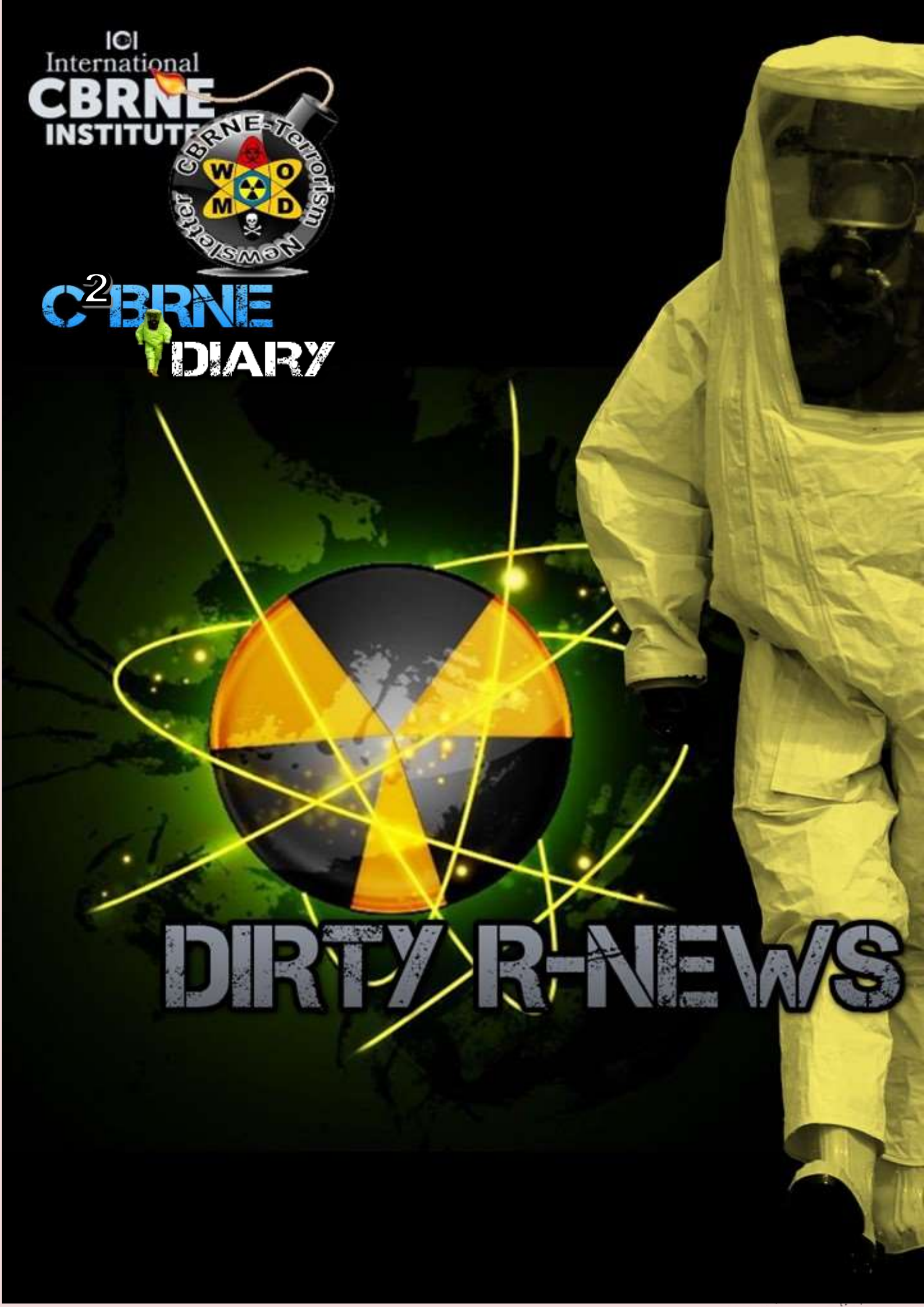
2 CBRNE DIARY

Dedicated to Global First Responders

September 2018


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

Did you know?

The KANUPP plant in Karachi, Pakistan, has the most people—8.2 million—living within 30 kilometres, although it has just one relatively small reactor with an output of 125 megawatts. Next in the league, however, are much larger plants—Taiwan's 1,933-megawatt Kuosheng plant with 5.5 million people within a 30-kilometre radius and the 1,208-megawatt Chin Shan plant with 4.7 million; both zones include the capital city of Taipei.

Nuclear reactors: Karachi's newest danger?

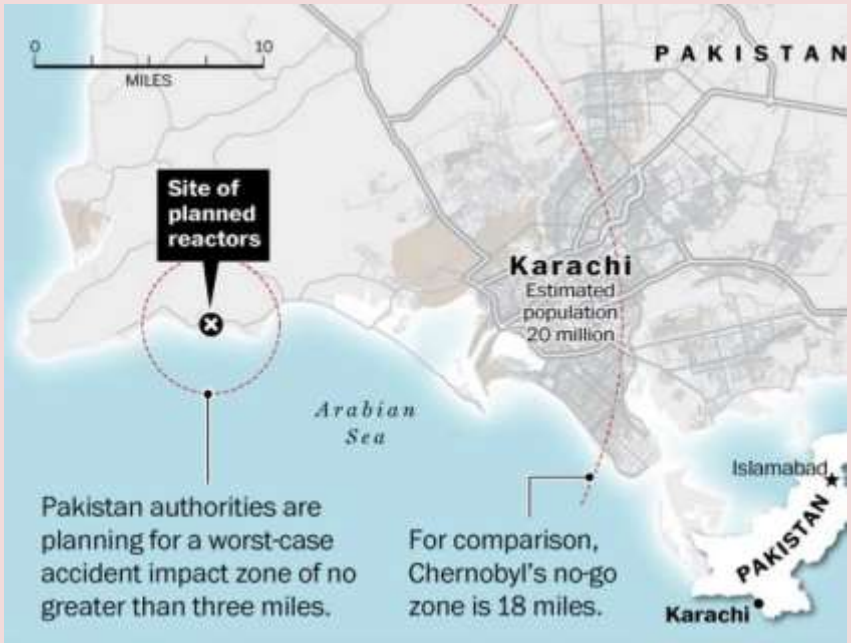
Source: https://www.dawn.com/news/1182150

2015 – Nuclear power and patriotic pride are inextricably intertwined in Pakistan. In the decades since the tests were conducted, Pakistan's possession of a nuclear bomb is believed to be by many, the sole reason for why the country; located as it is at the intersection of where superpowers like to spar, continues to exist.

It is a belief that is fed and promoted with zeal by politicians and popular culture; and all institutional arms of the state. Little kids cheer the bomb, that good bomb that can destroy everything, even as smaller bad bombs go off all around them.

The word nuclear then is considered by most to be an incontrovertible good thing. It is no wonder then that the construction of two additional nuclear reactors at KANUPP near Karachi are being regaled as the solution to the city's continuing plunge into darkness.

With more power it is assumed, and with nuclear power, the city of lights, now the city of darkness and death can be resurrected again. The city's inhabitants, their lives long cut up and diced away by constant power outages are eager for the reprieve. In the city's ever dimming reality; hoping for light is but a necessity.



But, like everything else produced in Karachi, the 1100 MW electricity produced by the AC-3000 reactors are not to be reserved for Karachi but rather for the national grid and for areas that will bear none of the environmental risk of living next door to a nuclear reactor.

The proximity is worth noting; the new reactor will be less than 20 miles from Karachi's downtown. Nearly 7,000 people live in every square mile of that distance. Even Chernobyl, the plant at the heart of one of the world's worst nuclear plant disasters, was located further away from such dense human settlement.

The nearness to hapless humans is not the only problem being ignored in this energy eager moment.

The new Chinese made nuclear reactor, which has the capacity to produce far more electricity than its predecessors, is not being used anywhere else. Karachi and its environs then will be the trial run for this mass nuclear energy production experiment.

Then there are Karachi's geographical realities; the plant will not simply be close to people it can kill, it will also be in an earthquake and tsunami prone zone.

In years past, when storms have skimmed the shore, the city has relied on the supernatural powers of the shrine at its coast. Arriving storms descending on nuclear reactors may not be held back by the luck and folklore.

The fallout from Japan's Fukushima nuclear plant continues even four years after the tsunami, with radioactive water still seeping into the ocean.

What will be the scale of Karachi's condemnation, if such a storm hits its soon to be nuclear coast?

A thin sliver of civil society had tried to fight the scapegoating of Karachi for the country's energy needs. To pacify them, without permitting them to actually influence the altering of the plan or its construction, a "public hearing" was held on April 27th 2015. To make it as inconvenient as possible, it was held at KANUPP instead of actually in the city precluding many from attending.

Perhaps, the organisers were underscoring just how "far" the nuclear reactor will be from the city. Radiation, however, travels faster than traffic and people, and unlike the annoying objections of environmental and civil activists; it cannot be stopped.

The over 300-page environmental impact report issued by the Pakistan Atomic Energy Commission is a daunting read. Its heft and technical details; along with the short time permitted to peruse its contents is of course, all meant to deter anyone from saying anything.

For those who may look through its pages; it is grim reading detailing the tons of liquid and solid radioactive waste that will be produced from the energy, making behemoth that will likely be Karachi's newest danger.

If you look past the report's promises and consider the ineptitude with which even non-radioactive waste is disposed off in Karachi, you cannot help but be terrified.

If things go wrong, and they do so often in Karachi, the poison will spread farther, to the 20 million inhabitants of Karachi who stand directly in the path of the plant's noxious and tainted effusions.

For those who may look through its pages; it is grim reading detailing the tons of liquid and solid radioactive waste that will be produced from the energy, making behemoth that will likely be Karachi's newest danger.

If you look past the report's promises and consider the ineptitude with which even non-radioactive waste is disposed off in Karachi, you cannot help but be terrified.

If things go wrong, and they do so often in Karachi, the poison will spread farther, to the 20 million inhabitants of Karachi who stand directly in the path of the plant's noxious and tainted effusions.

Just like the streets of Karachi, its dark corners and alleys and its million days of mourning bear the brunt of the nation's war and the nation's pain; so too, will they bear the weight of the nation's want; their contaminated lives lighting up the homes and havens of those far away, in other, luckier parts of Pakistan.

The US Government Is Updating Its Nuclear Disaster Plans And They Are Truly Terrifying

By Dan Vergano

Source: https://www.buzzfeednews.com/article/danvergano/north-korea-nuclear-bomb-fema-plans

Aug 24 – Amid concerns over North Korea, federal emergency managers are updating disaster plans to account for large nuclear detonations over the 60 largest US cities, according to a US Federal Emergency Management Agency official.

The shift away from planning for small nuclear devices that could be deployed by terrorists toward thermonuclear blasts arranged by "state actors" was discussed on Thursday at a two-day National Academies of Sciences workshop for public health and emergency response officials held at its headquarters across the street from the US State Department.

"We are looking at 100 kiloton to 1,000 kiloton detonations," chief of FEMA's chemical, biological, radiological, and nuclear branch Luis Garcia told BuzzFeed News. The agency's current "nuclear detonation" guidance for emergency planners, first released in 2010, had looked at 1 to 10 kiloton blasts — smaller than the 1945 Hiroshima and Nagasaki atomic bombs that killed more than 200,000 people at the end of World War II. Those smaller size detonations had seemed more reasonable after 9/11, with high concerns about an improvised terrorist bomb.

But last year North Korea tested an apparent thermonuclear bomb with a surprisingly large estimated blast size of 250

kilotons, a "city buster" much bigger than past test blasts and nearly the size of current US intercontinental ballistic missile warheads. The test blast kicked off a new era of nuclear anxiety in the US.

"The North Koreans have really changed the calculus," Cham Dallas of the Institute for Disaster Management at the University of Georgia told workshop participants. "We really have to look at thermonuclear now."

Dallas presented "speculative" analyses of a nuclear detonations in several cities — including New York and Washington, DC — at the workshop, suggesting that a thermonuclear blast roughly doubles the hundreds of thousands of dead and many more wounded (a 1979 analysis of a 1,000 kiloton blast in Detroit estimated 220,000 deaths, for example) compared to the atomic bomb blasts. They also cause many more burn injuries and larger fallout clouds that travel farther away.

The updated FEMA guidance would be for the 60 largest urban areas in the US and will rely on newer detonation models created by the Department of Energy's Lawrence Livermore National Laboratory. These models take into account weather patterns that direct and distort weapon clouds, as well as the shelter provided by concrete structures. "A 10 times larger [explosion] yield does not make things 10 times worse," LLNL's Brooke Buddemeier said at the workshop. People remaining in shelters in the hours and days after a blast greatly lower their chances of getting radiation sickness.

The new FEMA plan will also have to consider modern contingencies such as cyberweapons striking power plants and cell phone signals before a blast, or a nuclear blackmail scenario where a single bomb is detonated followed by threats to set off more unless demands are met. In response to an audience question, Garcia said the agency has also considered scenarios where a nuclear bomb, a cyberattack, a coordinated electromagnetic pulse, and biological weapons all hit the US at the same time.

BuzzFeed News

During the "Duck and Cover" period of the Cold War, US planners had fitfully called for civil defense measures for a nuclear war with the Soviet Union, most famously in a short-lived fallout shelter boom during the Cuban missile crisis of the early 1960's.

"All states, all large cities have all thought about this before," the CDC's Strategic National Stockpile Deputy Director Steve Adams said, and they already designate sites for medical supplies after disasters. "I think the challenge for us will be distribution, a very large one."

The national stockpile now contains medicine and medical material to treat radiation sickness, but Adams expressed concerns about burn kits. Medical specialists from the American Burn Association frequently raised concerns at the two-day workshop about numbers and training of burn experts nationwide, particularly for treating children. Colleen Ryan of Harvard Medical School told BuzzFeed News that there are only about 300 qualified burn surgeons nationwide, and that the burn treatment requirements for medical school training of surgeons were curtailed a decade ago.

Nursing expert Tener Veenema of the Johns Hopkins Bloomberg School of Public Health also questioned plans like FEMA's, pointing to studies suggesting that many nurses and doctors feared radiation above other threats, and might not show up to treat people after such a disaster, fleeing instead. "We need to analyze these plans for nursing shortfalls," she said, adding that no one has analyzed the costs of such a blast to the national economy to justify the extra spending and training that would be needed to make the plans justifiable to lawmakers.

Similarly, Ron Miller, acting director of the National Disaster Medical System at the US Department of Health and Human Services, raised concerns about the 6,000 doctors, nurses, and other medical professionals showing up after a nuclear explosion.

At least two kinds of widespread complacency make medical planning for a large nuclear detonation more difficult, Dallas added. The first is a belief in parts of the country far from major cities that a nuclear detonation won't affect their lives, when in reality such a catastrophe would be a significant blow to resources everywhere.

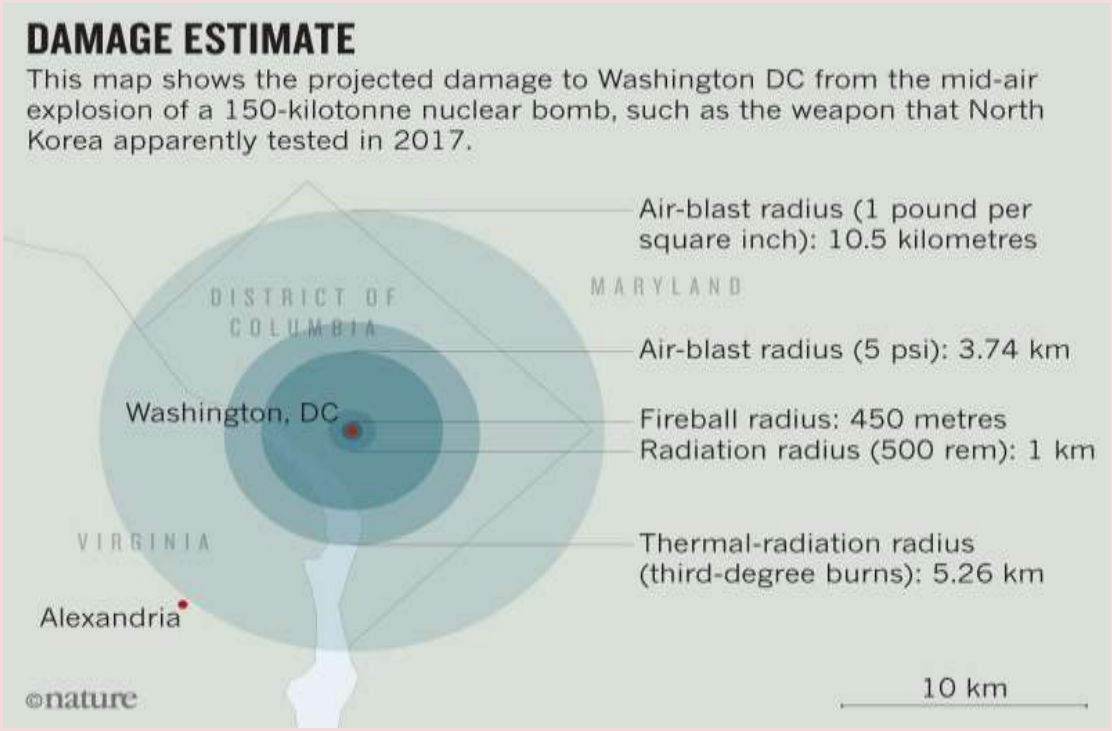
The other is that a blast will just kill everyone in its wake and that any effort at disaster planning is futile, when in reality acute radiation poisoning and severe burns can be treated.

"We have to get past this fatalism," he said. "There's a lot of denial going on."

United States woefully unprepared for nuclear strike, say scientists

Nature 560, 538-539 (2018)
Source: https://www.nature.com/articles/d41586-018-06077-x

Aug 28 – The United States is not prepared to deal with the aftermath of a major nuclear attack, despite North Korea's efforts to develop nuclear weapons and the increasing tensions between nations overall. That was the blunt assessment of public-health experts who participated in a meeting last week on nuclear preparedness, organized by the National Academies of Sciences, Engineering, and Medicine.
The gathering is "an acknowledgement that the threat picture has changed, and that the risk of this happening has gone up", says Tener Veenema, who studies disaster nursing at Johns Hopkins University in Baltimore, Maryland, and co-chaired the conference in Washington DC .



Source: nuclearsecrecy.com/nukemap

Since the fall of the Soviet Union in 1991, the United States's research and preparedness efforts for a nuclear strike have focused largely on the possibility of a terrorist attack with a relatively small, improvised 1-kilotonne weapon or a 'dirty bomb' that sprays radioactive material.
But North Korea is thought to have advanced thermonuclear weapons — each more than 180 kilotonnes in size — that would cause many more casualties than would a dirty bomb (see 'Damage estimates'). "Now that thermonuclear is back on the table, we're back to people saying, 'We can't deal with this,'" says Cham Dallas, a public-health researcher at the University of Georgia in Athens.
Veenema says that the science academies decided to do a study in November 2017, three months after North Korean leader Kim Jong-un threatened to launch a nuclear weapon at the US territory of Guam. The academies wanted to bring together the different government, academic and private sectors that would be involved in the medical response to a nuclear attack, Veenema adds. The academies' committee plans to release a report in December that lays out how the United States could plug the gaps in its response capabilities.
The US government's spending on nuclear-weapons research and response has dropped drastically over the past few decades — as has the number of health workers with training in radiation medicine and management. According to a 2017 study[1] by Dallas, more than

half of emergency medical workers in the United States and Japan have no training in treating radiation victims.

The same study suggests that even trained medical professionals might be too frightened to enter a nuclear-fallout zone or to treat radiation victims at the scene — Dallas's group found that 33% of medical professionals said they would not be willing to respond in such a scenario.

Compounding these concerns, treatments for radiation exposure and burns might not be available in sufficient quantities in the aftermath of a nuclear attack. James Jeng, a burn surgeon at Mount Sinai Health System in New York City, says that the detonation of a nuclear bomb can leave behind hundreds of thousands of burn victims. The best treatment for such injuries is skin grafting, he says, but there are only about 300 burn surgeons in the United States who know how to perform the procedure. It might also be difficult to quickly transport enough donor skin to treatment sites, Jeng adds.

North Korea's threat to Guam last year made clear to public-health officials there how limited their response capabilities are, says Patrick Lujan, emergency-preparedness manager for the Guam Department of Public Health and Social Services. Guam, an island of 163,000 people, has only three hospitals and no burn units. "We realized there's just so much you can do, being on an island," Lujan says.

Update of Health Effects of the Chernobyl Accident fact sheet

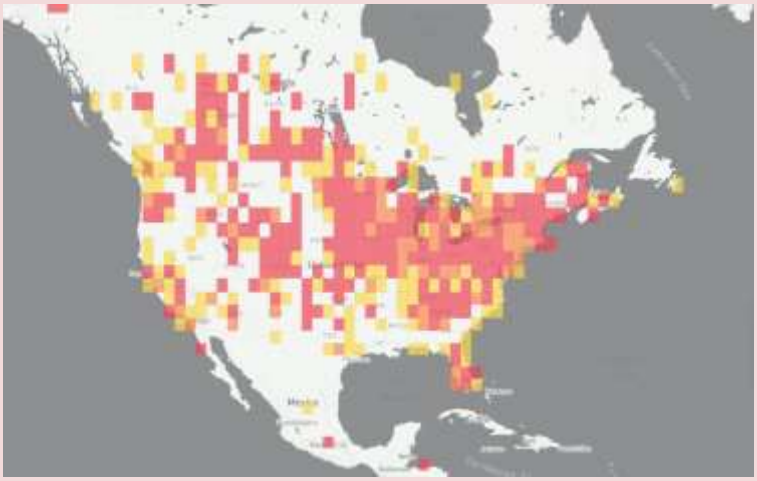
Source: http://nuclearsafety.gc.ca/eng/resources/health/index.cfm

Today, the CNSC published an update of its fact sheet titled Health Effects of the Chernobyl Accident to include the latest data collected on the health consequences of radiation exposure from the accident. New information is based on the United Nations Scientific Committee on the Effects of Atomic Radiation (UNSCEAR) 2018 white paper titled Evaluation of data on thyroid cancer in regions affected by the Chernobyl accident.

Global map of radioactive gas pulls data from a network of sensors in users' homes

Source: https://newatlas.com/airthings-radon-map/56202/

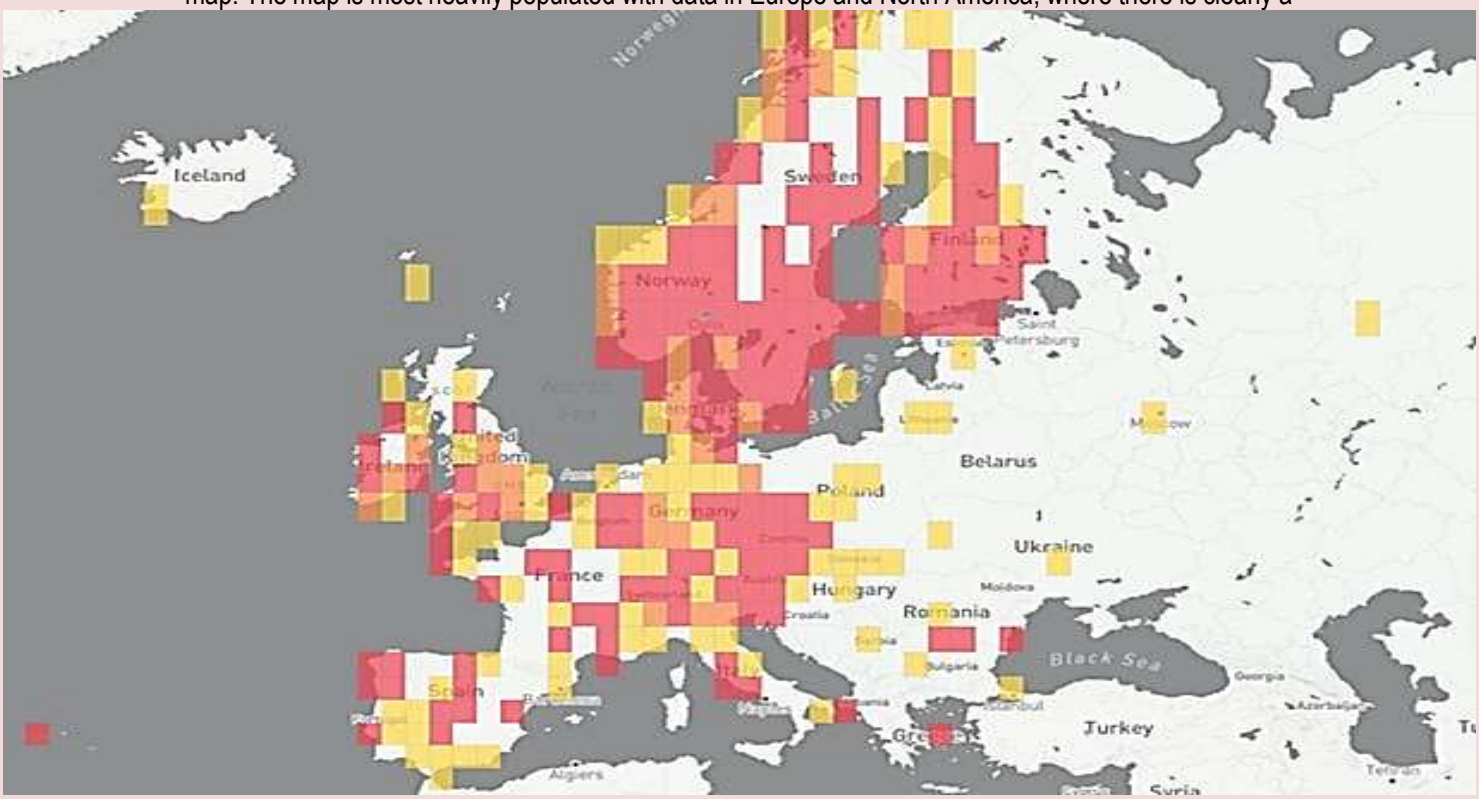
Sept 05 – Airthings, the company behind digital sensors that detect radon gas, has built a global map based on frequently updated data pulled from its distributed network of devices installed in customers' homes. Though the precise location of the sensors is hidden to protect users' privacy, the map does break localized regions into areas that Airthings deems lower, medium and high risk to radon gas.



Radon is a colorless and odorless radioactive gas belonging to the group of noble gases. It occurs as an intermediate step as the radioactive elements uranium and thorium decay into lead in the Earth's crust. Even in its most stable form it has a half-life of only 3.8 days. However, as it rises up from the Earth it can build up in enclosed spaces, including buildings. Studies suggest that high concentrations of radon can cause lung cancer, with the US Environmental Protection Agency (EPA) citing radon as the greatest cause of lung cancer after smoking. It's thought to cause 21,000 cancer deaths per year in the States, 2,900 of which are among non-smokers. Airthings posits that, because radon levels can fluctuate over time, radon detectors are a useful way to monitor risk. Indeed, the EPA makes radon test kits available from its website.

The company's own detectors start with the Wave – a €199 (US$230) device that you literally wave at for a visual indication of radon concentration in your home – green being good (under 100 Bq per cubic meter), red being bad (over 100 Bq per cubic meter), and amber meaning "temporarily high" (with readings somewhere in between). It can also feed more detailed results to a smart phone. The company makes a Wave Plus sensor, too, which additionally monitors carbon dioxide and volatile organic compounds.

But because these devices are networked, Airthings has been able to pull data to create this global radon map. The map is most heavily populated with data in Europe and North America, where there is clearly a



good distribution of Airthings devices. The data from remaining continents is very sparse indeed, though. It's important to take this for what it is: a tech demo rather than a scientific endeavor. The methods Airthings use to obfuscate the data to protect users' privacy may mean a lone sensor reading is the basis for an entire region. Airthings itself notes that concentrations can vary from home to home, let alone across the large minimum areas the map uses to break down the data.
Perhaps more intesting is how we're starting to see connected, smart devices in the home being used to build a global picture – in this case of radon concentrations, but this could just as easily be for energy consumption, robot vacuum user base, or Alexa voice queries for recipes including yam.
A red block on the map covering your part of the world may not be reason alone for undue alarm, if it helps to raise awareness of the risks posed by radon then that's no bad thing – even if Airthings does clearly stand to gain.

New Nuclear Notebook: Pakistani Nuclear Forces, 2018

By Hans M. Kristensen
Source: https://fas.org/blogs/security/2018/09/pakistan-notebook2018/

Sep 04 – The latest FAS Nuclear Notebook has been published in the Bulletin of the Atomic Scientists: Pakistani nuclear forces, 2018 (direct link to PDF). We estimate that Pakistan by now has accumulated an **arsenal of 140-150 nuclear warheads** for delivery by short- and medium-range ballistic and cruise missiles and aircraft.
This is an increase of about ten warheads compared with our estimate from last year and continues the pace of the gradual increase of Pakistan's arsenal we have seen for the past couple of decades. The arsenal is now significantly bigger than the 60-80 warheads the U.S.

Defense Intelligence Agency in 1999 initially estimated Pakistan might have by 2020. If the current trend continues, we estimate that the Pakistani nuclear warhead stockpile could potentially **grow to 220-250 warheads by 2025.**

A Babur-3 dual-capable SLCM is test-launched from an underwater platform in the Indian Ocean on January 9, 2017.

The future development obviously depends on many factors, not least the Pakistani military believes the arsenal needs to continue to grow or level out at some point. Also important is how the Indian nuclear arsenal evolves.

The Pakistani government and officials initially described Pakistan's posture as a "credible minimum deterrent" but with development of tactical nuclear weapons later began to characterize it as a "full spectrum deterrent." Moreover, development is now underway to add a sea-based leg to its nuclear posture, and a flight test was conducted in 2017 of a ballistic missile that Pakistani officials said would be capable of carrying multiple warheads to overcome missile defense systems.

Additional information can be found here:

- Pakistani nuclear forces, 2018
- Status of World Nuclear Forces

***Hans M. Kristensen** is the director of the Nuclear Information Project at the Federation of American Scientists where he provides the public with analysis and background information about the status of nuclear forces and the role of nuclear weapons.*

EDITOR'S COMMENT: It is strange that a country that posse's nuclear weapons cannot feed its own people forcing them to illegaly migrate to Europe (and Greece). It is the same with India of course and its over 1 billion population. I just wonder: in case of a future war, who will fight the enemy: the nuclear heads or the people?

Nuclear abolition — a growing national movement

Source: https://eu.vcstar.com/story/opinion/columnists/2018/09/08/nuclear-abolition-growing-national-movement/1217675002/

Sept 08 – Seventy-three years after the dawn of the nuclear age, a United States national movement is emerging calling for the abolition of these weapons.

This new movement is called "Back from the Brink: a Call to Prevent Nuclear War." It evolved as a grassroots U.S. response to the 2017 United Nations Treaty on the Prohibition of Nuclear Weapons.

The treaty, which opened for signature on Sept. 20, 2017, has been signed by 60 nations and ratified by 14, the latest being New Zealand in July. Once 50 nations ratify, it becomes international law — making nuclear weapons illegal, like all other weapons of mass destruction, to possess, develop, test, use or threaten to use.

The U.S. campaign is an all-in effort with the goal of preventing nuclear war while working to eliminate these weapons entirely. It endorses the treaty and additional important protective policies such as ending any president's sole and unchecked authority to launch a nuclear attack, renouncing the option of using nuclear weapons first, removing U.S. nuclear weapons from hair-trigger alert, and canceling U.S. plans to replace its entire arsenal with enhanced weapons at a projected cost of $1.7 trillion over 30 years.

The Call was crafted by dozens of organizations including scientific, religious and non-governmental organizations such as Physicians for Social Responsibility, the Union of

Concerned Scientists, and Soka Gakkai International.

In August our nation witnessed a rapid acceptance of the campaign. Following the unanimous endorsement by the U.S. Council of Mayors at its June meeting in Boston, it has gained significant support. Acknowledging the Aug. 6 and 9, 1945, nuclear attacks on Hiroshima and Nagasaki, the resolution was adopted unanimously by the Los Angeles and Baltimore city councils on Aug. 8 and 6, respectively. Ojai and 10 other cities around the nation, as well as over 150 faith organizations, NGO's and thousands of individuals have done so as well.

One of our own assembly members, Monique Limon, has helped move California into the national and international spotlight with her resolution AJR 33 entitled "Treaty on the Prohibition of Nuclear Weapons." It fully endorses the "Back from the Brink" Resolution and passed the State Assembly on Aug. 20 and Senate on Aug. 28.

This measure from the nation's largest state and sixth largest global economy puts California at the forefront of urging our federal leaders and nation to embrace the treaty and to make nuclear disarmament the centerpiece of our national security policy and furthermore to spearhead a global effort to prevent nuclear war. This Call can be endorsed by any and all, empowering citizens to take action in the international movement to abolish nuclear weapons.

Our local community has played a driving role in setting an example. Following Ojai's declaration as a nuclear-free zone supporting the resolution in April, adjacent communities have taken note. The city of Santa Barbara will soon consider a similar resolution as will many cities and organizations around the country. The common feature is the recognition that nuclear war has no winners and the existential threat it poses must be prevented. The only way prevention can occur is through the complete abolition of these weapons. Nuclear war remains the greatest public health threat we face.

Throughout the nuclear age, most of us have felt paralyzed and powerless in being able to express our fear of, frustration with and desire for the elimination of these weapons. We have become psychologically numbed to them.

With this new and growing movement, each of us has an opportunity to be empowered and demand action to protect our world for our children and future generations. Please join us in supporting this effort by making your voice heard.

***Robert Dodge** is a family physician practicing in Ventura, chairman of Citizens for Peaceful Resolutions and president of Physicians for Social Responsibility-Los Angeles.*

Improving X-ray detection technology

Source: http://www.homelandsecuritynewswire.com/dr20180914-improving-xray-detection-technology

Sept 14 – The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) has awarded a total of nearly $3.5 million in funding to three new research and development (R&D) projects designed to improve the threat detection capabilities of current X-ray technologies for checked baggage systems.

"The emergence of homemade explosives has placed many challenges on aviation security screening," said William N. Bryan, Senior Official Performing the Duties of the DHS Under Secretary for Science and Technology. "S&T is making important investments in technology that could be leveraged into the next generation of checked baggage screening equipment."

"We are addressing current, ongoing, and upcoming capability gaps with a three-pronged approach utilizing the continuous transition of hardware, software, and knowledge," said S&T Checked Baggage Program Manager, Sharene Young.

"If successful, these projects will significantly improve operational efficiency and security effectiveness for TSA baggage screening operations," said Eric Houser, Acting Director of the Analysis and Requirements and Architecture Divisions for the Transportation Security Administration (TSA).

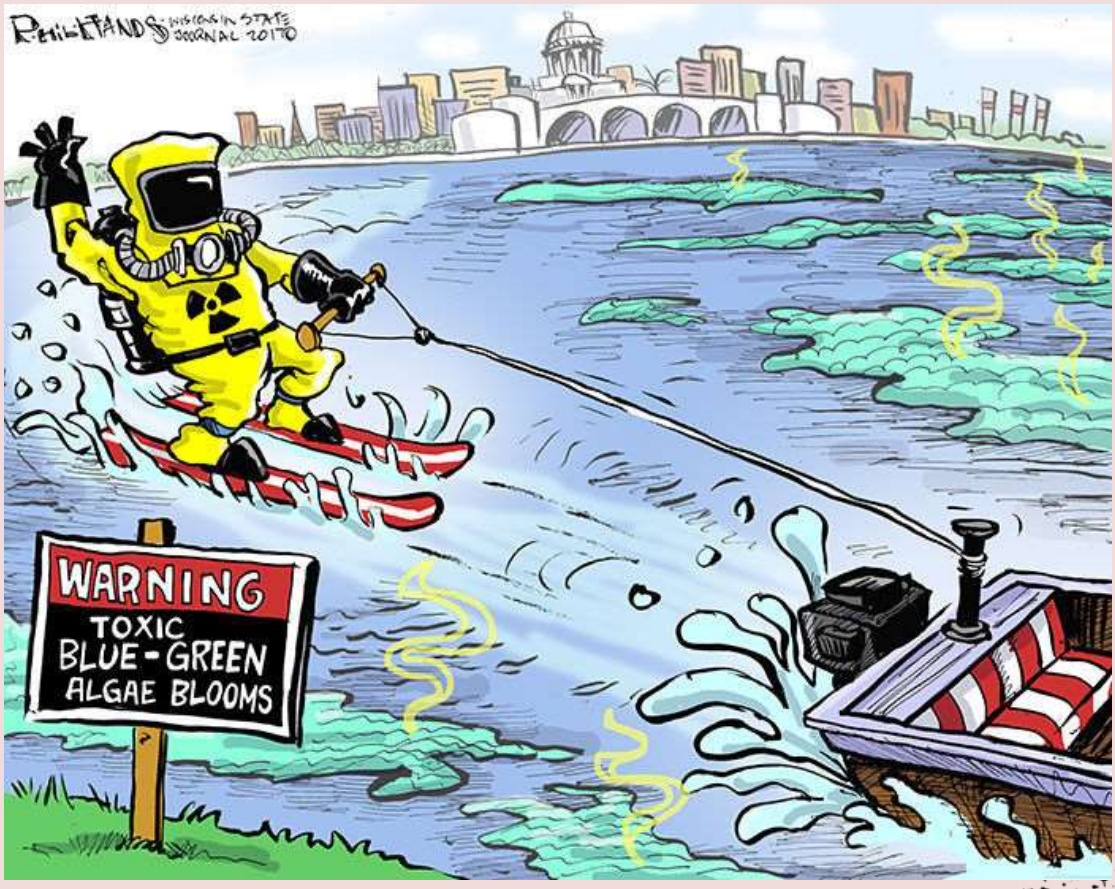
S&T notes that the three project contracts were awarded under Broad Agency Announcement HSHQDC-17-R-B0003, which was issued in December 2016. The solicitation consisted of three task areas: focusing on improving X-ray technologies for bag

screening systems, developing advanced algorithm technologies for checked and carry-on baggage, and focusing efforts to refine non-Commercial Off the Shelf long-term device technology.

The following groups and their projects are the funded BAA awards:

- ***Capture LLC, of San Diego, CA*** was awarded $1,168,773 to develop an automated threat detection algorithm for improved detection of prohibited items such as guns and knives. Capture will use a deep learning 3D convolutional neural network approach to enhance algorithm development. The goal is to deploy the automated threat recognition (ATR) algorithm on the TSA's checkpoint computed tomography (CT) systems. A new ATR will help screening efficiency and will help improve detection of threats.
- ***DxRay/Rapiscan, of Northridge, CA*** was awarded $817,444 to produce 12 large field-of-view, high-output count rate X-ray imaging arrays with high spatial and energy resolution which can operate at room temperature and be manufactured cost effectively. Developing this detector technology will help eliminate false positives in primary screening lanes by adding inline X-ray diffraction (XRD). XRD can resolve false positives, but is time consuming and expensive due to the current need for cryogenically cooled detectors to achieve the required resolution. This new technology directly addresses issues by delivering a better detector with better resolution that can be added in series to existing primary lanes.
- ***EV Products, of Saxonburg, PA*** was awarded $1,498,676 to improve high-speed coded-aperture X-ray scatter imaging (CAXSI) screening to stream-of-commerce rates. The project focuses on high-speed data acquisition and maximizing the count rate through the detector module without compromising other capabilities. This will allow X-ray machines to be more efficient, with both better detection and lower energy needs. Higher efficiency means easier detection of threats with a possibility of increased throughput.

These projects will be managed by the DHS S&T Checked Baggage Program, which supports TSA requirements to improve overall detection and false alarm performance for explosives detection system technologies.




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

Army EOD soldiers will soon get a whole new kit — and new robots

Source: https://www.armytimes.com/news/your-army/2018/08/22/army-eod-soldiers-will-soon-get-a-whole-new-kit-and-new-robots/

Arizona Army National Guard Soldiers from the 363rd Ordnance Company use a remote controlled Talon Mark II Robot to conduct an initial reconnaissance of an exploded vehicle during a training exercise. (Staff Sgt. Brian A. Barbour/Army)

Aug 22 — The explosive ordnance disposal community has played a key role in operations in recent wars, and that role will only grow as the Pentagon shifts its focus to major combat operations against near-peer threats.

With that growing role, the equipment those EOD technicians carry with them will change, too.

At the National Defense Industrial Association's annual Global EOD Symposium recently, multiple speakers focused on how the community has spent the past two decades primarily working the improvised explosive device threat. But they cautioned that old and new threats will emerge in major combat.

Repeated throughout their comments was the admonition that the community must be "full EOD, not just IED."

To meet that mission, the Army is turning to technology to help fill the gaps.

Pat McGrath, chief of the materiel development branch for Army Training and Doctrine Command's EOD concerns, laid out some of the new items in the works.

Army EOD teams will soon have three aerial drones, soldier-borne sensors, tiny "nano" helicopter drones and tethered Unmanned Aerial Sensors at their disposal.

The enhanced render safe kit will also include binocular night vision devices, lightweight dismounted X-ray machines, lightweight electronic countermeasures, and lightweight mobile detectors for radiation and chemicals.

The Army needs 176 kits and expects to have initial operational capability by 2021, McGrath said.

Beyond the immediate kit, the Army is putting a lot of resources into EOD robots.

The Enhanced Robotic Payloads-Render Safe, are new robots that can defuse or destroy explosive items, and the Army needs a bunch of them, specifically 533, in the force over the next decade.

They expect the new robot to be able to fire either eight slugs or seven "water shots," pick up 90 pounds and carry the object for 100 meters, and be able to pick up 12 pounds in the fully extended arm position.

Officials want production to begin by 2024 and be fully operational and fielded within five years.

The payloads that the robot will use will offer the most drastic difference from what current tech offers.

U.S. Soldiers assigned to the 663d Ordnance Company Explosive Ordnance Disposal (EOD), 242d Ordnance Battalion (EOD), and Officers of the Oklahoma Police Department view the operation of a TALON robot during Raven's Challenge 2018 at Camp Shelby.(Sgt. Ashley Hayes/Army)

They will combine tethered Unmanned Aerial Vehicles, use multispectral overlay cameras, be ready to provide "mesh networking" at extended ranges and do 3D mapping.

Is ISIS developing suicide CHICKENS? Pictures appear to show bombs strapped to hens by bird-brained jihadis

Source: http://www.dailymail.co.uk/news/article-3167978/Bird-brained-ISIS-jihadis-developing-suicide-chickens-strapping-homemade-bombs-hens-encouraging-wander-enemy-camps.html

July 2015 – Depraved jihadis fighting for the Islamic State in Iraq have started using chickens as mobile improvised explosive devices, it has been claimed.
Members of the terror group operating in and around the city of Fallujah are said to be strapping explosive

belts to chickens, which are then encouraged to wander into enemy camps.
Once the chickens are successfully within striking distance without having aroused suspicion, the ISIS extremists apparently use remote controls to set off the devices, killing all those close by.
Suicide chickens: ISIS jihadis operating in and around the city of Fallujah are said to be strapping the explosive belts to chickens, which are then encouraged to wander into enemy camps
Images of so-called 'suicide chickens' have been widely shared online by both pro and anti ISIS users, although their authenticity could not be verified.
Details of why the terror group are apparently using exploding birds were told to the Daily Star.
The crude devices show how ISIS is running low on ammunition following several years of all out war in Syria and Iraq, the newspaper quoted unnamed experts as saying.
'ISIS will use whatever means they can to bring death and destruction. Using animals has little military value - it is just another example of how their twisted minds enjoy dreaming up bizarre ways to kill people,' a unnamed British man fighting alongside Kurdish troops in the region added.
The bizarre claims that ISIS are using suicide chickens comes just days after reports of the terror group strapping IEDS to a goat that was sent into a Kurdish base in the Syrian city of Kobane.
Photographs of the animal IEDs emerged as the U.S.-led coalition battling ISIS dropped new leaflets over the terror group's de facto capital Raqqa, vowing to bring 'freedom' to those living there.
A Raqqa-based anti-Islamic State group and the Britain-based Syrian Observatory for Human Rights said the leaflets had drawings showing dead extremists and their flag turned upside down.

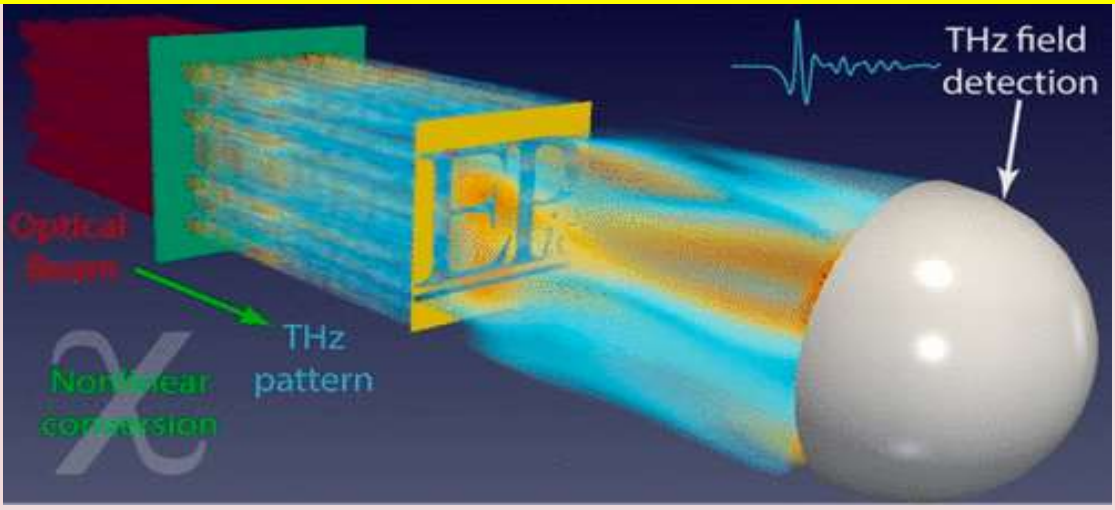
Four fighters with the main Kurdish militia, the People's Protection Units, or YPG, walked down a street in the picture, with words in Arab below: 'Freedom will come.'
The network called Raqqa is Being Silently Slaughtered posted a copy of the leaflets on its Twitter account. There was no immediate response from ISIS.
Coalition warplanes have dropped such leaflets in the past. One previous had a cartoon showing masked ISIS extremists at a 'hiring office' feeding people into a meat grinder.
ISIS holds about a third of Syria and neighboring Iraq in its self-declared 'caliphate.'
The latest leaflet drop comes as YPG fighters have been advancing in northern Syria as close as 30 miles north of Raqqa.
On Friday, a truck bombing by the group in Iraq's eastern Diyala province killed 115 people at a crowded market.
It is understood that the local police chief and three officers have been fired in the wake of the bombing. Two other officers are believed to be under investigation.

Developing new security scanners capable of detecting explosives

Source: http://www.homelandsecuritynewswire.com/dr20180831-developing-new-security-scanners-capable-of-detecting-explosives

Aug 31 – **Using a single pixel camera and Terahertz electromagnetic waves**, a team of physicists at the University of Sussex have devised a blueprint which could lead to the development of airport scanners capable of detecting explosives.
Miss Luana Olivieri, Ph.D. student and Dr. Juan Sebastian Totero Gongora, a Research Fellow in Experimental Photonics of the Emergent Photonics Lab directed by Professor Marco Peccianti and Dr. Alessia Pasquazi, have found an innovative way to capture with high accuracy, not just the shape of an object, but also its chemical composition using a special "single point" camera capable of operating at Terahertz (THz) frequencies.
Sussex says that although their work is mostly theoretical at this stage -they introduced a novel imaging concept named Nonlinear Ghost Imaging- their ability to capture a more detailed image to previous studies has landed them a prestigious front-page feature of the scientific journal, *ACS Photonics* .
Dr. Juan Sebastian Totero Gongora said: "Our approach produces a new type of image which is quite different from what you would get from a standard single-pixel camera as it provides much more information on the object. Compared to prior single pixel images, we also demonstrated that our resolution is inherently higher."
Lying between microwaves and infrared in the electromagnetic spectrum, Terahertz radiation has a much larger wavelength to visible light. It can easily penetrate several common materials like paper, clothes and plastics leading to the development of technology within security scanning and manufacture control which allows people to see inside objects and wrapping.
The radiation provokes a different response from biological samples though, allowing researchers to classify materials which are almost indistinguishable with visible light.
Scientists believe that THz waves could have enormous potential in developing critical applications such as explosives detection, medical diagnostics, quality control in manufacturing and food safety.
The challenge, however, lies in the development of reliable and cost-effective cameras as well as the ability to identify objects smaller than the wavelength.
But, by taking a different approach to previous studies in this field, the team of the Emergent Photonics Lab may have found a way to overcome these limitations.
While previous research has illuminated objects with many patterns of laser light in just one color to extract an image, the researchers illuminated an object with patterns of THz light which contain a broad spectrum of colors.
A single pixel camera (rather than a standard one containing multiple pixels as sold on the high street) can capture the light reflected by the object for each pattern. In the team's study, they found that the camera can detect how the pulse of light is altered in time by the object (even if the THz pulse is an extremely short event). By combining

this information with the known shape of the patterns, the shape of the object and its nature are revealed.



The technique may recall the way the brain develops understanding in the vision by focusing separately on different elements and then fusing the relevant information.

Professor Marco Peccianti added: "This is a really significant development and we're really happy that *ACS Photonics* decided to lead with our research on their front cover. Previous approaches to THz single-pixel cameras cannot preserve the complete information on an object but we understood where the issue lay and identified a way to extract a more complete image. We hope that a similar system to ours could be used in real-life applications in biology, medicine and security to determine the chemical composition of an object and its spatial distribution in just one step."

The team's findings are a considerable improvement on established technologies and could have a huge impact beyond the field of THz cameras. For instance, their technique could be used to design high-resolution cameras in other frequency ranges which could then become part of technology for collision sensors, body scanner or ultra-rapid radars for self-driving cars.

The researchers are now following up on their research, which is largely based on simulations, to experimentally demonstrate their device.

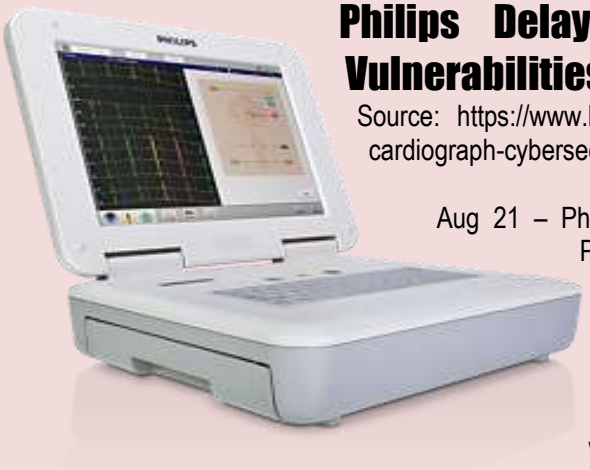
— Read more in Luana Olivieri et al., "Time-Resolved Nonlinear Ghost Imaging," ACS Photonics 5, no. 8 (3 July 2018).

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C²BRNE DIARY

CYBER NEWS



Philips Delays Fix for Cardiograph Cybersecurity Vulnerabilities

Source: https://www.hstoday.us/subject-matter-areas/cybersecurity/philips-delays-fix-for-cardiograph-cybersecurity-vulnerabilities/

Aug 21 – Philips does not intended to fix cybersecurity vulnerabilities in its PageWriter Cardiograph devices, which could allow attackers to modify settings on the devices, until mid-year 2019, according to an August 16 advisory from ICS-CERT.

The PageWriter TC10, TC20, TC30, TC50, TC70 [photo] Cardiograph devices suffer from improper input validation and use of hard-coded credentials, the advisory noted.

With the improper input validation, the PageWriter device does not sanitize data entered by user, which can lead to buffer overflow or format string vulnerabilities, the advisory noted.

Oil and gas industry 'needs to wake up to cyber threat from hostile states'

Source: https://www.independent.co.uk/news/uk/home-news/cyber-attacks-threat-oil-gas-industry-brian-lord-gchq-abu-dhabi-a8495666.html

A typical large oil and gas company uses half a million processors just for oil and gas reservoir simulation and stores petabytes of sensitive and competitive field data (Getty)

Aug 17 – The oil and gas industry should brace itself for the increased risk of cyber attacks from hostile states, the former Deputy Director of GCHQ has warned.

Brian Lord OBE said a successful attack on its infrastructure could cause “unprecedented damage” and “unrest across the world”.

With a complex ecosystem of computation, networking, and physical operational processes spread around the world, the industry has a large attack surface with many attack vectors.
A typical large oil and gas company uses half a million processors just for oil and gas reservoir simulation and stores petabytes of sensitive and competitive field data.
The topic will be high on the agenda for industry leaders at an upcoming meeting in Abu Dhabi.
Mr Lord said: "The oil and gas industry is the second most susceptible to cyber attacks, with the potential to cause unprecedented damage and unrest across the world.
"The primary cyber threat to oil and gas infrastructure comes from hostile states who are developing disruptive capabilities in order to deliver power projection for their own long-term geopolitical and politico-military ends."
Mr Lord added: "If they are not taken now, hostile actors will continue to virtually roam freely and unchallenged around oil and gas infrastructures, achieving a greater understanding of how to deliver future attacks at will.
"As it digitalises its workforce to keep up with increasing demand, it is clear that the industry will continue to be a target for such actors."

How Hacked Water Heaters Could Trigger Mass Blackouts

Source: https://www.wired.com/story/water-heaters-power-grid-hack-blackout/

Aug 13 – When the cybersecurity industry warns about the nightmare of hackers causing blackouts, the scenario they describe typically entails an elite team of hackers breaking into the inner sanctum of a power utility to start flipping switches. But one group of researchers has imagined how an entire power grid could be taken down by hacking a less centralized and protected class of targets: home air conditioners and water heaters. Lots of them.

At the Usenix Security conference this week, a group of Princeton University security researchers will present a study that considers a little-examined question in power grid cybersecurity: What if hackers attacked not the supply side of the power grid, but the demand side? In a series of simulations, the researchers imagined what might happen if hackers controlled a botnet composed of thousands of silently hacked consumer internet of things devices, particularly power-hungry ones like air conditioners, water heaters, and space heaters. Then they ran a series of software simulations to see how many of those devices an attacker would need to simultaneously hijack to disrupt the stability of the power grid.

Just a one percent bump in demand might be enough to take down the majority of the grid.

Their answers point to a disturbing, if not quite yet practical scenario: In a power network large enough to serve an area of 38 million people—a population roughly equal to Canada or California—the researchers estimate that just a one percent bump in demand might be enough to take down the majority of the grid. That demand increase could be created by a botnet as small as a few tens of thousands of hacked electric water heaters or a couple hundred thousand air conditioners.
"Power grids are stable as long as supply is equal to demand," says Saleh Soltan, a researcher in Princeton's Department of Electrical Engineering, who led the study. "If you have a very large botnet of IoT devices, you can really manipulate the demand, changing it abruptly, any time you want."

The result of that botnet-induced imbalance, Soltan says, could be cascading blackouts. When demand in one part of the grid rapidly increases, it can overload the current on certain power lines, damaging them or more likely triggering devices called protective relays, which turn off the power when they sense dangerous conditions. Switching off those lines puts more load on the remaining ones, potentially leading to a chain reaction.

"Fewer lines need to carry the same flows and they get overloaded, so then the next one will be disconnected and the next one," says Soltan. "In the worst case, most or all of them are disconnected, and you have a blackout in most of your grid."

Power utility engineers, of course, expertly forecast fluctuations in electric demand on a daily basis. They plan for everything from heat waves that predictably cause spikes in air conditioner usage to the moment at the end of British soap opera episodes when hundreds of thousands of viewers all switch on their tea kettles. But the Princeton researchers' study suggests that hackers could make those demand spikes not only unpredictable, but maliciously timed.

The researchers don't actually point to any vulnerabilities in specific household devices, or suggest how exactly they might be hacked. Instead, they start from the premise that a large number of those devices could somehow be compromised and silently controlled by a hacker. That's arguably a realistic assumption, given the myriad vulnerabilities other security researchers and hackers have found in the internet of things. One talk at the Kaspersky Analyst Summit in 2016 described security flaws in air conditioners that could be used to pull off the sort of grid disturbance that the Princeton researchers describe. And real-world malicious hackers have compromised everything from refrigerators to fish tanks.

Given that assumption, the researchers ran simulations in power grid software MATPOWER and Power World to determine what sort of botnet would could disrupt what size grid. They ran most of their simulations on models of the Polish power grid from 2004 and 2008, a rare country-sized electrical system whose architecture is described in publicly available records. They found they could cause a cascading blackout of 86 percent of the power lines in the 2008 Poland grid model with just a one percent increase in demand. That would require the equivalent of 210,000 hacked air conditioners, or 42,000 electric water heaters.

The notion of an internet of things botnet large enough to pull off one of those attacks isn't entirely farfetched. The Princeton researchers point to the Mirai botnet of 600,000 hacked IoT devices, including security cameras and home routers. That zombie horde hit DNS provider Dyn with an unprecedented denial of service attack in late 2016, taking down a broad collection of websites.

Building a botnet of the same size out of more power-hungry IoT devices is probably impossible today, says Ben Miller, a former cybersecurity engineer at electric utility Constellation Energy and now the director of the threat operations center at industrial security firm Dragos. There simply aren't enough high-power smart devices in homes, he says, especially since the entire botnet would have to be within the geographic area of the target electrical grid, not distributed across the world like the Mirai botnet.

But as internet-connected air conditioners, heaters, and the smart thermostats that control them increasingly show up in homes for convenience and efficiency, a demand-based attack like the one the Princeton researchers describes could become more practical than one that targets grid operators. "It's as simple as running a botnet. When a botnet is successful, it can scale by itself. That makes the attack easier," Miller says. "It's really hard to attack all the generation sites on a grid all at once. But with a botnet you could attack all these end user devices at once and have some sort of impact."

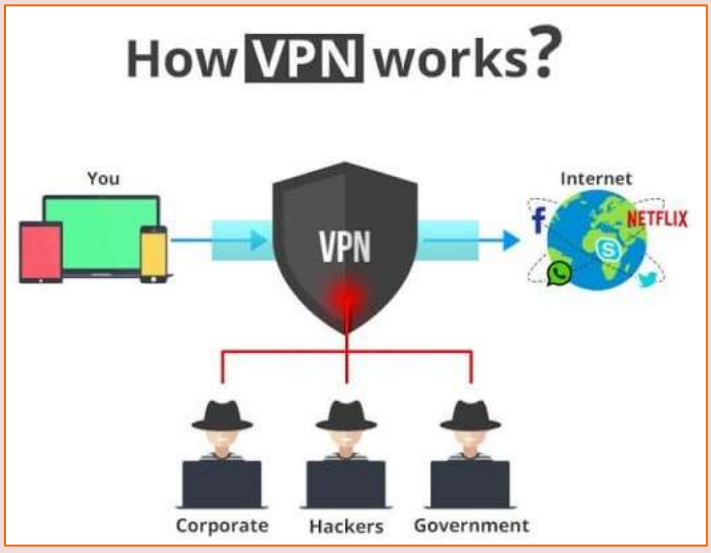
The Princeton researchers modeled more devious techniques their imaginary IoT botnet might use to mess with power grids, too. They found it was possible to increase demand in one area while decreasing it in another, so that the total load on a system's generators remains constant while the attack overloads certain lines. That could make it even harder for utility operators to figure out the source of the disruption. If a botnet did succeed in taking down a grid, the researchers' models showed it would be even easier to *keep* it down as operators attempted to bring it back online, triggering smaller scale versions of their attack in the sections or "islands" of the grid that recover first. And smaller scale attacks could force utility operators to pay for expensive backup power supplies, even if they fall short of causing actual blackouts. And the researchers point out that since the source of the demand spikes would be largely hidden from utilities, attackers could simply try them again and again, experimenting until they had the desired effect. The owners of the actual air conditioners and water heaters might notice that their equipment was suddenly behaving strangely. But that still wouldn't immediately be apparent to the target energy utility. "Where do the consumers report it?" asks Princeton's Soltan. "They don't report it to Con Edison, they report it to the manufacturer of the smart device. But the real impact is on the power system that doesn't have any of this data."

That disconnect represents the root of the security vulnerability that utility operators need to fix, Soltan argues. Just as utilities carefully model heat waves and British tea times and keep a stock of energy in reserve to cover those demands, they now need to account for the number of potentially hackable high-powered devices on their grids, too. As high-power smart-home gadgets multiply, the consequences of IoT insecurity could someday be more than just a haywire thermostat, but entire portions of a country going dark.

VPN – What is It and Why Do Armed Forces Use It?

Source: https://i-hls.com/archives/85002

Aug 22 – VPN, or virtual private network, is a term we hear more and more. This is understandable if you take into consideration the many varied benefits of using one. Not only does it keep your personal data safe, VPNs provide a secure path to the Internet that keeps others from tracking your usage, prevent the recording of your connection's IP address, and can even "trick" networks into thinking you're connecting from a country other than the one you're actually located in at the time.



According to vpnmentor.com, a VPN has three main components to it: **security protocols, encryption** and **servers**. VPNs use a **security protocol** that protects any information that passes through the server. This protocol creates a secure connection and also influences the type of encryption the VPN uses.

Encryption goes hand in hand with the security protocol. This feature guards your data by encrypting it. So, even if a hacker or someone else gets a hold of your data, they won't be able to decipher it.

And finally, When you use a VPN, your data first goes to the VPN's **server**, and then the VPN sends it to the intended server. When you ping a server for a website, you constantly send data back and forth over that connection. If you insert a VPN in the middle, your request for the website goes to the server, but your data only moves between your device and the VPNs server which is an encrypted tunnel. Therefore, the

intended server does not receive any of your information.This is how VPN users remain anonymous online and also how VPNs can change your location to unblock certain websites.
Anyone can benefit from using a VPN, whether it is to access content outside of your territory, protect your private information, or get access to cheap airfares.
Businesses use VPNs to connect remote data centers, and individuals can use VPNs to get access to network resources when they're not physically on the same LAN (local area network), or as a method for securing and encrypting their communications when they're using an untrusted public network.
All of those are great reasons for anyone to use a VPN, but this type of tool is especially handy for military personnel. According to privatewifi.com, whether it's trying to watch Netflix from a foreign deployment base or forwarding a secure communication from a local national contact, a VPN can offer another layer of protection that soldiers can appreciate, no matter what type of connectivity work they're doing.
Some of the best reasons for active duty military members to employ a VPN can include signing into sensitive accounts, especially while deployed to a foreign country, relaying sensitive communications to other soldiers or officials in the chain of command, especially with regards to the names or locations of contacts, checkpoints, or while submitting other detailed notifications.
It should be noted that there are military-specific VPN's and that their functions may be somewhat different than those offered to everyday citizens. A specific VPN assigned for military use and communications may be monitored and archived for later evaluation and does not offer the same types of privacy that the civilian public has, this is to help the armed forces ensure mission readiness and security.
Whether it's to keep others from prying into your Internet activities or to enable the legitimate use of websites that other countries censor, a VPN keeps your online behaviors private and your network use easy and efficient.

Germany creates cybersecurity R&D agency

Source: http://www.homelandsecuritynewswire.com/dr20180829-germany-creates-cybersecurity-r-d-agency

Aug 29 – The German government today (Wednesday) announced the creation of a new federal agency to develop cutting-edge cyber defense technology.
Some lawmakers have expressed their unease with the new agency, which, they said, may also develop state-of-the-art cyber offensive capabilities.
German Defense Minister Ursula von der Leyen said the agency would allow Germany to invest in new technologies and in the protection of critical digital infrastructure. She added that the agency would also partner with other EU countries on agency projects.
DW reports that the federal agency will be managed by the Ministry of Defense and the Ministry of the Interior.
The agency would resemble the U.S. Defense Advanced Research Projects Agency (DARPA), which is credited with developing the early internet and GPS, von der Leyen said.
The German agency, unlike DARPA, will focus on cyber defense ad cyber protection. DARPA's range of defense-related research and development is much broader.
Some lawmakers have expressed their concerns about the new agency.
Anke Domscheit-Berg, digital policy spokeswoman for the Left Party, told DW that while Germany needs to do more to protect digital infrastructure, she doubts the agency's mandate is the best way to do it.
"More digital security would definitely do us all good, and if the new cyber agency does that, it would be a step forward," Domscheit-Berg said. "We need better encryption and more open source software, but I'm skeptical an agency located somewhere between the Defense Ministry and the Interior Ministry is setting the right priority."
Green Party spokesman Konstantin von Notz took it further, arguing that such an agency works against the Foreign Ministry's work.
"The agency would massively undermine the Foreign Ministry's efforts at the UN to outlaw cyber weapons," von Notz told DW. "Instead of promoting a spiraling escalation in the digital space, the government needs to make a U-turn on IT security."
The issue of military-led and cyberwarfare has been a contentious topic in Germany, and some German lawmakers have questioned whether the Bundeswehr should have the

capability to launch offensive cyberattacks.
But von der Leyen noted that the same rules that apply to Germany in the "analogue world will also apply to the virtual one."
Providing new data on thyroid cancer, the white paper acknowledges that this form of the disease is the major health issue (in individuals who were children or adolescents at the time of the accident) and that further investigation is needed to determine the long-term consequences of radiation exposure.
Previous studies have shown that there were no global consequences of the accident in Asia and North America, which remains true today.

The Rise of the Cyber-Mercenaries

By Neri Zilber
Source: https://foreignpolicy.com/2018/08/31/the-rise-of-the-cyber-mercenaries-israel-nso/

Aug 31 – The first text message showed up on Ahmed Mansoor's phone at 9:38 on a sweltering August morning in 2016. "New secrets about torture of Emiratis in state prisons," it read, somewhat cryptically, in Arabic. A hyperlink followed the words. Something about the number and the message, and a similar one he received the next day, seemed off to Mansoor, a well-known human rights activist in the United Arab Emirates. He resisted the impulse to click on the links.

Instead, Mansoor sent the notes to Citizen Lab, a research institute based at the University of Toronto specializing in human rights and internet security. Working backward, researchers there identified the hyperlinks as part of a sophisticated spyware program built specifically to target Mansoor. Had he clicked on the links, the program would have turned his phone into a "digital spy in his pocket," Citizen Lab later wrote in a report—tracking his movements, monitoring his messages, and taking control of his camera and microphone.
But the big revelation in the report wasn't so much the technology itself; intelligence agencies in advanced countries have developed and deployed spyware around the world. What stood out was that Citizen Lab had traced the program to a private firm: the mysterious Israeli NSO Group. (The name is formed from the first initials of the company's three founders.) Somehow, this relatively small company had managed to find a vulnerability in iPhones, considered to be among the world's most secure cellular devices, and had developed a program to exploit it—a hugely expensive and time-consuming process. "We are not aware of any previous instance of an iPhone remote

jailbreak used in the wild as part of a targeted attack campaign," the Citizen Lab researchers wrote in their report.

Israel is a world leader in private cybertechnology, with at least 300 firms covering everything from banking security to critical infrastructure defense. But while most of these firms aim to protect companies from cyberattacks, a few of them have taken advantage of the thin line between defensive and offensive cybercapabilities to provide clients with more sinister services. In the case of Mansoor, the UAE is believed to have deployed NSO tools to conduct surveillance on the country's most famous dissident. (He is now serving a 10-year prison sentence for publishing "false information" on his social media accounts.) "[T]hese companies apply techniques as sophisticated, or perhaps sometimes more sophisticated, than U.S. intelligence agencies," Sasha Romanosky, a policy researcher at the Rand Corp., wrote last year.

The privatization of this offensive capability is still in its infancy. But it raises broad concerns about the proliferation of some very powerful tools and the way governments are losing the monopoly over their use. When state actors employ cyberweapons, there is at least the prospect of regulation and accountability. But when private companies are involved, things get more complicated. Israel offers a good test case. It produces a steady supply of highly skilled cyberoperators who learn the craft during their military service in one of the country's elite signals intelligence units—Unit 8200 is the best known among them—and then go on to work in the private sector. Nadav Zafrir, a retired brigadier general and former commander of Unit 8200, said even soldiers who spend their service defending Israel from cyberattacks end up knowing something about how to attack the other side. "In order to mitigate the gap between defense and offense, you have to have an attacker's mindset," he said.

The Mansoor case was not an isolated one. Up to 175 people have been targeted by the NSO Group's spyware since 2016, according to Citizen Lab, including human rights workers and dissidents. Other Israeli firms offer similar products. "There's no way around it: In order to provide network defense, you need to map vulnerabilities," said Nimrod Koz-lovski, an adjunct professor at Tel Aviv University and a lawyer specializing in cybersecurity. "It's built from [Israel's] deep knowledge of these weaknesses and attack methods. We're deeply familiar with what targets look like."

Take the most famous of these alleged targets: Iran's uranium enrichment facility at Natanz, where Unit 8200, in collaboration with the U.S. National Security Agency (NSA), reportedly carried out an attack in 2009-2010. They were apparently able to introduce a computer virus—called Stuxnet—into the facility despite it having an air gap in place, meaning that the facility was physically disconnected from the wider internet. The virus targeted the operating system for Natanz's uranium centrifuges, causing them to speed up wildly and break; the monitoring system was also apparently hacked so that the damage, when it happened, initially went unnoticed by the Iranians.

It's probably no coincidence that many Israeli cyberdefense firms market products aimed at forestalling Stuxnet-style attacks on critical infrastructure. These firms include Aperio Systems, which is headed by a former intelligence officer named Liran Tancman. Aperio, in fact, has a product that detects data manipulation—a "truth machine," as Tancman puts it—in sensor readings at industrial plants.

Stuxnet is name-checked repeatedly by experts in the field and with good reason: It was a highly successful cyberattack against a state actor that caused real physical damage. Yet Stuxnet may already be outdated as an analytical touchstone. As Gabriel Avner, an Israel-based digital security consultant, said, "A decade in tech is an eternity." These days, the attack surface is growing, said Zafrir, the former Unit 8200 commander who now runs Team8, a combination venture capital fund, incubator, and ideas lab. The development that worries him and other experts most is the proliferation of the internet of things. "Everything is becoming a computer—your phone, your fridge, your microwave, your car," said Bruce Schneier, an expert on cyber-related issues at Harvard University. The problem is that the internet, which came of age in the 1970s and 1980s, was never designed with security in mind. So everyone is now scrambling to play catch-up, patching holes in both information systems (e.g., software programs) and operating systems (e.g., physical industrial plants) that are outdated, poorly written, or simply insecure. "Attacks always get faster, easier, and better," added Schneier, the author of *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World*.

Does this mean we're all doomed?

The short answer is no—at least, probably not. Thus far, apart from Stuxnet, the most successful reported instances of a cyberattack causing widespread physical damage have

taken place in Ukraine and Estonia. Although these attacks—against power grids, financial institutions, and government ministries—caused real harm, they were nevertheless identified and rectified relatively quickly. None of the doomsday scenarios that experts and pundits like to warn about—such as hackers seizing control of a nuclear weapon or a commercial airliner or malware causing Wall Street to collapse—has materialized.

Part of the explanation is that "state-sponsored hackers will always have more resources," Tancman said. "The question is how far ahead of the [nonstate actors] you're running. A 'cyber-nuke weapon' today won't be relevant in a year or two. The issue is the pace of development between attackers and defenders. Always keep running."

If part of the danger comes from the blurriness of the line that separates cyberdefense and cyberoffense, another part comes from the almost nonexistent distinction between the private and public spheres online. In July, for example, Israeli authorities announced multiple indictments against a former employee of NSO Group, alleging that he had stolen sensitive proprietary code on his way out of the firm. But the unnamed employee was also charged with attempting to undermine national security: He had apparently tried to sell the information for $50 million in cryptocurrency to a foreign buyer on the darknet, the vast anonymous hinterland of the internet inaccessible by regular search engines.

This incident, quickly detected by the firm, is just one case among many that shows how intimately the private and public spheres are linked in cyberwarfare. Capabilities that were once the sole province of governments frequently find their way into private—often criminal—hands.

The Stuxnet virus code is now publicly available. In 2013, a cyberweapon developed by the NSA that exploited vulnerabilities in Microsoft Windows was stolen by hackers—possibly Russian—and posted online; in May 2017, other hackers—possibly North Korean—then used the tool to launch a worldwide ransomware attack. The attack, called WannaCry, is believed to have infected 200,000 computers in more than 150 countries, including major parts of the British National Health Service, before it was rolled back. In a separate 2013 case, Mandiant, a private U.S. cybersecurity firm, proved that hackers affiliated with the Chinese military were targeting U.S. corporations and government agencies. And in 2015, Unit 8200 reportedly hacked into Kaspersky Lab, a global leader in anti-virus software, and discovered that the private company had been acting as a back door for Russian intelligence into its clients, including two dozen U.S. government agencies.

"In the physical world of warfare, what is public has always been clear: tanks, Iron Dome [missile defense systems], F-16s," said Rami Ben Efraim, a retired Israeli brigadier general and the founder of BlueOcean Technologies, an offensive cybersecurity firm. "In cyber today, it's complicated." Critical infrastructure, such as power utilities or water treatment plants, may be privately owned, as is often the case in the United States, but would cause national damage if its systems crashed. Mobilization messages for Israeli reserve forces in wartime go through privately held telecom networks. And the internet of things—which has connected so many of our consumer products—has also created massive vulnerabilities.

"If you want to take down a plane, if you want to ground air power, you don't go through the front door, the cockpit," said Ben Efraim, a former fighter pilot. "You go after the airport. … You go after the logistics systems. You go after the iPads the pilots take home." There are no "stand-alone entities anymore—everything is part of a network," Ben Efraim added. As Lithuania's vice minister of defense, Edvinas Kerza, told me last fall in the capital of Vilnius, alluding to Russia's actions against other former Soviet states: "The attacks come from within—banks down, government not responsive, general instability. … 'It's fine to set up a border,' they say. 'We'll come from the inside.'"

Israel, for one, has chosen to combat the problem on a statewide level by linking the public and private spheres, sometimes literally. The country's cyberhub in the southern city of Beersheba is home not just to the Israeli military's new technology campus but also to a high-tech corporate park, Ben-Gurion University of the Negev's cyber-research center, and the Israel National Cyber Directorate, which reports directly to the prime minister's office. "There's a bridge between them—physically," Avner, the security consultant, said by way of emphasis.

In a world where Israel's vaunted internal security agency, the Shin Bet, recently launched a private start-up accelerator, such private-public collaboration will only grow. Indeed, it must if it is to keep up with rapid developments in areas such as artificial intelligence, machine learning, and other breakthroughs in computational power.

Cyberwar has not only blurred the lines between offense and defense; it has also blurred the notion of sovereign property when it comes to technological development—namely what, exactly, constitutes an Israeli (or U.S. or Chinese) company. The internet has eclipsed borders, and cyberwarfare is no exception. As Harvard's Schneier put it, the "chips are made in X, assembled in Y, and the software is written all over the world by 125 different nationals." Such fluidity is especially common in Israel, where deep-pocketed foreign firms have established research and development outposts and bought up local start-ups.

While the international nature of computer technology confers many benefits, it also makes it hard to ascertain the origin of a cyberattack. That lack of attribution then makes it harder for governments to respond, and the lack of a threat of reprisal makes deterrence difficult, if not impossible. "That is why cyberweapons have emerged as such effective tools for states of all sizes: a way to disrupt and exercise power or influence without starting a shooting war," David Sanger wrote in a *New York Times* article adapted from his book *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*.

While the private sector may be able to pay its people more, drawing talent—and technological prowess—away from public service, the government still holds one trump card: the law. Which brings us back to the NSO Group and Mansoor, the Emirati dissident. In order to legally sell the offensive cyberweapon used to target him, NSO would have needed permission from Israel's weapons export regulator, which sits in the Defense Ministry. In this way at least, cyberweapons are as tightly regulated as other weapons systems sold by the Israelis to foreign governments. And the clients are solely governments.

"Selling such systems to nongovernments, like a company or oligarch, is completely illegal," said Yuval Sasson, a partner specializing in defense exports at Meitar, one of Israel's leading law firms. "Just like with a drone or assault rifle, the regulator looks at the end user: the identity of the government and what it does. Functionality is a central test." In the case of the UAE and Mansoor, some officials within the regulator's office counseled against selling such a system to an Arab state, according to the Israeli daily *Yedioth Ahronoth*. It reported that the cyberweapon the regulators ultimately approved was weaker than the one proposed by NSO and said some officials in the Defense Ministry opposed the deal because the technology was being sold to an Arab country. "It's a scandal that they gave a permit like this," the newspaper quoted a senior official at the ministry as saying.

NSO, for its part, said in a statement that it complies with all relevant laws and that it "does not operate the software for its clients, it just develops it." That is a disingenuous distinction, perhaps, but it offers another example of the offense-defense and private-public conundrums: The same private cybertools deployed against perceived enemies of the state, such as journalists and dissidents, can be, and are, used to interdict narcos and terrorists as well. Indeed, in 2016 the FBI hired a separate Israeli firm, Cellebrite, to break into the iPhone of one of the terrorists involved in the 2015 San Bernardino, California, attack with a different cybertool (after Apple refused). Cellebrite reportedly sells its products in more than 100 countries.

While some critics blame Israel for rogue behavior, the country is no outlier; there are few saints in the global weapons trade, even among Western democracies. It is in the interest of Israeli firms to comply with the law, avoid abuses, and prevent technology from falling into the wrong hands. As Avner put it, "There's a lot of money to be made, and they can do it legally. Why be in the shadows?"

The upshot is that NSO wasn't operating in the shadows. The Israeli government approved the sale by a private company of an advanced cyberweapon to an Arab government with which it has intelligence and security exchanges. That decision was symbolic of how technology, warfare, and politics have changed dramatically in just a few short years. Espionage, information operations, and military attacks have been with us forever; so have private actors selling weapons all around the world (including, in recent decades, many former Israeli military personnel). The difference now is the reach and speed of these new cybertools and their easy proliferation. A "cyberarms race of historic but hidden proportions has taken off," according to Sanger—and the race is global. The potential downside is obvious: an arms race with no rules or norms and with no clear front lines. But there is no going back.

"We need to be humble. We're only starting to understand it," Ben Efraim said. "But it's a real revolution. A hundred years ago, there was no air element to warfare. Now it's a critical component of any military."

"Cyber is bigger than even that," he said. "Today, you open your eyes in the morning—you're in it."

Neri Zilber is a journalist and analyst on Middle East politics and culture and an adjunct fellow of the Washington Institute for Near East Policy. He is the co-author, most recently, of State with No Army, Army with No State: Evolution of the Palestinian Authority Security Forces, 1994-2018.

Can new regulations in the EU, U.S. help combat cyber terrorism?

Source: https://www.jpost.com/Jpost-Tech/Can-new-regulations-in-the-EU-US-help-combat-cyber-terrorism-567214

Sept 14 – There were two major developments this week in the EU and US's ongoing battle against terrorists use of social media, one of which unexpectedly also relates to using weapons of mass destruction.

The first was the European Commission's release on Wednesday of proposed new binding rules that would require social media platforms to remove illegal terrorist content within an hour of national authorities flagging it.

This comes after Germany successfully implemented a similar one-hour rule earlier in 2018.

Those that fail to comply could be fined billions of dollars based on 4% of global annual revenue.

That penalty is the same big-time threat that the EU unsheathed in May to enforce its new privacy rules with social media.

Twitter, Google and Facebook have been working with the EU voluntarily in recent years on the issue.

However, the EU Commission's new move toward binding rules after multiple rounds of escalating non-binding guidelines, implies that more needs to be done and by using a blunt stick.

Around 700 new pieces of ISIS propaganda were disseminated online in January 2018 alone, said the commission.

Moreover, online platforms will need to have direct lines open on a constant basis between law enforcement and decision- makers so that there can be fast responses.

Social media is also being encouraged to use more automated artificial intelligence algorithms to identify and delete certain suspicious users.

Of course, the real test will be whether the fines will be enforced.

To date, Germany has not issued a major fine and the EU has not finalized major fines relating to its new privacy rules – though privacy rules allow for private lawsuits, which have been filed.

Still, it continues the sea change in the EU's attitude toward terrorism on social media after some years of criticizing Israel for cracking down on online platforms.

Until recently, social media platforms could argue that they were not responsible for content posted by third-parties.

The new rules make them responsible and with a loaded (from an economics perspective) gun.

The second development was the publishing of a ground-breaking report by the James Martin Center for Nonproliferation Studies about "weaponizing social media to muddy the WMD waters."

Discussing Russia's cyber influence operation of the 2016 US election is common.

But the idea that states, most likely Russia, now regularly uses social media on a grand scale to influence US political debate on issues like intervention in Syria following the use of chemical weapons, is eye-opening.

The report said that "synthetic actors" (bots, trolls, and cyborgs, which masquerade under false pretenses to accomplish a political goal) on social media are "likely the main driving force behind shaping the character of the counter-narrative discussion surrounding the use of chemical weapons in Syria."

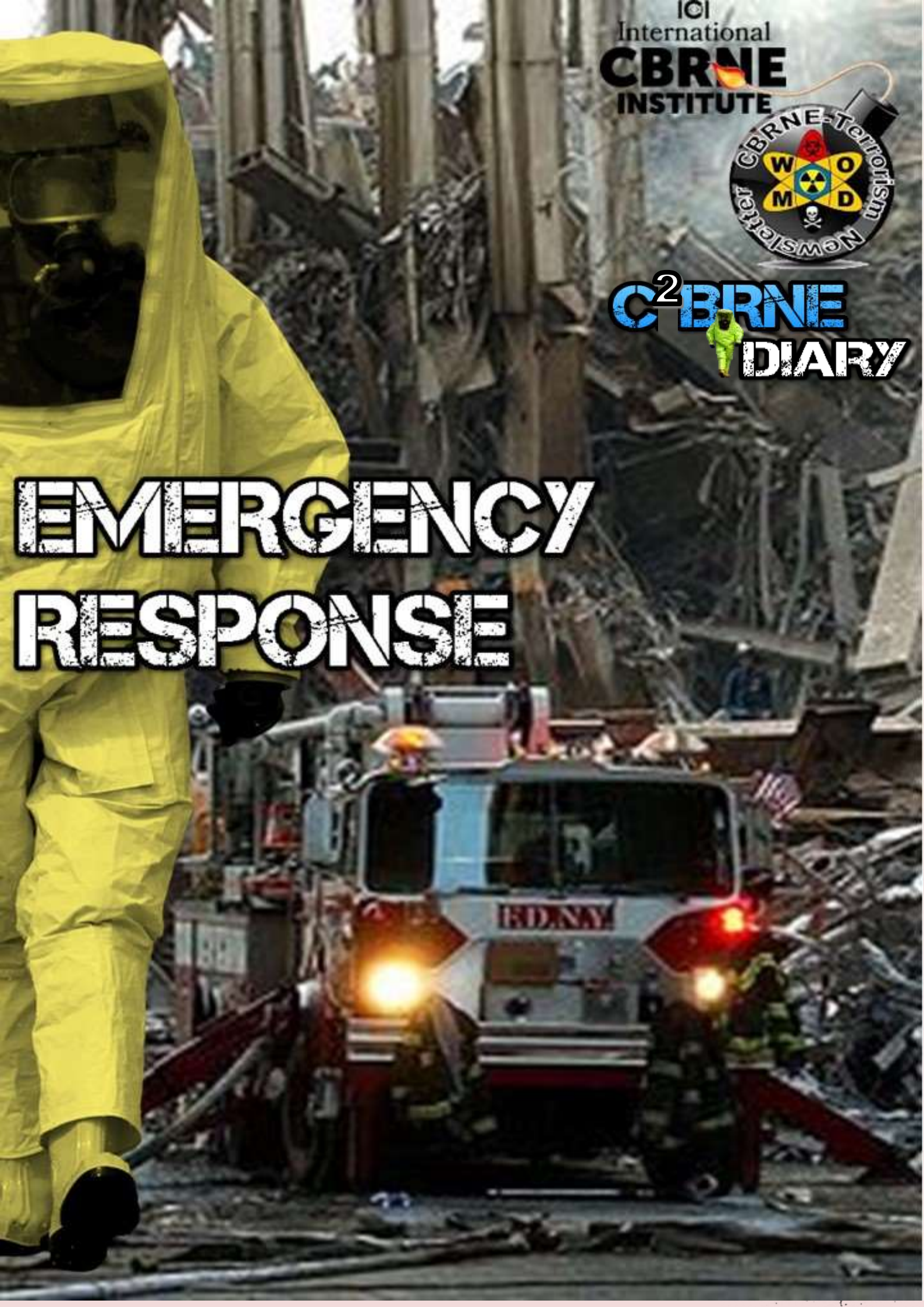
Analyzing the trade craft and possible effects of disinformation produced by suspected synthetic actors on Twitter concerning chemical weapons use in Syria, the report found that a staggering 16% to 20%, of all Twitter counter-narrative messaging is likely disseminated by Russia.

A network of highly message- disciplined synthetic actors was activated following the April 7, 2018, chemical attack in Douma, Syria.

After the messaging attempt "failed," when the Trump administration intervened, many counter-narrative accounts went inactive, bolstering the report's ability to identify them as synthetic actors.

Fascinatingly, the most common procedural tactic employed by these users was threatening not to vote for Trump again.

The idea was that this tactic would disarm Trump supporters into being open to someone who seems like a struggling supporter like them.
The report listed four other main tactics: 1) defaming Western institutions to discredit their claims about Syrian use of chemical weapons; 2) blaming jihadists for the attacks; 3) hinting that a destructive (often nuclear) escalation would result from a Western retaliatory strike; and 4) preying on Western religious and cultural sympathies for supposedly besieged Syrian Christians and the secular Bashar Assad regime.
Probably the most important recommendation from the report is that "social networks… take care to scrutinize accounts that were created immediately after controversial events if the accounts only engage in discussion about that event," such as Syria's use of chemical weapons.
The simplest step social networks can take, said the report, is to ban scripted bot accounts which can be distinguished from organic accounts "in that their fully automated content typically consists of large, abnormal degrees of repetition." Twitter can likely detect this using metadata analysis.
It said that Twitter has already started this process, claiming to have banned 70 million accounts in the first half of 2018, but that Twitter had missed active bots.
The report also encouraged Twitter to institute a verification system, which could alert other users to questionable accounts.
Unlike the EU's rules, however, these are just suggestions from a think tank.
Social media giants have shown that at the end of the day, they are ready to tackle terrorists and state manipulations of their platforms only up until a point.
Getting beyond that point, like in most areas of business, requires a stick.
Maybe curtailing influence operations will be included in a later round of rules.


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

The Hajj Is a Perfect Laboratory for Disease Warning Systems

By Maryn McKenna

Source: https://www.wired.com/story/hajj-who-early-disease-warning-system/

Aug 23 – Right now, one of the world's largest mass gatherings is taking place in the desert of Saudi Arabia. The hajj, the yearly pilgrimage to Islam's holiest sites, is required of every observant Muslim who can perform it. More than 2 million people have poured into the country, over land, by air, and in massive charter deployments, from essentially every place around the globe where Muslims reside.

Anywhere there are massive crowds in limited space, disease is likely to spread—and so it has at the hajj, everything from minor respiratory infections to polio. This year, though, a layer of protection has been built into the pilgrimage that never existed before: an electronic early-warning system, created with the help of the World Health Organization, that will sound an alarm at the first signal of any kind of outbreak. (Friday is the hajj's last day, and in a piece of good news, no alarm has rung yet.)

Syndromic surveillance systems, as they're called, aren't perfect; they've rung false alarms before. But Saudi Arabia's willingness to create one doesn't just signal an awareness of disease risks. It also indicates new transparency from a government that has been less than forthcoming about diseases in the past. If that transparency continues, it could create a rich data source for public health officials to predict the risks of gatherings to come.

The hajj is an extraordinarily complex logistical undertaking that happens to take place out of sight of most of the world; participation, and entry to the holy sites, is limited to Muslims. The millions who attend arrive over the course of weeks, but they converge in one jostling five-day trek that covers almost 30 miles, looping from the Grand Mosque of Mecca through a massive tent city to the slopes of Mount Ararat and back. Vehicle traffic on parts of the route so often comes to a standstill that many walk. The heat can be brutal—temperatures this week rose to 110 degrees Fahrenheit—and the crowds are so tightly packed that pilgrims periodically have been crushed to death in surges.

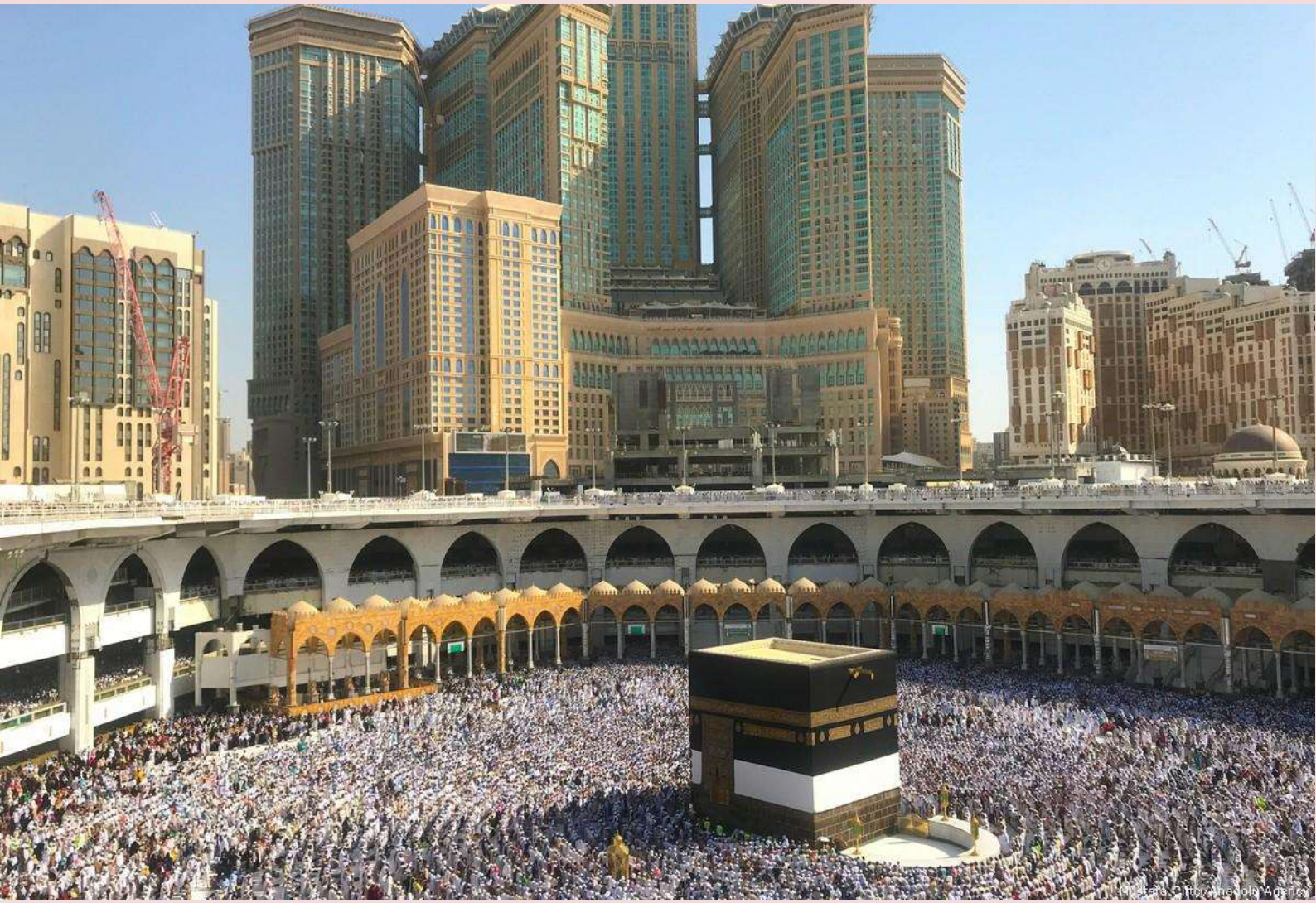
Dehydration, exhaustion, close quarters, shared food and razors, and skin-to-skin contact—the ritual garments for men, called *ihram*, leave part of the upper body exposed—all open the door to disease transmission. There have been outbreaks of meningococcal disease, gastrointestinal illnesses, pneumonia, and flu (the dates of the hajj move because it is scheduled according to the lunar calendar, so it sometimes falls in flu season).

To protect the pilgrims, the Saudi Ministry of Health requires vaccination against specific diseases: against meningitis and flu for everyone arriving, and against yellow fever and polio

if they come from areas where those diseases have occurred recently. It also asks especially vulnerable people—pregnant women, young children, those with serious illnesses—not to make the trip.

Pilgrims seem to be complying: This year, according to ministry statistics, the network of field hospitals and clinics it throws up for the hajj season has found 96 percent were vaccinated against yellow fever, 87.5 percent had received the polio vaccine, and 80 percent had been vaccinated against meningitis.

The Saudi Ministry of Health already tries to run illness-monitoring efforts, but there's no guarantee that they'll move fast enough to catch an outbreak.



The ministry knows about pilgrims' vaccination status because it already tries to run illness-monitoring efforts in the pilgrimage area. But there's no guarantee that they'll move fast enough to catch an outbreak. Some diseases can slip past detection—and epidemiologists have long been worried about the hajj giving a boost to rare diseases especially. In 2005, for instance, a case of polio in Indonesia was was found to be caused by a strain from the horn of Africa that may have transited through Saudi Arabia via an unknowing pilgrim. Genomic evidence shows that mosquito-borne dengue virus has been imported into the kingdom multiple times over decades.

And five years ago, the Saudi government came under close scrutiny when international health authorities felt it was not being open about the risks of MERS, a respiratory virus with a high mortality rate that was first found in that country in 2012. (A multi-hospital outbreak of MERS in South Korea in 2015 began with a traveler returning from Saudi Arabia—though that outbreak began several months before that year's hajj season.)

Because of the millions who come on hajj and related pilgrimages, Saudi Arabia is "a mixing bowl for emerging infections," says Peter Jay Hotez, who made five trips to Saudi Arabia to negotiate for disease surveillance and vaccine development as President Barack Obama's

US science envoy. It's also sandwiched between conflict zones—in Yemen, Syria, and Iraq—where diseases are surging as civil infrastructure breaks down. Hotez, who is a physician and dean of the National School of Tropical Medicine at Baylor College of Medicine, cowrote a paper that appeared a week ago in *PLoS Neglected Tropical Diseases*, containing a warning list of diseases that pilgrims might import or carry home, from cholera to drug-resistant bacteria to leishmaniasis.

The new system pings an alarm at the government's public health command center, based on automated sifting through medical records.

The new system created by the Saudi health ministry and the WHO's eastern Mediterranean region aims to boost the kingdom's own infrastructure by installing an extra—and extra-sensitive—apparatus for the detection of diseases. It pings an alarm at the government's public health command center for the hajj, based on automated sifting through medical records from hospitals and clinics.

On their own, the problems the system looks for don't sound major: fever, for instance, and GI distress, coughs and lung problems, and neurological symptoms. But diseases that can cause fast-moving outbreaks share many of the same signs and symptoms as minor and unrelated health problems. The new system will make a first evaluation of what needs a second look, and the command center will decide whether a rapid-response team needs to be dispatched.

The system got its first workout this week in eight hospitals and 25 clinics in two stops along the pilgrimage route, a joint effort of the Saudi health ministry and the WHO's eastern Mediterranean region. The WHO described the system in a blog post this week, but didn't respond to a request for an interview—so it isn't clear how the trial will be judged successful, how it will be scaled up in subsequent years, or how the data might be used to warn pilgrims' home countries of what might be coming their way.

The strategy behind the system, which depends on looking for anomalous signs and symptoms as an early-warning signal of something going wrong, dates back to the World Trade Center and anthrax attacks in the United States in 2001, and the fear that biological weapons might become a routine tool for international terrorism. How well it works—and it's never worked quite as well as was first imagined—depends on how much data the place where it's being deployed has in advance about the people who might have been exposed.

Because Saudi Arabia has such oversight over who is entering the country, its early-warning system may possess more predictive power than those in other places.

The hajj is a unique situation, though. Because the Saudi government strictly controls visas, it knows exactly how many people are entering the country, where they came from, and, crucially, where they are during their time within its borders. In analyzing outbreaks, public health officials often struggle with what's called the denominator question: They know how many people became ill with something, but they may not know how many were exposed, and thus can't calculate the risk of illness occurring. Saudi Arabia, however, may be able to answer that question—and solving that equation might give its early-warning system more predictive power than those in other places have had.

Some researchers are hoping the data from the new Saudi system could be put to an additional use that its designers may not have envisioned. It could be useful not just for detecting outbreaks during the hajj but also for delivering a comprehensive snapshot of everyday illnesses that might be moving through those surging millions as well.

"People get excited for surveillance to discover the very scary things—MERS, Ebola, the next pandemic virus," says Amesh Adalja, a physician and senior scholar at the Johns Hopkins University Center for Health Security. "But it is really important to know what is circulating even if it is not causing people to be very sick or to die."

The hajj represents not only an enormous number of people, but also extraordinary diversity—of age, income, underlying healthfulness or illness, and geographic origin. The data set they collectively represent is unfathomably rare, and the ability to track illnesses moving through them would be more rare still.

That knowledge would certainly help frontline physicians who might be diagnosing and comforting sickly pilgrims in future years of the hajj. If it is made open and public, it might also help protect not just the families and nations those pilgrims are returning to, but the future health of the world.

Maryn McKenna *is an Ideas contributor for WIRED, a senior fellow at the Schuster Institute for Investigative Journalism at Brandeis University, and the author of Beating Back the Devil, Superbug, and Big Chicken. She previously wrote WIRED's Superbug blog.*

New technology may help police tackle emergencies at public events

Source: http://www.homelandsecuritynewswire.com/dr20180904-new-technology-may-help-police-tackle-emergencies-at-public-events

Sept 04 – Medical emergencies for fans during athletic events can quickly turn into life-or-death situations. That's why as another Boilermaker football season gets underway, Purdue University researchers are using technology to help police monitor emergency and public safety information on game day.

"This is a giant leap for social media analytics tools," said David Ebert, director of Purdue's Visual Analytics for Command, Control and Interoperability Environments center by the Department of Homeland Security and the Silicon Valley Professor of Electrical and Computer Engineering. "Police departments and first responders can use the social media posts to reach people in need of assistance, including medical emergencies, disaster emergencies or criminal activity. During the start of football season, it can be used to find fans having heat-related medical issues."

Purdue says that the platform also has applications for monitoring traffic, finding victims when hurricanes make landfall, analyzing school threats and helping with security at major speeches or visits by people of note.

"We use the technology during special events to build word clouds based on the type of event," said John Cox, Purdue's police chief. "We use it during dignitary protection details where there could be a threat of violence or there is a history surrounding the subject of the dignitary's visit."

Ebert and his research team created an online platform, called the Social Media Analytics and Reporting Toolkit, to help first responders better monitor areas of natural or human-made disasters.

On game day, Purdue police can monitor the browser-based platform to see filtered social media content related to key words and geographic regions. Watch a video explaining how the platform works at http://bit.ly/Purdue-SMART.

The platform technology allows first responders to select key words and themes, such as various types of medical incidents or crimes, which are then visually displayed and highlighted on a map as they are talked about on social media within a specific geographic area.

"Users have told us our technology is easy to use and allows them to clearly see and monitor what is going on within a specific area," Ebert said. "Practically everyone is on social media these days, so there is a rich amount of data available."

Purdue's technology also allows users to set up customizable email alerts for relevant key words within a specified time frame.

Purdue notes that the Purdue team worked with the Purdue Office of Technology Commercialization to patent its work. The team is looking to license or sell the technology.

PERSPECTIVE: What Does Preparedness Cost?

Source: https://www.hstoday.us/subject-matter-areas/emergency-preparedness/perspective-what-does-preparedness-cost/

Sept 07 – It was a late Sunday afternoon in early November when my Mom called me with the news. *"There's been a fire. Your grandfather is fine, but he's lost everything. His apartment building caught fire and there's not much, if anything left."*

At the time, my then 89-year-old grandfather was living in a retirement community in Cabot, Pa., a rural community just over 30 miles north of Pittsburgh. While slower in his steps, but still sharp in mind, when the fire occurred on the third floor of his apartment building, my grandfather had the sense of mind to leave his possessions behind and proceed to the stairwell to get out. With obvious concern for what was happening around him, he and several other elderly and less mobile residents literally sat down on the stair steps and scooted down on their backsides step by step three stories to safety.

By the time he and others got to the bottom floor, they had enough strength to get themselves up and walk out to where emergency rescue personnel and building staff were arriving to help them and tackle the all-consuming blaze. At the end of the day, all 137 residents of his

apartment building survived the devastating fire with no injuries or fatalities. By itself, that metric was a miracle that left local responders, regional media and residents in awe.

So, what made the difference?

All of the facility's residents had been coached and prepped about what to do in the event of an emergency. For them and all of the residents' families, those efforts paid off tremendously. The only losses that day were the possessions of 29 residents – one of those being my grandfather, who literally only had the clothes on his back as to what he had left in the world.

Losing everything in a fire, a flood, tornado or whatever is always devastating. There is certainly the physical shock of what's occurred and what you no longer have, but there is also the emotional trauma that goes with a sudden and monumental loss. My grandfather certainly felt that the rest of his life and I've thought about that a lot lately, especially after seeing the news footage of the devastating fire at the National Museum of Brazil this past weekend.

While there were no fatalities, *"the loss to Brazilian science, history and culture was incalculable."* An archive of 20 million items – the majority irreplaceable – was consumed by a fire that, firefighters now report, burned as crews did not have enough water to try to put the blaze down. It was also revealed that pleas by museum staff and curators to better protect collected treasures from harm had been consistently ignored by any number of people and government offices who could have made a difference. A nation's history of itself, the region around it as well as the world were wiped out in a matter of a few evening hours. Heartbreaking may be the most apt word to describe the public reaction to the loss. I can only imagine how we in the U.S. would feel if one of the Smithsonian museums were destroyed by a similar event and our science, history and culture were left to be smoldering ash.

Once you lose something like that it's gone forever. No new rendering of whatever the lost items might be will ever capture the charm, history or content of the original.

While there is a world of difference in possession value between my grandfather's items and those of a country's national museum, I am still wrestling with the question: What does preparedness cost?

For my grandfather, it was the insurance that he and the retirement community had that allowed him to recover and move forward with his life. As important as those policies were (and they didn't cover everything), it was the emergency drills, the hall captains and building staff that he and his fellow residents had that saved their lives. While my grandfather would pass away a year afterward from cancer, having that extra year with him was priceless for my family.

I'm sure there are some type of insurance policies that Brazil possesses that will cover some of what they lost, but it is the steps they didn't take: the pleas that were ignored from museum

staff, curators and even the public to be better stewards of these priceless items, and the lack of time and resources they put into preparing for the unimaginable that will be the costliest of burdens to carry. It was a national abdication of responsibility. But that is not something unique to Brazil. It's a problem here as well.

The New York Times' Aug. 31 article "In Quake-Prone California, Alarm at Scant Insurance Coverage" gives a devastating preview of the prospective costs that Golden State residents, insurers and national taxpayers might experience when the "BIG ONE" finally hits. As jaw-dropping as those prospective losses might be, it is a fact that only 13 percent of California households have earthquake insurance. That is 34,605,842 people – 87 percent of California's population – (California's population is 39,776,830 people) that is at maximum risk.

The coverage statistics for flood insurance are not much better, with a majority of U.S. state residents not having any type of flood coverage at all.

The insurance gap that FEMA, and in particular Deputy Administrator for Resilience Dan Kaniewski, has become so vocal about is very real. For some people, the gap between what your insurance policies cover and what your recovery costs are can either be a fissure that can be adequately patched and covered by savings or be a bottomless Grand Canyon of debt from which you never climb out. The decisions and risks associated with that gap are owned by each of us as individuals. And anyone thinking that a FEMA check is going to cover all of their losses from an epic disaster is in for a rude awakening. While it is certainly within FEMA's responsibilities to help communities prepare, respond and recover from any and all threats, individual solvency, resilience and preparedness are personal responsibilities that no one can ever afford to ignore.

It's a lesson that was imparted to me in personal terms nearly a dozen years ago by a near-tragedy. And one that still leaves painful and costly consequences every day around the world in terms of lost lives, cultures, communities, economies and solvency.

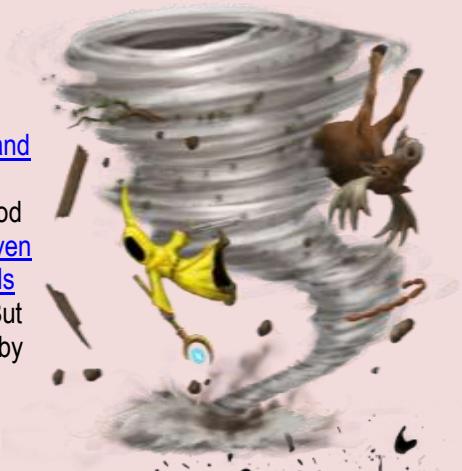
Because in the end, preparedness is ultimately priceless, and it always will be.

Rich Cooper *is Editor-at-Large for HSToday. A former senior member of DHS' Private Sector Office (PSO), Cooper has been a frequent writer and contributor to numerous media outlets. He is a Senior Fellow with GWU's Cyber and Homeland Security Institute; a Senior Policy Principal for Homeland Security and Justice at SAS Federal and a Principal with Catalyst Partners, LLC. He has also served in senior positions at NASA, the US Chamber of Commerce Foundation, and several other profit and not-for-profit enterprises.*

Keeping buildings functioning after natural disasters

Source: http://www.homelandsecuritynewswire.com/dr20180914-keeping-buildings-functioning-after-natural-disasters

Sept 14 – After an earthquake, hurricane, tornado, or other natural hazard, it's considered a win if no one gets hurt and buildings stay standing. But an even bigger victory is possible: keeping those structures operational. This outcome could become more likely with improved standards and codes for the construction of residential and commercial buildings, according to a new report recently delivered to the U.S. Congress by the National Institute of Standards and Technology (NIST).



"Current standards and codes focus on preserving lives by reducing the likelihood of significant building damage or structural collapse from hazards," said Steven McCabe, director of the NIST-led, multiagency National Earthquake Hazards Reduction Program (NEHRP) and one of the authors of the new publication. "But they generally don't address the additional need to preserve quality of life by keeping buildings habitable and functioning as normally as possible, what we call 'immediate occupancy.' The goal of our report is to put the nation on track to achieve this performance outcome."

The impact of a natural hazard on a community is usually most evident in the lives lost and physical destruction, but the accompanying economic shock, social disruptions and

reduced quality of life can often be devastating as well. "Cities and towns can be rebuilt, but lifestyles are damaged, sometimes permanently, if businesses, schools, utilities, transportation and other essential operations are out of service for an extended period," said Therese McAllister, manager of NIST's Community Resilience Program and another report author.

The infamous 1906 San Francisco earthquake provides a dramatic example of that impact. In the half-century following the 1840s Gold Rush in California, San Francisco was the fastest growing metropolitan

area in the region. That all changed on 18 April 1906, when the quake and resulting fires destroyed 80 percent of the city, killed some 3,000 residents and left nearly 300,000 people—three-fourths of the population—homeless, out of work and without essential services. Though San Francisco would rebuild quickly, the disaster diverted trade, industry and people south to Los Angeles, which then supplanted the "City by the Bay" as the largest, most important urban center in the western United States.

Even with modern building codes and standards in place, there is still room for improvement, as evidenced by the massive damage from the May 2011 tornado in Joplin, Missouri, and the three major 2017 hurricanes striking Texas, Florida and Puerto Rico.

"Immediate occupancy performance measures would help avoid catastrophes because they could build up a community's resiliency against natural hazards so that people still can live at home, still can go to work and still can have the supporting infrastructure providing them services such as water and electricity," McCabe said.

NIST notes that in 2017, Congress tasked NIST to define what it would take to achieve immediate occupancy performance codes and standards for all buildings in all types of natural hazards, specifically in terms of fundamental research needs, possible technological applications based on that research and key strategies that could be used to implement any resulting regulations.

The result of that effort is the new NIST report, *Research Needs to Support Immediate Occupancy Building Performance Objective Following Natural Hazard Events(NIST Special Publication 1224)*. The publication identifies a large portfolio of research and implementation activities that target enhanced performance objectives for residential and commercial buildings.

"The report provides valuable information about steps that could be taken to achieve immediate occupancy in the future," McAllister said.

The potential research activities presented in the report to Congress were developed with the assistance of a steering committee of recognized experts and stakeholder input obtained during a national workshop hosted by NIST in January 2018. The workshop participants identified four key areas that they believe must be considered when developing plans to achieve immediate occupancy performance: building design, community needs, economic and social impacts, and fostering acceptance and use of new practices.

For example, the report states that immediate occupancy performance measures must be developed, established and implemented with a sensitivity to how they will economically

affect building owners, business operators, occupants and even whole communities. "You have to make sure that the cost of keeping buildings functional after natural hazards remains reasonable enough that everyone will be able to afford them," McCabe said.

The report also discusses key challenges facing the effort to make buildings functional in the wake of natural hazards, such as motivating communities to make the investment, managing how costs and benefits are balanced, and garnering public support.

Finally, the report concludes by recognizing that "increasing the performance goals for buildings would not be easily achieved, but the advantages may be substantial" and that making such objectives a reality "would entail a significant shift in practice for development, construction and maintenance or retrofit of buildings." The report, its authors state, is the first step toward creating an action plan to achieve immediate occupancy across the nation with coordinated and detailed research goals and implementation activities.

"Our report outlines the steps that could be taken for a big raise of the bar—perhaps the biggest change in building standards and codes in 50 years—but one we believe is possible," McCabe said.

An elevator tech that could save lives in a high-rise fire

By Brian Blum

Source: http://www.homelandsecuritynewswire.com/dr20180917-an-elevator-tech-that-could-save-lives-in-a-highrise-fire

Sept 17 – When there's a fire in a high-rise building, safety rules dictate that you don't take the elevator. You head for the stairs instead. But what if using the elevator could actually be the fastest – and safest – way to evacuate a building on fire?

Salamandra Zoneis an Israeli startup that wants to make it possible for people trapped in a burning building to flee using the lift. Today, elevators automatically shut off if they detect a fire because the poisonous gases released from the fire can quickly overwhelm the elevator cab. **Indeed, some 95 percent of deaths from building fires are not caused by getting caught in the flames but from inhaling carbon-based gases and other byproducts of the fire.**

Those same gases also fill the stairwell, making it just as toxic as the elevator cab and even more dangerous when a panicked office building's workers crowd into a congested space all at once.

Salamandra Zone's solution: Don't shut down the elevator. Rather, turn the cab into a traveling "safe room" that can facilitate rescue operations.

Salamandra Zone's main product under development, B-Air, is a

small box placed on top of an elevator cab. It has two functions.

First, it converts toxic gases into breathable air in nanoseconds. Second, it adds a high-powered fan to the roof of the cab, which pushes cooled air into the elevator and prevents smoke from entering. It works even when the elevator doors are open. B-Air has a backup battery providing at least three hours of operation.

"High-rise buildings are very vulnerable," Salamandra Zone COO Gil Tomer tells ISRAEL21c. "Staying in place and waiting for the firefighters to rescue you is not an option. The highest ladders in the world can reach only to the 12th floor."

Modern high-rises soar dozens of floors, and sometimes over 100 — the Burj Khalifa in Dubai has 160 floors and 57 elevators.

And if you still need proof of how deadly high-rise fires can be, you only need to look back to June 2017, when a fire broke out in the 24-storey Grenfell Tower block in London, killing 72 people. Fire services told residents of the building to stay in their apartments and wait to be rescued. The advice was disastrous.

B-Air's sophisticated sensors can detect the exact concentrations of the noxious gases outside. The unit contains a mix of its own counter chemicals intended to react instantly with the sensed gases and convert them into breathable oxygen. CO2, for example, is split into its molecular components until only O2 is left.

As it converts the gases, B-Air sucks the toxic air from the elevator shaft into the cab at 72 kilometers per hour, creating a high-pressure zone that keeps any unfiltered gases out. It can easily be retrofitted into an existing elevator.

What about the fear that fire in an elevator shaft will snap the elevator cables? That kind of construction is long gone. "Decades ago, elevator shafts were built from different materials, including wood," Tomer points out. "Today, the shaft is one of the most protected areas in a building. It's made of concrete and never catches on fire."

For a building to change protocols and allow its elevators to continue operating during a fire, the B-Air system must work flawlessly. That was the main reason the entire seven-person staff of Salamandra Zone spent three weeks in the offices of Underwriter's Laboratory in the United States earlier this year to perform testing.

Still, Tomer estimates it will take two to three years until B-Air will be released in partnership with an elevator manufacturer. Salamandra has letters of intent to install its software with three industrial plants in Israel.

B-Air can also create stationary refuge rooms like those required by Israeli law for new construction following the Second Gulf War.

C-Air for industry

Salamandra Zone's second product, C-Air, is aimed at industrial plants that might have a gas leak or simply need a more efficient, less expensive way to clean up polluted output from their facilities.

Many industrial plants combine all their sources of emissions into a single pipe and then run it through a "scrubber" before it's released into the atmosphere, Tomer says. "But in the best cases, they only have 40 percent efficiency."

Installing C-Air at the end of the pipe – instead or in addition to the scrubber – can clean the gas "with 99.8 percent efficiency," Tomer claims. Moreover, "the infrastructure is cheaper and it needs less chemistry."

Tomer expects C-Air to be released sometime next year, just in time for European factories to be in compliance with a change in the way the European Union tracks pollution – from measuring concentration to measuring weight.

"They only have two years to stop these emissions," Tomer says. "It's like a sword hanging over their necks."

Once the system gains traction in Europe, the United States and China (with its famously polluted cities and a government mandate to clean them up) will be next.

Salamandra Zone was founded in 2014 by Marat Maayan following his 27-year career in the Israel Defense Forces. One of his last military roles was to map and identify risks to buildings at sensitive facilities. One risk he found: evacuation from fire.

Maayan hooked up with Hebrew University Casali Institute of Applied Chemistry Prof. Yoel Sasson, who had received a provisional patent on converting carbon dioxide into breathable air.

Salamandra Zone was formed as a joint venture and set about creating a commercial product that could cleanse more than just CO2. Sasson serves as the company's senior scientific adviser.

Salamandra Zone's headquarters are in Yehud, with R&D at the Hebrew University in Jerusalem. The company has raised $2.5 million from the Israel Innovation

Authority, private investors and founder Maayan.

The company's name is Hebrew for "salamander," an animal than can breathe air but also lives in the water, Tomer says. "Ancient tribes in South America called salamanders 'divine creatures' because they could survive forest fires while other animals ran away or died. The salamanders would dive into the water and only surface after the fire had gone."

Could Salamandra Zone have helped save more people during the 9/11 attack in New York City? Tomer says absolutely.

"We ran models looking at the two buildings," Tomer explains. In one, the fire didn't trip the software algorithms that stopped the elevators, so people were able to evacuate more quickly. "I don't want to say a specific number, but based on our calculations, it could have been in the hundreds."

Brian Blum *writes about startups, pharmaceutical advances, and scientific discoveries for Israel21c.*

Source: http://www.torchmarketing.co.uk/wp-content/uploads/2018/09/WSRSepOct2018.pdf