messaging account, as the content provider would text an activation code to the new mobile number given to the third party.
The second option for an individual banned from a social media platform is to use an alternative. These include private Telegram channels, live talks on Paltalk, and a social media platform called VK, or "VKontakte". The latter is the largest European online social networking service, based in Saint Petersburg and available in several languages, but most popular among Russian speaking users. VK is ranked globally, for all social networks, second only to Facebook and higher than Instagram or Twitter, due to the ease with which an account can be created.
However, how effective are these alternatives? Not very, given the demand that Rabar Mala faced. After all, in order for a messaging campaign to be consumed effectively, it requires an audience of followers, and a large and popular reach.
Take the example of Islamic State. Its 'media mujahideen', or online army of internet fans, would meticulously share and re-post official content across a number of social media platforms, as part of a coordinated effort to maximize the organisation's impact and relevance, and assist in recruitment. Given the largely inaccessible nature of encrypted channels like Telegram and Paltalk, it is perhaps unsurprising that mass recruitment rarely took place on these channels. Though terrorist propaganda is likely to exist in relative abundance on the Darknet and other encrypted platforms, proselytization and recruitment will continue on main platforms where a general audience can be found.

But even with these alternatives, the British government is becoming more effective in catching and prosecuting offenders. Recently, Shafi Mohammed Saleem was convicted of, and plead guilty to, encouraging terrorism online. Throughout 2016 and 2017, Saleem had used over 20 Twitter and Instagram accounts to share pro-Islamic State material. One of the tweets he posted was an image of 'zombie knives', which are illegal in the UK. Included in what Detectives recovered from Saleem's home was a photo saved on the Telegram app of Saleem holding a handgun, as well as videos of Islamic State propaganda and Osama bin Laden.
Commander Dean Haydon of the Met's Counter Terrorism Command noted how important it is to hold those who share subversive material accountable: "Every tweet has the potential to radicalize vulnerable people." As of February 2018, Saleem had been sentenced to two years in prison.

Nikita Malik *specialises in countering extremism, radicalisation and terrorism. She is currently the Director of the Centre on Radicalisation and Terrorism (CRT) at the Henry Jackson Society, where she serves as a research expert in countering violent extremism, terrorism, and hate-based violence. Her work has been regularly featured in the media, and my findings and policy recommendations have been discussed in the House of Commons, House of Lords, European Parliament, the US State Department, the United Nations, and other key government departments across the world.*

Biohackers Are Implanting Everything from Magnets to Sex Toys

Source: https://www.bloomberg.com/news/articles/2018-10-19/biohackers-are-implanting-everything-from-magnets-to-sex-toys

Oct 19 – Patrick Kramer sticks a needle into a customer's hand and injects a microchip the size of a grain of rice under the skin. "You're now a cyborg," he says after plastering a Band-Aid on the small wound between Guilherme Geronimo's thumb and index finger. The 34-year-old Brazilian plans to use the chip, similar to those implanted in millions of cats, dogs, and livestock, to unlock doors and store a digital business card.
Kramer is chief executive officer of Digiwell, a Hamburg startup in what aficionados call body hacking—digital technology inserted into people. Kramer says he's implanted about 2,000 such chips in the past 18 months, and he has three in his own hands: to open his office door, store medical data, and share his contact information. Digiwell is one of a handful of companies offering similar services, and biohacking advocates estimate there are about 100,000 cyborgs worldwide. "The question isn't 'Do you have a microchip?' " Kramer says. "It's more like, 'How many?' We've entered the mainstream."
Research house Gartner Inc. identified do-it-yourself biohacking as one of five technology trends—others include artificial intelligence and blockchain—with the potential to disrupt businesses. The human augmentation market, which includes implants as well as bionic limbs and fledgling computer-brain connections, will grow more than tenfold, to $2.3 billion, by 2025, as industries as diverse as health care, defense, sports, and manufacturing adopt such technologies, researcher OG Analysis predicts. "We're only at the beginning of this trend," says Oliver Bendel, a professor at the University of Applied Sciences & Arts Northwestern Switzerland who specializes in machine ethics.
A Spanish dancer named Moon Ribas has a chip in her arm connected to seismic sensors, which is triggered when there are tremors anywhere on the planet. She uses it in a performance art piece called *Waiting for Earthquakes*. Neil Harbisson, a colorblind artist from Northern Ireland, has an antennalike sensor in his head that lets him "hear" colors. And Rich Lee, from St. George, Utah, has spent about $15,000 developing a cyborg sex toy he calls the Lovetron 9000, a vibrating device to be implanted in the pelvis. Lee hasn't sold (or used) the Lovetron yet, but he's got magnetic implants in his fingertips to pick up metal objects, two microchips in his hands that can send messages to phones, and a biothermal sensor in his forearm to measure temperature. "We're the first movers," Lee says. "But as the technology becomes more mainstream, there will be potential uses for pretty much everybody."
Lee gave an address at BdyHax, a conference in Austin where people in the business can meet fellow cyborgs, discuss trends, and check out gadgets. At this year's conclave, speakers included the developer of an artificial pancreas, a representative of a group advocating tech connections to the brain, and a researcher from the U.S. Defense Advanced

Research Projects Agency—the developer of the internet—who's exploring biohacks to fight memory loss and improve the lives of people without limbs.

Kramer demonstrates how to unlock a door with a microchip-implanted hand. Photographer: Adam Berry/AFP/Getty Images

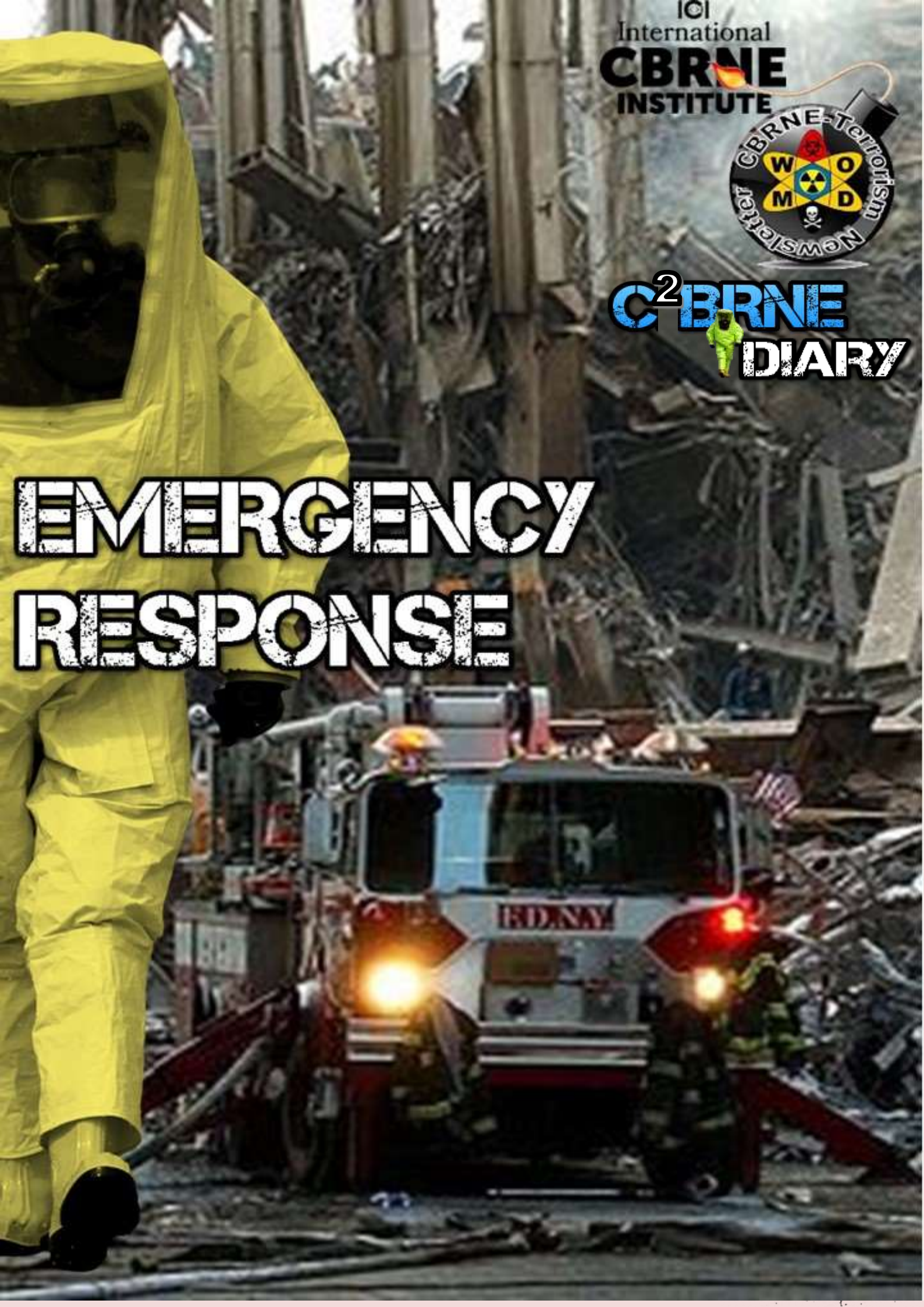
Biohacking raises a host of ethical issues, particularly about data protection and cybersecurity as virtually every tech gadget risks being hacked or manipulated. And implants can even become cyberweapons, with the potential to send malicious links to others. "You can switch off and put away an infected smartphone, but you can't do that with an implant," says Friedemann Ebelt, an activist with Digitalcourage, a German data privacy and internet rights group.

Those concerns haven't stopped some businesses from embracing biohacks. Tesla Inc. founder Elon Musk, who says people must become cyborgs to stay relevant, has raised at least $27 million for Neuralink Corp., a startup developing brain-computer interfaces. Neuralink is planning an announcement that's "better than probably anyone thinks is possible," the ever-self-promotional Musk said in a Sept. 7 video podcast where he was seen smoking marijuana. And last year, Three Square Market, a company in Wisconsin that makes self-service kiosks for office break rooms, asked its 200 employees if they'd be interested in getting chipped. More than 90 said yes, and they now use the implants to enter the building, unlock computers, and buy snacks from the company's vending machines.

Digiwell's microchip implants run from $40 to $250, and Kramer charges $30 to inject them, either in his Hamburg office or while traveling (he did Geronimo's implant in the lobby of a Berlin hotel). His clients include a lawyer who wants access to confidential files without remembering a password, a teen with no arms who uses a chip in her foot to open doors, and an elderly man with Parkinson's disease who once collapsed in front of his house after trying for two hours to get his key into the lock. He now uses a chip in his hand to open the door.

Kramer is also a co-founder of a company called VivoKey Technologies, which is developing a more advanced implant expected to be introduced next year. The device will be able to generate passwords for online transactions, and buyers can download software to upgrade it with more functions. "Humanity can't wait millions of years for evolution to improve their brains and bodies," Kramer says. "That's why we're doing it ourselves."

BOTTOM LINE - Biohacking advocates say 100,000 people have chips implanted under their skin, which they use to open doors, store passwords and personal data, and augment their art.

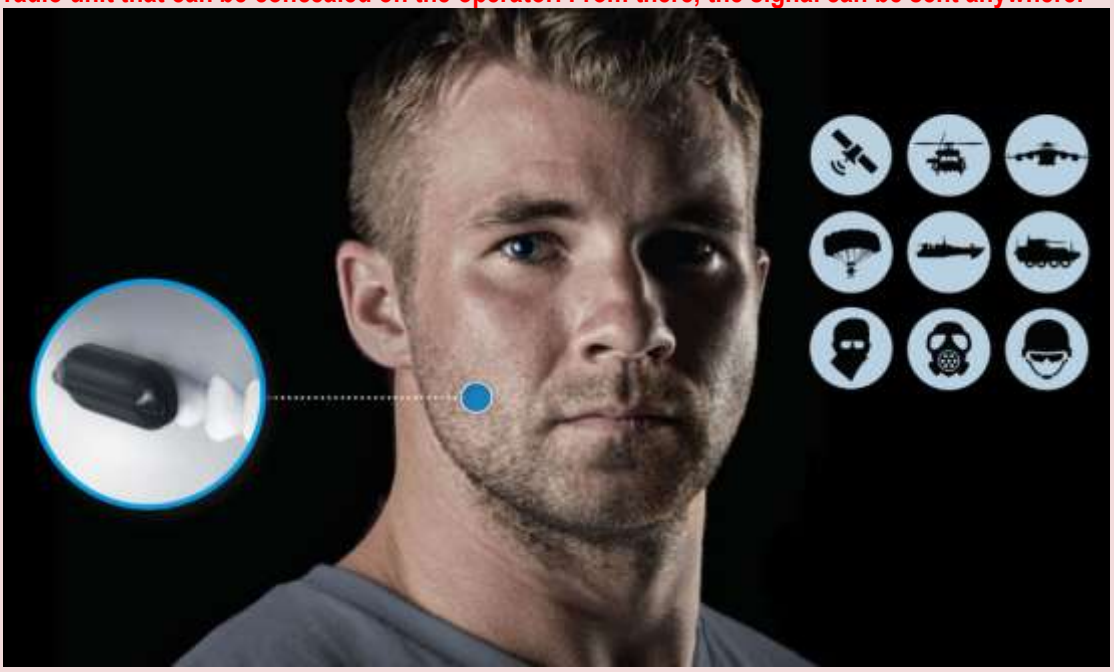

ICI
International
CBRNE
INSTITUTE
CBRNE-Terrorism Newsletter
W
O
M
D
C2BRNE
DIARY
EMERGENCY
RESPONSE

Unexpected Communication Channel for Search and Rescue

Source: https://i-hls.com/archives/85515

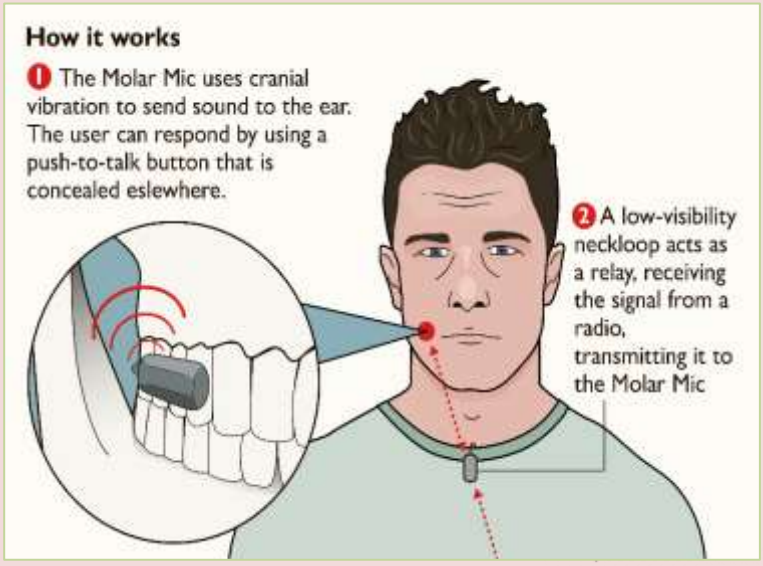
Sept 20 – First responders, soldiers, hazard material teams, etc. need hand-free communications equipment in order to be able to concentrate more on their missions. The development of a new secure communication gear that clips to your back teeth will be backed by the Pentagon. Dubbed the Molar Mic (a molar is a tooth at the back of the mouth), it's a small device which is both microphone and "speaker," allowing the wearer to transmit without any conspicuous external microphone and receive with no visible headset or earpiece.

Incoming sound is transmitted through the wearer's bone matter in the jaw and skull to the auditory nerves; outgoing sound is sent to a radio transmitter on the neck, and sent to another radio unit that can be concealed on the operator. From there, the signal can be sent anywhere.



The **Molar Mic** connects to its transmitter via near-field magnetic induction. It's similar to Bluetooth, encryptable, but more difficult to detect and able to pass through water.

"Essentially, what you are d oing is receiving the same type of auditory



information that you receive from your ear, except that you are using a new auditory pathway — through your tooth, through your cranial bones — to that auditory nerve," said Peter Hadrovic, CEO of Sonitus Technologies.

The ability to understand conversations transmitted through bone improves with practice. "Over the period of three weeks, your brain adapts and it enhances your ability to process the audio," said Hadrovic. But even "out of the gate, you can understand it," he said.

He declined to say whether CIA operatives had used the device in intelligence gathering. But the Molar Mic has seen the dust of Afghanistan and even played a role in rescue operations in the United States.

In Aug, 2016, the company was introduced to the Defense Innovation Unit Experimental, or DIUx (since rebranded simply DIU), and to pararescuemen who airdrop behind enemy lines to rescue downed aircrews. A few of the airmen took prototypes of the device on deployment to Afghanistan. Although they didn't use it during missions, they were able to test it repeatedly and offer feedback.

The Molar Mic was also tested during the rescue operations for Hurricane Harvey in the US. Hadrovic said the airmen were pleased with its performance during complicated operations involving water, helicopters, and a lot of external noise.

The same technology holds the potential for far more rich biometric communication between operators and their commanders, allowing soldiers in the field and their team to get a timely sense of how the soldier is responding to pressure or injury, without him or her having to communicate all of that explicitly. It's something that the military is working toward.

"As we look to the future human-machine interface… the human creates a lot of information, some of it intentional, some of it unintentional. Speaking is one form of information creation," says Hadrovic. "Once you've made something digital, the information can be interspersed…We have a tremendous wealth of opportunities to communicate out of the person and back to the person, information that can be either collected from them and processed offline and given back in a nice feedback loop. What we've done is invested in the platform that will support these future elements."

Evacuation decision-making: How people make choices in disasters

Source: http://www.homelandsecuritynewswire.com/dr20180927-evacuation-decisionmaking-how-people-make-choices-in-disasters

Sept 27 – After hurricanes Harvey and Irma, the National Science Foundation (NSF) funded research to investigate the broad impacts of these disasters. A year later, some of the researchers funded by awards from the agency's Social, Behavioral, and Economic Sciences Directorate are reporting results produced to date. This is the sixth article in the series. Roxane Cohen Silver, professor of psychological science, medicine, and public health at the University of California, Irvine studies the details of why people chose to evacuate or stay put as Hurricane Irma approached.

Stanley Dambroski writes:

> *We surveyed more than 1,600 Floridians in the 60 hours before Hurricane Irma made landfall in Florida, and again four to six weeks later. Having a sample that were surveyed both before an impending disaster and after its occurrence allowed us to answer important questions about who evacuates ahead of a hurricane, who doesn't, and why.*
>
> *Our initial analyses suggest that individual risk perception is the strongest predictor of who will evacuate before and during a hurricane. But it appears that some individuals' self-reports of their evacuation risk did not agree with what emergency response agencies decided were the highest risk areas. That is, preliminary analysis of perceived and actual evacuation orders suggests misinformation or misunderstanding by respondents in our sample.*
>
> *Based on preliminary analysis of post-hurricane responses, almost 50 percent of those who evacuated did not live in areas that received mandatory evacuation orders. In addition, fewer than one-third of individuals who were in a mandatory evacuation zone appeared to have evaluated this information accurately. Our analysis suggests that individuals' perceptions were based on the amount of media they consumed before the hurricane, past experiences of loss from a hurricane, and other personal factors not tied to the recommendations of emergency response agencies.*

In emergencies, targeted evacuations save lives. When people in evacuation zones stay put, they may place themselves and responders in danger. When people outside evacuation zones evacuate, there is a cost economically, and they may make evacuations more difficult for those in zones with the highest risk. Evacuation efforts and decision-making can be facilitated by coordinated risk communications from trusted sources (such as The National Weather Service, other government officials and broadcast meteorologists) who work together to ensure that appropriate messages are communicated, heard, and acted upon.

Our data illustrate how pre-hurricane factors predict post-hurricane responses and demonstrate how vulnerable populations of individuals who are at risk for exposure to future hurricanes are coping with these recurrent stressors.

EDITOR'S COMMENT: Decision for evacuation depends on the nature of the hazard. It is different when the threat is a wildfire or a progressing flooding despite the fact that both can become catastrophic. It is the perspective of the people not the threat itself that defines their decision to go. A second factor is the presence of pets or domestic animals. Many would prefer to evacuate their children and stay and fight the threat trying to save their animals (many examples from Katrina and other wet disasters).A third factor might be if there is previous experience with a similar threat. In the first wildfire in 2010 we evacuated our premises the moment that our fence trees was on fire and literaly we drive into flames to a safer area. In 2016, the presense of grey smoke behind the hills located in close proximity of our estate made us to load the cars and wait with engines operating until to see what was going on and what measures have been taken or see the fire fighting airplanes flying over our heads. When smoke disappeared, our heart returned to its normal place!

New System Developed to Evacuate Citizens

Source: https://i-hls.com/archives/85630

Sept 26 – Data-based modeling system may now help emergency managers to better determine when to call for evacuations due to a wildfire. The system has the ability to accurately predict the speed and direction of wildfire's movements. This information is then interfaced with a traffic simulator which assists in estimating how long it will take affected residents in an area to safely evacuate.

Behind the system is researcher and Assistant Professor at South Dakota State University (SDSU) Department of Geography, Dapeng Li, who says determining evacuation orders during a wildfire is difficult because of the plethora of factors involved in the decision-making process.

Commanders overseeing wildfire incidents are responsible for accounting for the rate of fire spread, population density and distribution, and the available outlets for evacuation traffic.

By looking at environmental hazards which include specifics about the natural, human and built surroundings in a given area, Li's system has been able to identify specific warning triggers for an evacuation. The spread and traffic simulations coupled with these triggers to help determine the proper timing of an evacuation.

According to Li, "the first step is to model the progression of the fire in the landscape. We need to take into account factors such as topography, fuel type, fuel moisture, wind direction and speed. We can use fire spread modeling to derive fire spread rates at different locations in the landscape and compute fire travel times. We then need to estimate how many cars will be in the road network during the evacuation. If it is too congested, the evacuees could be trapped en route by the fire and die in their cars."

While the case study took place in San Diego, California, the integrated modeling techniques can be applied to any geographic location, regardless of its population or infrastructural factors.

By merging fire spread and traffic data, many questions surrounding the timing of evacuation warnings can be properly addressed.

By using the paired modeling, incident commanders can examine the spatial patterns of fire perimeters and evacuation traffic for every minute in the evacuation simulation. This could help them improve their situational awareness and issue more effective protective action recommendations, according to ifiberone.com.

Why every hospital needs a natural disaster recovery plan

Source: https://searchhealthit.techtarget.com/opinion/Why-every-hospital-needs-a-natural-disaster-recovery-plan

In the first week of September 2018, news of a potentially destructive Category 4 hurricane that was forecast to make landfall on the coast of the Carolinas sent many of the hospitals and medical practices in both states rushing to dust off their disaster recovery and business continuity plans in preparation for it. Evacuation drills were reviewed and many other operating procedures were rehearsed and evaluated. But most of all, health IT systems were being tested and reassessed for their natural disaster recovery readiness. Most healthcare groups focused on a few aspects of their IT to ensure they were prepared for whatever outcome the storm had in store for them.

In any given hurricane season, healthcare organizations in areas that are affected by these natural disasters are no strangers to preparing for power outages, and potential structural damage from flooding, high winds or downed trees. Some of the prep work by their IT departments can include moving IT equipment off the ground or out of the basement to testing system failovers and backups. During Hurricane Florence, many healthcare organizations in the Carolinas quickly came to realize the importance of having a natural disaster recovery plan. Those who didn't now face significant obstacles to get back to the business of patient care.

The dependence on EHRs is significantly greater today than it was few decades ago, when paper charts could be used if computers' systems went offline. Providers now need to review electronic documentation that is collected and managed within their EHR systems to care for patients. Operating without these record systems can limit their ability to provide patient care since they are not able to review patient information such as medical history, medication lists and previous lab results. With this heavy reliance on technology and infrastructure, the need for IT to ensure its availability during or right after a natural disaster becomes critical.

How is natural disaster recovery different from disaster recovery?

While every healthcare organization should have a disaster recovery plan, it is a good idea to have a natural disaster recovery plan as well. According to SearchDisasterRecovery, a sister site of SearchHealthIT, natural disaster recovery requires its own type of planning because the scenarios that may result can have unpredictable circumstances that differ from those caused by cybercrime or human error. Healthcare organizations in areas that are prone to certain types of natural disasters should be sure to implement that type of disaster into their DR plan.

There were also widespread outages after Hurricane Florence moved away from the Carolinas that left even well-prepared practices unable to use their systems. For example, internet outages affected those using cloud-based EHRs in rural areas that may not have had redundant internet connections due to limited access.

For many healthcare organizations, the biggest question during a natural disaster is around when they will be able to recover from any system outages. Once a storm passes, many residents in hurricane-affected areas are likely to use healthcare services either as a result of the storm or for their regular follow-ups. IT has the responsibility of determining the estimated time required to get all systems back online in the event some of the equipment has been damaged and requires replacement. From the IT perspective, off-site data centers that contain the practice's or hospital's backups can be used temporarily to access records while their main systems are being repaired.

The growing concerns around the possible increase in strength of hurricanes is forcing many to focus on their natural disaster recovery and business continuity plans in the event of another storm like Hurricane Florence. Some in IT are taking these events as an opportunity to accelerate their transition to the cloud while others focus on ensuring their DR plans are up to date and fully tested. But no matter what the nature of the environment is, performing recovery drills and reevaluating their natural disaster recovery plans is the best way to know for sure a healthcare organization is prepared for what the next storm may bring to them.

First Responders Are Beginning to Address Their Own Health

Source: http://www.govtech.com/em/preparedness/First-Responders-Are-Beginning-to-Address-Their-Own-Health-.html

Oct 05 – First responders see a lot and the public wonders how they deal with it all. The reality is that first responders don't always deal with what they've seen in a healthy manner and many have traumatic stress issues that they try to keep quiet.

Oftentimes the stress manifests itself at home, affecting family relationships. The divorce rate for law enforcement personnel is around 75 percent. More than 80 percent of firefighters experience symptoms of mental health issues. Almost 25 percent of dispatchers have symptoms of Post-Traumatic Stress Disorder.

Much of the time, first responders feel they can't reveal their feelings to co-workers or management for fear that they might be considered weak or lose out on a promotion. Often, there is a code of silence about such issues at work and the fear of reprisal.

"They hear everything and see everything, it's the worst moments in people's lives and they're supposed to be calm and handle it," said Dr. Stephen Odom, CEO of New Vista Behavioral Health. "They compartmentalize it, and you can only do that for so long. Over time, it begins to take its toll."

For many reasons, first responders hold it in, don't ask for help and only when they get home, it seems do they let off steam, often to the detriment of the family. "That's the only safe place there is," Odom said. "It's tough to be a first responder's family."

First responders also feel they should be strong and be able to take it. They think they are or should be built differently than the rest of us and that if they can't handle the stress, it's a personal failing.

"They only come through our doors a couple of ways," Odom said. "Either something really bad happens or they have been told they need to come get help." Oftentimes, it's the family that can't take it anymore, he said. "The spouse can't take the drinking, or they have that thousand-yard stare all the time."

It's also difficult for first responders to share their problems with the rest of the public. And there are now specialized 12-step meetings for first responders, part of the change that Odom says he's beginning to see that addresses the issue.

"Coming up with a world in which they can talk about mental health issues among their peers seems to work better," he said. "More and more, they are beginning to talk about mental wellness now and not mental illness. Departments need to acknowledge the issue."

An important step in getting first responders to seek help or stay healthy is to get people to understand that it's one of the consequences of the job. "And that everyone who experiences these kinds of things will have these consequences," Odom said. "We are working hard to normalize it; to say this is what happens when you're a firefighter or a police officer and it's part of the job."

He said agencies have the resources, they just have to acknowledge the issue and lead the charge. "There are employee assistance programs, departmental wellness people, but they have to be given permission and clout to put these things out there so people want to be a part of it," Odom said.

There is debriefing that must occur both before and after incidents. First responders can be taught resiliency techniques, such as combat breathing, where they are taught how to breathe in such a manner that tamps down anxiety, helps the coping mechanism.

There's also Eye Movement and Desensitization and Reprocessing, which teaches the brain to reprogram memories and puts them in their place and takes away the emotional power they have. There also needs to be debriefing after the fact. "Every time something happens we should talk through it, so you can get it out of your head, because you need to," Odom said.

Odom used the airplane oxygen mask analogy to explain the importance of first responder health. "They tell you if the oxygen mask drops, put it on yourself before you take care of the kids next to you. The same thing needs to be said for first responders. You can't really be the best first responder you can be if you're not taking care of yourself first."

EDITOR'S COMMENT: It would be very interesting to read a similar article addressing the same problem but this time regardfing medical personnel (physicians, nurses, ambulance crews). They also face death on almost daily basis (depending on medical specialty) but nobody cares to address their feelings in the aftermath of a hard day. It is their job they say; it will make a young doctor tuffer but what if death affect the individual in an adverse way? What if phobias are installed and affect both his/her personal and professional life? There is always time for improvement but only if we really care about our colleagues and their well being!

Best practices for providing alerts to the public on disasters and incidents

Source: https://www.dhs.gov/sites/default/files/publications/1051_IAS_Report-on-Alerting-Tactics_180807-508.pdf

Helping the Chronically Ill During Natural Disasters

By Allegra Balmadier

Source: https://www.domesticpreparedness.com/healthcare/helping-the-chronically-ill-during-natural-disasters/

Oct 24 – Although 2017 was a historic year for natural disasters, 2018 is turning out to be more of the same. Filled with wildfires, tornadoes, floods, tropical systems, and the devastating Hurricanes Florence and Michael, it appears the frequency of natural disasters is increasing. Preparedness professionals face challenges meeting the needs of everyone impacted by such events, especially those with chronic conditions. Fortunately, with pre-disaster planning and post-disaster recovery and evaluation, preparedness professionals can better help the most vulnerable access the resources they need.

Individuals with chronic conditions typically face an array of daily challenges – even without an impending natural disaster. Taking multiple medications, relying on essential treatments, using medical equipment, and making regular visits to a health care provider are often part of the routine. When a disaster strikes, all that is upended. Critical medications, treatments, and caregivers may not be available. Mobility may be restricted and, if the power is out, medical equipment may not work. Without needed health care, a chronic condition can quickly lead to failing health – even death.

To make matters worse, data from the U.S. Centers for Disease Control and Prevention (CDC) indicate that individuals with chronic conditions are prevalent in many states that are

most susceptible to natural disasters. Nursing@USC, the online FNP program from the University of Southern California, created a visualization that depicts the number of people living with chronic conditions in each state.

Planning for Disaster

Preparedness professionals can help the vulnerable in their communities by encouraging them and their caregivers to create a contingency plan before disaster strikes. It should include:

- A clear understanding of all medical conditions, needed medications, and treatments;
- An updated list of medications and any significant health history that may affect care;
- A medical alert bracelet that identifies a chronic condition or specific care requirement;
- A 10-day supply of all necessary medications;
- A plan to deal with loss of power – especially if there is equipment dependent on electricity, such as an oxygen concentrator;
- A supply of emergency food, battery-operated flashlights, and a change of clothes;
- Devices at home that monitor vital signs and changes in physical health;
- Assurance that family members and close neighbors know how to administer care;
- An evacuation plan, including identifying stable buildings in the community for shelter and registering with first responders to assist with evacuation needs;
- Sign-up for community warning systems for weather alerts;
- Communication plan with family members in the event of lost power; and
- A list of emergency phone numbers for providers and medical facilities in an accessible place.

It is also important for preparedness professionals to help the vulnerable in their communities learn more about available resources, so they will know where to seek help after a natural disaster. For instance, Healthcare Ready provides an array of resources for those impacted by disasters, including Rx Open, which lists pharmacies that are open in an affected disaster area.

Providing Care During & After a Disaster

During and after a disaster, one of the greatest challenges for individuals with chronic conditions is achieving continuity of care. Hospitals and clinics may not be available, shelters may lack essential supplies, and individuals may be trapped in their homes. First responders and health care volunteers must establish priorities and remain flexible.

Since local resources are rarely adequate to deal with such challenges, partnering with government and relief organizations is essential to gain access to vulnerable populations and provide needed supplies and care. For instance, in the Carolina regions devastated by Florence-related flooding, Direct Relief staff members were on the ground pre- and post-storm delivering requested emergency medical aid and coordinating with local health staff. The organization also provided emergency medical backpacks filled with medicines to manage chronic conditions and other critical medicines and supplies to one local clinic. This made it possible for the clinic's staff to provide medical care at a local shelter where several hundred residents had been living since Florence hit.

Post-Disaster Follow-Up

Once the event has passed, the difficulties for those with chronic conditions may be just starting. When medications run out, when oxygen tanks are empty, when it is time for another session of dialysis, the most vulnerable populations may begin to feel the deepest impact of the disaster.

That is why pre-disaster planning is so essential. When preparedness professionals take time to understand the needs of individuals in their communities, they are better prepared to follow up and provide the type of support required to address chronic health issues. Some are even using predictive algorithms to better understand who may need the most help after a disaster.

Post-disaster evaluation is also critical to better understand which pre-disaster strategies were most effective and where improvement is needed. For instance, in "Emergency and Disaster Preparedness for Chronically Ill Patients: A Review of Recommendations," the authors used specific criteria to conduct a retrospective analysis of relevant guidelines addressing the needs of individuals with chronic illnesses during disasters. Although they were able to create a summary of disaster preparedness recommendations for major chronic illnesses, the authors also introduced three suggestions to improve disaster preparedness:

- More evidence-based recommendations, because many were based on anecdotal evidence or expert opinions;
- More consistent messaging regarding recommendations to prevent confusion for patients and health care providers; and
- Increased feasibility for patients, because what is theoretically sound may not be practical for patients who are often limited in a variety of ways.

When a natural disaster strikes, individuals with chronic illnesses are among the most vulnerable. With effective pre-disaster planning and post-disaster recovery, preparedness and response professionals can help those in need better weather the storm.

Allegra Balmadier *is a digital public relations coordinator covering health at 2U Inc. She supports outreach for public health and clinical health programs, like the nursing program at the University of Southern California.*


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

World has 12 years to limit catastrophic impacts of climate change

Source: http://www.homelandsecuritynewswire.com/dr20181010-world-has-12-years-to-limit-catastrophic-impacts-of-climate-change

Oct 10 – Limiting global warming to 1.5°C would require rapid, far-reaching, and unprecedented changes in all aspects of society, the IPCC said in a new assessment. With clear benefits to people and natural ecosystems, limiting global warming to 1.5°C compared to 2°C could go hand in hand in hand with ensuring a more sustainable and equitable society, the Intergovernmental Panel on Climate Change (IPCC) said on Monday.

The Special Report on Global Warming of 1.5°C was approved by the IPCC on Saturday in Incheon, Republic of Korea. It will be a key scientific input into the Katowice Climate Change Conference in Poland in December, when governments review the Paris Agreement to tackle climate change.

"With more than 6,000 scientific references cited and the dedicated contribution of thousands of expert and government reviewers worldwide, this important report testifies to the breadth and policy relevance of the IPCC," said Hoesung Lee, Chair of the IPCC.

Ninety-one authors and review editors from forty countries prepared the IPCC report in response to an invitation from the United Nations Framework Convention on Climate Change (UNFCCC) when it adopted the Paris Agreement in 2015.

"One of the key messages that comes out very strongly from this report is that we are already seeing the consequences of 1°C of global warming through more extreme weather, rising sea levels and diminishing Arctic sea ice, among other changes," said Panmao Zhai, Co-Chair of IPCC Working Group I.

The report highlights a number of climate change impacts that could be avoided by limiting global warming to 1.5°C compared to 2°C, or more. For instance, by 2100, global sea level rise would be 10 cm lower with global warming of 1.5°C compared with 2°C. The likelihood of an Arctic Ocean free of sea ice in summer would be once per century with global warming of 1.5°C, compared with at least once per decade with 2°C. Coral reefs would decline by 70-90 percent with global warming of 1.5°C, whereas virtually all (> 99 percent) would be lost with 2°C.

"Every extra bit of warming matters, especially since warming of 1.5°C or higher increases the risk associated with long-lasting or irreversible changes, such as the loss of some ecosystems," said Hans-Otto Pörtner, Co-Chair of IPCC Working Group II.

Limiting global warming would also give people and ecosystems more room to adapt and remain below relevant risk thresholds, added Pörtner. The report also examines pathways available to limit warming to 1.5°C, what it would take to achieve them and what the consequences could be. "The good news is that some of the kinds of actions that would be needed to limit global warming to 1.5°C are already underway around the world, but they would need to accelerate," said Valerie Masson-Delmotte, Co-Chair of Working Group I.

The report finds that limiting global warming to 1.5°C would require "rapid and far-reaching" transitions in land, energy, industry, buildings, transport, and cities. Global net human-caused emissions of carbon dioxide (CO2) would need to fall by about 45 percent from 2010 levels by 2030, reaching 'net zero' around 2050. This means that any remaining emissions would need to be balanced by removing CO2 from the air.

"Limiting warming to 1.5°C is possible within the laws of chemistry and physics but doing so would require unprecedented changes," said Jim Skea, Co-Chair of IPCC Working Group III.

Allowing the global temperature to temporarily exceed or 'overshoot' 1.5°C would mean a greater reliance on techniques that remove CO2 from the air to return global temperature to below 1.5°C by 2100. The effectiveness of such techniques are unproven at large scale and some may carry significant risks for sustainable development, the report notes.

"Limiting global warming to 1.5°C compared with 2°C would reduce challenging impacts on ecosystems, human health and well-being, making it easier to achieve the United Nations Sustainable Development Goals," said Priyardarshi Shukla, Co-Chair of IPCC Working Group III.

The decisions we make today are critical in ensuring a safe and sustainable world for everyone, both now and in the future, said Debra Roberts, Co-Chair of IPCC Working Group II.

"This report gives policymakers and practitioners the information they need to make decisions that tackle climate change while considering local context and people's needs. The next few years are probably the most important in our history," she said.

The IPCC is the leading world body for assessing the science related to climate change, its impacts and potential future risks, and possible response options.

The report was prepared under the scientific leadership of all three IPCC working groups. Working Group I assesses the physical science basis of climate change; Working Group II addresses impacts, adaptation and vulnerability; and Working Group III deals with the mitigation of climate change.

The Paris Agreement adopted by 195 nations at the 21st Conference of the Parties to the UNFCCC in December 2015 included the aim of strengthening the global response to the threat of climate change by "holding the increase in the global average temperature to well below 2°C above pre-industrial levels and pursuing efforts to limit the temperature increase to 1.5°C above pre-industrial levels."

As part of the decision to adopt the Paris Agreement, the IPCC was invited to produce, in 2018, a Special Report on global warming of 1.5°C above pre-industrial levels and related global greenhouse gas emission pathways. The IPCC accepted the invitation, adding that the Special Report would look at these issues in the context of strengthening the global response to the threat of climate change, sustainable development, and efforts to eradicate poverty.

The IPCC notes that Global Warming of 1.5°C is the first in a series of Special Reports to be produced in the IPCC's Sixth Assessment Cycle. Next year the IPCC will release the Special Report on the Ocean and Cryosphere in a Changing Climate, and Climate Change and Land, which looks at how climate change affects land use.

James Hansen, the former Nasa scientist who helped raised the alarm about climate change, said both 1.5C and 2C would take humanity into uncharted and dangerous territory because they were both well above the Holocene-era range in which human civilization developed. But he said there was a huge difference between the two: "1.5C gives young people and the next generation a fighting chance of getting back to the Holocene or close to it. That is probably necessary if we want to keep shorelines where they are and preserve our coastal cities," he told the *Guardian*.