11\20

HZS

C²BRNE DIARY

Dedicated to Global First Responders

November 2020

A HOTZONE SOLUTIONS GROUP PUBLICATION


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

Elevated Radiation Found Near US Fracking Sites Has Public Health Experts Worried

Source: https://www.sciencealert.com/elevated-radiation-levels-discovered-near-us-fracking-sites-study-finds

Oct 23 – Residents who live downwind of fracking wells are likely being exposed to **radioactive airborne particles**, according to a new statistical analysis of public data.

While the levels measured in this case are not extremely dangerous, if inhaled on a regular basis, scientists worry they may cause adverse health outcomes, like lung cancer, in nearby areas.

Once these radioactive particles are in a person's body, they can continue releasing ionising radiation, possibly inducing oxidative stress and inflammation, even at the low levels observed.

Fracking is known to produce radioactive waste, usually from briny water welling up to the surface and bringing isotopes or uranium and radium up from below.

But the potential health effects of these particles are unclear and the current literature is limited. Despite many reasons to worry – including links to high-risk pregnancies, adverse birth outcomes, migraines, chronic rhinosinusitis, and severe fatigue – radioactive drilling waste from fracking is "virtually unregulated" in the United States, and both presidential candidates support the practice.

"If you asked me to go and live downwind [of fracking sites], I would not go," public health scientist Petros Koutrakis from Harvard University told The Guardian.

"People should not go crazy, but I think it's a significant risk that needs to be addressed."

Gathering over 320,000 measurements of particle radioactivity in the air from across the United States, the analysis found **communities between 20 and 50 kilometres downwind of operational fracking sites experienced worse radioactive pollution.**

The closer these communities got to the wells, the greater the levels of radioactivity.

"With adjustment for environmental factors regarding the natural emission and movement of particle radioactivity, an additional 100 upwind [fracking] wells within 20 kilometres was associated with a 0.024 mBq/m^3 increase in the level of particle radioactivity," the team writes in the study.

Such radiation levels translate to roughly 7 percent above the nationwide background levels of 0.35 mBq/m^3.

But the most affected place in the country appears to be Fort Worth, Texas, which had nearly 600 wells 20 kilometres upwind in 2017. Based on the team's calculations, this could result in a 40 percent increase of radiation levels above normal.

The association is too great to ignore, and while more research needs to dig into possible causes, the authors suspect several factors, including accidental spills and the sneaky release of natural gas, as well as the management, storage, and disposal of radioactive waste water, mud, and radioactive drill cuttings.

Another recent review of the potential risks faced from fracking found radioactive pollutants might even be present in natural gas pumped into people's houses if it's not stored away for long enough.

That sounds really scary, but the authors say with appropriate regulation of "exploratory drilling, gas capture and the use and storage of fracking fluid" the risk to the environment and public health can be minimised.

While some states in the US and other countries around the world have banned fracking until further research is done, the current analysis suggests there are still many communities in the United States where invisible pollutants in the air are putting people's health at risk.

"Our hope is that once we understand the source more clearly, there will be engineering methods to control this," Koutrakis told Reuters.

Of course, stopping the drilling is another option, too.

▶▶ **The study was published in** *Nature Communications*.

Infection with Novel Corona Virus and Radionuclide Contamination

Dr. Makoto Akashi

Source: https://nct-magazine.com/nct-magazine-october-2020/infection-with-novel-corona-virus-and-radionuclide-contamination/

Since the start of the outbreak of the coronavirus disease (COVID-19) caused by a virus called SARS-CoV-2 in December 2019 in China, the disease rapidly spread to all over the world. It goes without saying that Japan has been highly affected by COVID-19. I have worked on radiation emergency medicine for 30 years. After that, I was involved in the public response to the COVID-19 infection at the public health center of Ibaraki prefecture in Japan until the end of July 2020. In Japan, the public health center was a forward base for battling the outbreak at the time and played an important role as a "call center for Japanese returnees and potential contacts". Therefore, people developing symptoms such as fever, dry cough and shortness of breath had to call the center before seeing a doctor to be advised. Our public health center is located about 45 kilometers of the northeast center of Tokyo. Many people working in Tokyo reside in the area where our public center has jurisdiction. As the number of people infected with the virus increased in Tokyo, many houses started to get infected in the area.

	SARS-CoV-2	Radionuclide
Latent period	a few days to 2 weeks	> a few years (cancer)
In the body	Increase (number of virus particles)	Decrease (decay) (physical half-life)
Prevention	Vaccination	None
Treatment	Inactivation	Reduction of the amount
Understandings of the general public	Poor	Poor
Discrimination/prejudice	Caused	Caused
Economic damages	Huge	Huge

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

Dr. Makoto Akashi is Professor @ Faculty and Postgraduate School of Nursing Tokyo Healthcare University

How to Prepare for Something that Rarely Happens, like a Nuclear Incident?

By Mr. Thorsten Hackl

Source: https://nct-magazine.com/nct-magazine-october-2020/how-to-prepare-for-something-that-rarely-happens-like-a-nuclear-incident/

This is the difficult question to answer when looking at the risks of certain rare incidents. Especially if the risk is low but the impact huge. I am talking about nuclear disasters like Fukushima and Chernobyl. It is obvious that every nation with a nuclear facility wants to prevent any kind of incidents at those facilities. It is also obvious that all organizations involved in nuclear safety need to prepare for those incidents. The big question is, how much preparation is enough?

I usually start my lectures on nuclear safety with the following theorem: "You will fail handling a nuclear incident". I do this for two reasons. First, I want to lower the expectations: if you don't gain experience (which you do not want in case of a nuclear incident) you will probably make a lot of mistakes. In a way, I want to prepare people for disappointments and setbacks during an incident like Fukushima. The second reason is that I want them to focus on resilience and not waste too much time on thinking about all scenarios and on trying to prepare for all expected events. It is most likely the unexpected events that they will have to respond to. Therefore, by preparing people to be resilient, you make them better prepared and able to adapt quicker, thus benefiting the outcome of the mitigation. And this comes with a bonus. There are high chances that a lot of us will reach retirement without experiencing a nuclear incident. However, the improvement of the resilience capacity will improve the general incident management capabilities which is very good.

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

Mr. Hackl has specialized in HazMat incident management since 1999 and he was the team leader of the first Emergency Preparedness and Response Mission in Fukushima, Japan. During the course of his career he has trained over 1000 first responders in HazMat and nuclear protection.

Looking for Evidence of the Construction of Iran's New Centrifuge Assembly Plant: New Possible Preparations Identified

By David Albright, Sarah Burkhard, and Frank Pabian

Source: http://www.homelandsecuritynewswire.com/dr20201029-looking-for-evidence-of-the-construction-of-iran-s-new-centrifuge-assembly-plant-new-possible-preparations-identified

Oct 29 – In early September 2020, Iran announced its earlier decision to replace its Iran Centrifuge Assembly Center (ICAC), destroyed in early July of this year,[1] with a new facility in a mountain near the Natanz uranium enrichment site. According to Ali Akbar Salehi, head of the Atomic Energy Organization of Iran (AEOI); "It was decided to establish a more modern, wider and more comprehensive hall in all dimensions in the heart of the mountain near Natanz. Of course, the work has begun."[2] The destroyed site was designed to assemble thousands of advanced centrifuges each year. Its destruction set back Iran's plans to expand its centrifuge program by at least a year and perhaps longer. Exactly how long will depend on Iran's ability to rebuild the new facility, outfit it with sensitive equipment, and bring it into operation.

A building damaged by a fire, at the Natanz uranium enrichment facility some 200 miles (322 kilometers) south of the capital Tehran, Iran, in a photo released on July 2, 2020. (Atomic Energy Organization of Iran via AP)

It is hard to envision that Iran could quickly replace its assembly plant able to churn out thousands of centrifuges in a year. The above ground center at the Natanz enrichment site took years to finish and bring into operation, although some of that delay was caused by restrictions in the Joint Comprehensive Plan of Action (JCPOA). Nonetheless, absent the JCPOA, Iran would have needed more than a few years to build and operate a production scale plant.

Building the new plant in a mountain would further complicate its construction. The tunnel must include clean rooms necessary for assembling advanced centrifuges. Some of the replacement equipment is controlled internationally and highly sophisticated, likely requiring Iran to try to obtain it from abroad. Since Iran is banned from buying it, it will need to activate its illicit procurement networks, potentially causing further delays.

Iran could shorten the time to build the new assembly center by placing it in a pre-existing tunnel complex associated with the Natanz enrichment site. At the Institute, in 2007, we located and characterized this tunnel complex about two kilometers due south of the Natanz enrichment site, and published a study of its visible features at the time.[3] Figure 1, an 11 June 2020, Google Earth image, provides a perspective overview of the mountain area

southeast of the Natanz enrichment site as the area appeared prior to the ICAC's destruction, identifying the following key areas of interest: the existing tunnel facility, a security guard forces gunnery range, and a former construction site about halfway in between the two. Figure 2 shows a commercial satellite image of the tunnel area in 2007, the year that the tunnel facility was built [all the figures are available here, and in the report].

Although the existing tunnel facility is associated with the Natanz enrichment site, it is unclear what role it serves or if it was inspected by International Atomic Energy Agency (IAEA), unlike the tunnel complex associated with the Esfahan uranium conversion site, discovered in 2004 and subsequently inspected by the IAEA.[4] After the Natanz tunnel's discovery in 2007, Iran was not as forthcoming and resisted an inspection. Whether this tunnel facility was addressed in the JCPOA is unknown. As a result, less may be known about the internal structures and capabilities of this existing Natanz tunnel facility.

Iran could choose another site, and there are suitable locations to do that. However, that choice would require building an entirely new tunnel, further delaying the centrifuge assembly's start up. Iran could also build a hybrid facility with part underground and part half-buried adjacent to a tunnel entrance, a plan considered at the former nuclear weaponization Shahid Boroujerdi site being built under the Amad Plan in the early 2000s.[5]

Preparations for a New Facility May Have Begun

Construction at Iran's Natanz uranium-enrichment facility that experts believe may be a new, underground centrifuge assembly plant, annotated by experts at the James Martin Center for Nonproliferation Studies at Middlebury Institute of International Studies, October 26, 2020. (Planet Labs Inc. via AP)

To assess Iran's announcement, the Institute obtained recent high-resolution commercial satellite imagery of the existing tunnel site south of the Natanz uranium enrichment site and surveyed the surrounding area looking for new construction subsequent to the destruction of the above ground Iran centrifuge assembly center. Figure 3 shows the key area of interest including the existing tunnel facility as of August 31, 2020; Figure 4 shows it on September 18, 2020. Comparing these more recent images with the ones from prior to July 2020 leads to several conclusions.

The Institute determined that the pre-existing tunnel facility has not changed significantly since 2007, and there continued to be very little visible activity through the end of September 2020. Figures 5 and 6 show the existing tunnel facility as it appeared on 31 August and 18 September 2020, respectively. There has not yet been any indication of new road construction to, or tunneling or other excavation work in, the mountains south of the Natanz enrichment site, including at the pre-existing tunnel facility.

The most notable changes in the monitored area between June and late September 2020 occurred at the gunnery range. Comparing imagery from August 31 and September 18,

2020, the Institute was able to identify new road grading from the main highway at a point where there is an abandoned anti-aircraft artillery (AAA) site over to the guard forces gunnery range (See Figures 3 and 4). Moreover, the role of the gunnery range appears to have been converted to that of a construction support and staging area (See Figures 7 and 8). The evidence of that conversion is manifest in the presence of two bulldozers parked inside the firing range, along with the erection of two sheds that are probably intended for construction support. The sheds block the former line of fire, rendering the firing range unfit for its original purpose.

This Oct. 21 satellite photo provided by Maxar Technologies, shows construction at Iran's Natanz uranium-enrichment facility that experts believe may be a new, underground centrifuge assembly plant. Satellite photos show Iran has begun construction at its Natanz nuclear facility. That's after the head of the U.N.'s nuclear agency acknowledged Tehran is building an underground advanced centrifuge assembly plant after its last one exploded in a reported sabotage attack last summer. - Satellite image ©2020 Maxar Technologies via AP

Further, it is significant that additional road grading now also connects this converted gunnery range with the former construction area, which the Institute identified in 2007, located in the more mountainous terrain roughly 500 meters south of the gunnery range (See Figures 9-11). That area includes two small reveted areas containing two small buildings, suggesting that the buildings were likely originally designed to store explosives, such as that which could now be used for any future tunnel construction.
Given the conversion of the guard forces gunnery range and the presence of new road grading to the former construction area, Iran may be planning entirely new construction instead of repurposing the existing tunnel facility; if this new activity indeed represents preparations for the construction of an underground centrifuge assembly facility. Alternatively, Iran may be planning on constructing more than one assembly facility.

Conclusion

Construction of the main centrifuge assembly center could start soon. The tunnel area and its surroundings should continue to be monitored closely.
Bringing a new centrifuge assembly center into operation may take several years, if the goal is to assemble thousands of advanced centrifuges per year. The ICAC's destruction has set

back Iran's plans to deploy thousands, even tens of thousands of advanced centrifuges per year.
Faced with expected delays, Iran may opt to build more than one or modular facilities, where each one has a smaller annual capacity but could be constructed more quickly.
Whatever Iran pursues, including the construction of more than one facility or an underground one, these sites will remain vulnerable to attack. Rendering inoperable a centrifuge assembly facility, dependent on a clean room environment, does not require the destruction of the tunnel itself.
Although it is understandable that Iran would be determined to rebuild following the destruction of the ICAC, Iran should also consider the economic, civilian pointlessness of its centrifuge program. While highly useful as part of an effort to make nuclear weapons, Iran's advanced centrifuge will remain uneconomic, compared to buying enriched uranium overseas, and an on-going threat to the international and regional communities. If Iran's true goal is the development of a large-scale civilian nuclear power program, it would be far more likely to succeed if it abandoned its domestic centrifuge program, starting with not building a new advanced centrifuge assembly center.

1. David Albright, Sarah Burkhard, and Frank Pabian, "Update on Assessing the Detonation at the Natanz Iran Centrifuge Assembly Center: New High Resolution Satellite Imagery Refines Details on the Explosion and Fire," *Institute for Science and International Security,* July 9, 2020, https://isis-online.org/isis-reports/detail/update-on-assessing-the-detonation-at-the-natanz-iran-centrifuge-assembly

2. Parisa Hafezi, "Iran building new production hall for centrifuges in mountains near Natanz," Reuters, September 8, 2020, https://www.reuters.com/article/iran-nuclear-natanz/iran-building-new-production-hall-for-centrifuges-in-mountains-near-natanz-idUKL8N2G540Z

3. David Albright and Paul Brannan, "New Tunnel Construction at Mountain Adjacent to the Natanz Enrichment Complex," *Institute for Science and International Security* (ISIS), July 9, 2007, https://isis-online.org/uploads/isis-reports/documents/IranNatanzTunnels.pdf.

4. Institute for Science and International Security, "New Satellite Images Show Tunnel Construction at Esfahan Facility in Iran," February 17, 2005, https://isis-online.org/isis-reports/detail/new-satellite-images-show-tunnel-construction-at-esfahan-facility-in-iran/8

5. On Shahid Boroujerdi, see https://isis-online.org/isis-reports/detail/a-key-missing-piece-of-the-amad-puzzle and https://isis-online.org/uploads/isis-reports/documents/Annex_5_Parchin_Tunnel_Overlay.pdf

David Albright, *a physicist, is founder and President of the non-profit Institute for Science and International Security.*
Sarah Burkhard *is a co-author and lead researcher on the Institute's Peddling Peril Index (PPI), which ranks countries' export control systems.*
Frank Pabian, *a Nonresident Affiliate at Stanford University's Center for International Security and Cooperation, a center of the Freeman Spogli Institute for International Studies. He is a globally recognized expert in the fields of nuclear nonproliferation and satellite imagery intelligence analysis.*

Drug and Biologic Essential Medicines, Medical Countermeasures, and Critical Inputs – Radiological

Source: https://www.fda.gov/media/143406/download

Drug Category: Radiologic-Nuclear Threat MCMs			
Calcium diethylenetriamine pentaacetate (DTPA)	IV	API only	x
Ferric Hexacyanoferrate (Prussian blue; Radiogardase)	oral	API only	x
Pegfilgrastim (Neulasta)	SQ	API, master cell bank storage, +	x
Sargramostim (Leukine)	SQ	API only	x
Zinc diethylenetriamine pentaacetate (DTPA)	IV	API only	x
Hematopoietic Progenitor Cells- Cord Blood (HPC-C)	injectable	Human Cord Blood	x

Key Russian company withdraws from Turkish nuclear project

Source: https://ahvalnews.com/russia-turkey/key-russian-company-withdraws-turkish-nuclear-project-columnist

Oct 31 – A Russian company has withdrawn from plans to build Turkey's first nuclear power plant following tensions between Moscow and Ankara over issues including the conflicts in Libya, Syria, and Nagorno-Karabakh, a columnist at Turkish newspaper Dünya said on Saturday.
Turkey and Russia have stepped up economic cooperation in recent years, including the joint venture to develop **Akkuyu Nuclear Power Plant** in southern Turkey.

The landmark deal to build the 4.800-Megawatt facility was signed by Turkish President Recep Tayyip Erdoğan and his Russian counterpart Vladimir Putin 2010, but may now be in doubt as the two leaders find themselves at odds over a series of foreign policy questions.

Inter Rao, one of Russia's largest public energy companies, withdrew from the project following a board meeting on Oct. 26, Kerim Ülker said.

The move comes after Turkey's military intervention to support Azerbaijan in its conflict with Armenia over the disputed Nagorno-Karabakh region, traditionally seen as within Russia's sphere of influence.

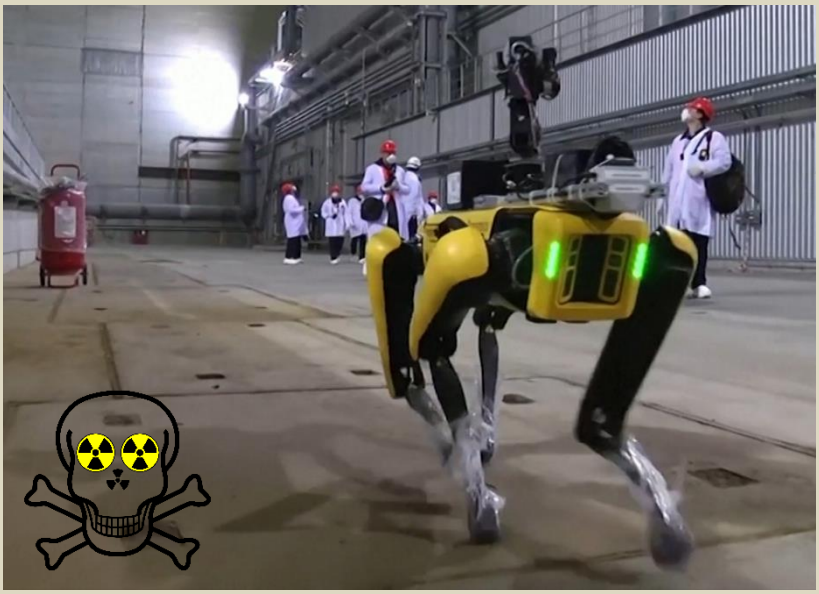
Despite only holding a one per cent stake in Akkuyu, Ülker said the significance of the decision came from the political connections of Inter Rao's chairman Igor Sechin, who is Putin's "de-facto assistant".

"It is remarkable that Inter Rao, which is under the management of Igor Sechin, known as the second most powerful name in Russia, has withdrawn from the Akkuyu Nuclear Power Plant project. Especially in the immediate aftermath of Turkey's support for Azerbaijan in Nagorno-Karabakh," Ülker wrote.

The Robot Dog Got a Job at Chernobyl

Source: https://www.popularmechanics.com/technology/robots/a34480039/spot-robot-dog-chernobyl-radiation/

Oct 28 – Thirty-four years after a bungled reactor systems test led to the worst nuclear disaster in world history, the Chernobyl Exclusion Zone is still mostly a ghost town, with the exception of scientists, stray dogs, and some tourists with a morbid fascination. That's due to the high levels of radiation in and near the reactor plant in Pripyat, Ukraine.



Now, Boston Dynamic's famous robot dog, Spot, is the newest resident. The robo-pup is on a mission to measure radiation levels so scientists can create a comprehensive 3D map to illustrate the distribution of the harmful electromagnetic waves.

On October 22, researchers at the University of Bristol—in conjunction with Ukraine's Central Enterprise for Radioactive Waste Management—first deployed the quadruped robot, according to Ukrinform, a state-owned information source.

This content is imported from YouTube. You may be able to find the same content in another format, or you may be able to find more information, at their web site.

In a YouTube video filmed at the Chernobyl site, David Megson Smith, a senior research associate at the University of Bristol's School of Physics, characterizes Spot's new role as a way to study robotic systems in extreme environments.

That way, his team can design new sensors, and therefore better robotic platforms, to autonomously survey nuclear plants.

This content is imported from {embed-name}. You may be able to find the same content in another format, or you may be able to find more information, at their web site.

Spot can be seen trekking around the former site of the Unit 4 reactor, which ruptured after a failed safety test in April 1986, meant to simulate an electrical power outage. In the video, you can see the robot dog examining various sites in and around the New Safe Confinement structure, a sarcophagus meant to contain the reactor's radioactive materials.

This isn't the University of Bristol's first foray into the Chernobyl Exclusion Zone. In April 2019, a multidisciplinary team conducted a series of radiation mapping surveys with a crew of drones. That included the first-ever unmanned aerial vehicle to map both gamma rays and neutrons, according to a press release.

After those tests, which covered the four miles of forest surrounding the nuclear power plant—known as the "Red Forest"—the team identified new radioactive hotspots that were previously unknown to local officials. Presumably, Spot's job is to find more of these dangerous locations.

Researchers discover how gut bacteria can protect from radiation damage

Source: https://newatlas.com/medical/microbiome-gut-bacteria-cancer-radiotherapy-protection/

Nov 01 – We know radiation therapy is an aggressively toxic treatment methodology for fighting cancer. Gastrointestinal distress is a common side-effect but researchers are only now discovering exactly how the massive population of bacteria living in our gut is influenced by acute radiation. New research led by scientists from the University of North Carolina at Chapel Hill is suggesting certain bacteria species may actually provide protection from the harmful effects of radiation.

Recent research has offered incredible new insights into the relationship between cancer and the gut microbiome. As well as potentially influencing cancer risk, and speeding up metastatic spread, specific species of gut bacteria has been found to either help or hinder responses to treatment.

Published in the journal *Science*, a new study presents novel evidence to suggest **certain species of gut bacteria can protect an organism from radiation-induced damage.** The study began by identifying a small subset of mice with the strange ability to survive a high dose of radiation that would kill most other mice.

The researchers called these mice "elite-survivors" and closely investigated their gut microbiome to find out how certain bacterial species could be conferring this unexpected protection from radiation. **Those "elite-survivors" were found to harbor a high abundance of two kinds of bacteria: *Lachnospiraceae* and *Enterococcaceae*.**

Further investigations revealed two metabolites produced by the bacteria, **propionate and tryptophan**, seemed to play a role in protecting the animals against the adverse effects of radiation exposure. These metabolites helped attenuate radiation-induced DNA damage, as well as reduce damage to bone marrow stem cell production.

Looking to validate these findings in humans, the researchers analyzed a cohort of leukemia patients receiving aggressive radiation therapy. They found those patients with the least adverse side effects from the radiation had the highest volume of *Lachnospiraceae* and *Enterococcaceae*.

Subsequent animal tests revealed direct treatment with propionate and tryptophan rendered mice somewhat resistant to radiation damage. Closer analysis revealed, what the researchers noted were, "a realm of metabolites that were affected by radiation and selectively increased in elite-survivors."

Corresponding author on the new research, Jenny P.Y. Ting, is cautious to draw a line from the animal research to humans just yet. She suggests larger studies are necessary to validate the findings in people before doctors and patients begin self-administering probiotics or postbiotics in conjunction with radiotherapy.

"Granulocyte-colony stimulating factor is the only drug that has been approved by the FDA as an effective countermeasure for high-dose radiation exposure, but it is expensive and has potential adverse side-effects," says Ting. "However, bacteria that we can cultivate, and especially metabolites that are relatively inexpensive and already elements in the food we eat, may be a good alternative."

A clinical trial is currently being planned to explore whether direct administration of these metabolites to patients undergoing radiation therapy reduces adverse effects.

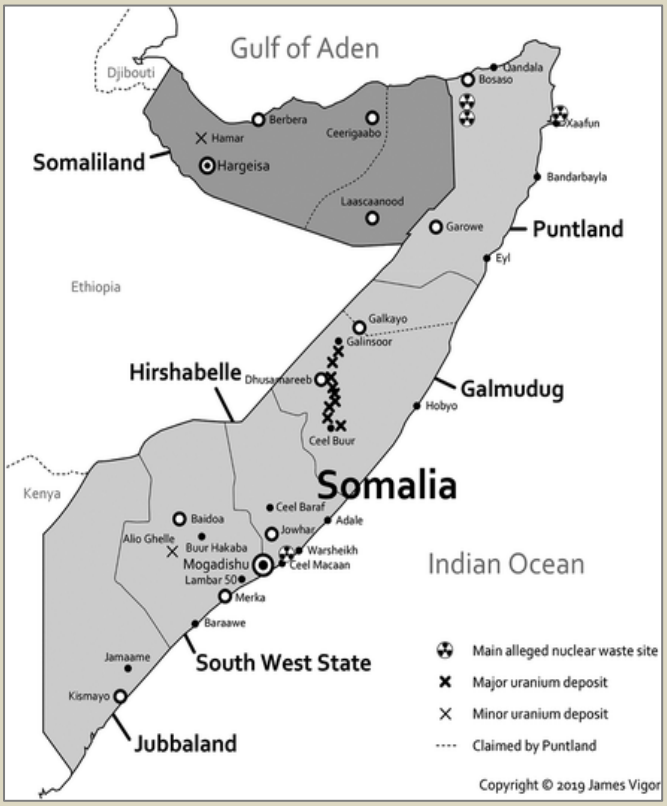
▶▶ **The new study was published in the journal** *Science*.

Nuclear security and Somalia

By Eric Herring, Latif Ismail, Tom B. Scott, and Jaap Velthuis

Global Security: Health, Science and Policy | Volume 5, 2020 - Issue 1

Source: https://www.tandfonline.com/doi/full/10.1080/23779497.2020.1729220



ABSTRACT

Scholars have not regarded Somalia as a place of relevance to thinking about nuclear security. This article gives four reasons why this perspective is not well founded. **First**, as the state strengthens it needs an International Atomic Energy Agency (IAEA) nuclear security regime for the control of nuclear materials. **Second**, it has unsecured uranium reserves that could be smuggled abroad. **Third**, those unsecured uranium reserves could be accessed by terrorists for use in a 'dirty' bomb. **Fourth**, there is evidence of past 'ecomafia' intent and planning, and possible success, in dumping radioactive waste on land in Somalia or in its territorial waters.

Uranium deposits and main alleged nuclear waste dumping sites

The article proposes an innovative system of uranium ore fingerprinting, covert sensors, mobile phone reporting and surveying and evaluation capabilities that would address all four issues. The proposed system would include a low-cost method for turning any smart phone into a radiation detector to crowdsource reporting of possible nuclear materials, plus aerial and underwater drones with low cost radiation sensors.

Eric Herring is Professor of World Politics in the School of Sociology, Politics and International Studies at the University of Bristol. His current research focuses mainly on promoting locally led development and he has wider research interests in international security and political communication. He is Co-Director of the Somali First initiative to promote Somali-led development. His books include Iraq in Fragments: The Occupation and its Legacy (Cornell University Press, 2006) with Glen Rangwala; The Arms Dynamic in World Politics (Lynne Rienner Publishers, 1998) with Barry Buzan; and Danger and Opportunity: Explaining International Crisis Outcomes (Manchester University Press, 1995).

Why a China-Saudi Deal Could Trigger a Mideast Arms Race

Source: https://www.theminotaurgroup.com/mideastnuke

On 4 August of this year, The Wall Street Journal published its discovery that Saudi Arabia had built a nuclear energy facility with the help of China, signaling a new era in Eurasian geopolitics. The facility, situated in the sparsely populated northwest part of Saudi Arabia, is being used to extract "yellowcake" from uranium ore, a preliminary yet consequential step in developing the capabilities to power a civil nuclear energy plant—and, potentially, to build nuclear weapons.

Subsequent to the groundbreaking reportage, Saudi and Chinese officials declined to comment on inquiries from U.S. and allied officials, keeping the details of the facility's purposes secret. Only the Saudi Energy Ministry offered a comment, stating that the ministry "categorically denies" that a uranium ore facility was built in the identified location. Ministry officials went on to state that, if any sort of yellowcake extraction is pursued, it is simply part of the Wahhabi Kingdom's "Saudi Vision 2030," Crown Prince Mohammed bin Salman's (MBS) flagship initiative for economic diversification.

Last month, however, on 17 September, The Guardian reported that, after seeing confidential documents, Saudi Arabia's uranium extraction efforts are, indeed, underway, and are moving at "breakneck speed." The documents in question were prepared by the Saudi government and sent to Chinese geologists for review, leaving no doubt about the Saudi-China bilateral cooperation. The Riyadh-Beijing partnership became official in August of 2017, with the announcement that the China National Nuclear Corp (CCNC) had signed a memorandum of understanding with The Saudi Technology Development and Investment Co. (Taqnia), the two countries' leading nuclear project developers, respectively.

While most transatlantic attention has generally been preoccupied with Iran's nuclear program and Russia's malign activities in the Middle East, a new set of threats and players is emerging in plain sight. At the broader level of the Eurasian supercontinent, China's increasing engagement in the Middle East is part of its comprehensive, systematic strategy for achieving hegemony. At the regional level, there is the immediate issue of Saudi Arabia.

A nuclear Saudi Arabia would be a game-changer for the security environment and balance of power in the Middle East, further destabilizing an already fraught geospace. Currently, Israel is the only nuclear power in the Middle East, and adding Saudi Arabia to the roster of WMD states will accelerate the expansion of the region's nuclear arm space.

The MBS era has been defined by his unpredictable and erratic leadership, including foreign policy adventurism and domestic intrigue. Doubly concerning is the Saudis' choice of China as the facilitator in this development project. Saudi Arabia is currently a nuclear "hedger," a country which can weaponize nuclear energy capabilities with alacrity. Some experts, like Iran economic specialist Saeed Ghasseminejad at the Foundation for Defense of Democracies, have theorized that Riyadh looked to Beijing very deliberately, reasoning that, if the Saudis decide "to move towards military nuclear capabilities, China and Chinese companies will be more accommodating or at least less hostile towards such a move."

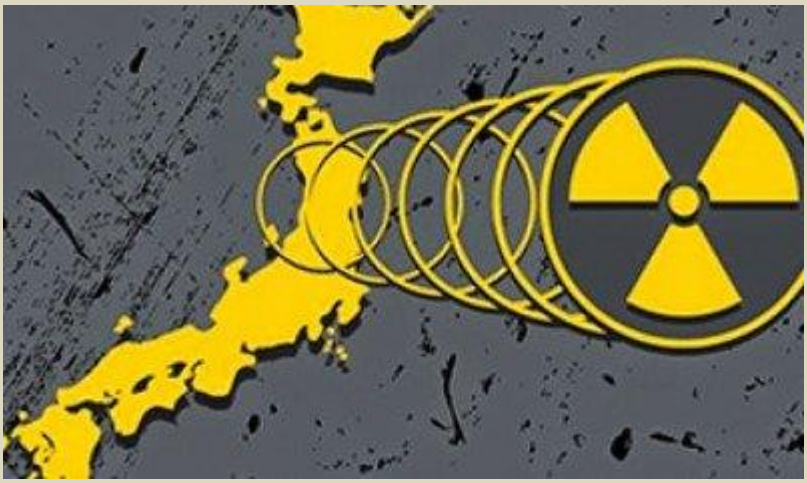
Furthermore, the Saudi-China nuclear relationship involves a calculus by other non-democratic, destabilizing actors in the Mideast. Turkey's President Recep Tayyip Erdoğan has been open about his country's aggressive nuclear campaign. Turkey has been pursuing nuclear energy since 2006, and, after years of failed development plans, began construction on its first nuclear facility in 2015. The facility, Akkuyu Nuclear Power Plant, is being built with the help of Rosatom, a leading Russian nuclear energy corporation, and will have four large civilian nuclear power reactors. Construction is expected to be completed in 2023, which also happens to be the centennial of the founding of the Republic of Turkey. When complaining of Turkey's lack of nuclear weapons, President Erdoğan said, "This, I cannot accept." Given Turkey's volatility,

and Erdoğan's increasing foreign adventurism in Artsakh, Syria, and Cyprus, the impending reality of a Turkey with nuclear weapons is an even larger threat with the power dynamics now emerging with Saudi Arabia.
Egypt makes for greater volatility in a potentially nuclear Middle East. The most populous country in the Middle East and North Africa, Egypt is one of Turkey's strongest regional competitors, and will likely follow suit if Turkey weaponizes their emerging nuclear capabilities. Egypt has begun construction on several nuclear reactors (which are also Russian-built), and, as reported by Foreign Policy, has long operated "a large Argentine-designed research reactor capable of producing more than a bomb's worth of plutonium each year and has tinkered with reprocessing."
The prospect of a nuclear Saudi Arabia may easily produce a nuclear arms race that will degrade the security environment in the Middle East, creating the kind of regional instability that will advance China's goals for geopolitical hegemony across Eurasia.

Fukushima, the Nuclear Pandemic Spreads

By Manlio Dinucci
Source: https://www.globalresearch.ca/fukushima-nuclear-pandemic-spreads/5728591

Nov 05 – It was not Covid, therefore the news went almost unnoticed: Japan will release over a million tons of radioactive water from the Fukushima nuclear power plant into the sea. The catastrophic incident in Fukushima was triggered by the Tsunami that struck the northeastern coast of Japan on March 11, 2011, submerging the power plant and causing the core of three nuclear reactors to melt.



The power plant was built on the coast just 4 meters above sea level with five-meter-high breakwater dams, in a tsunami-prone area with waves 10-15 meters high. Furthermore, there had been serious failures by the private company Tepco managing the plant, in the control of the nuclear plant: the safety devices did not come into operation at the time of the Tsunami.
Water has been pumped through the reactors for years to cool the molten fuel. The water became radioactive, and was stored inside the plant in over a thousand large tanks, accumulating 1.23 million tons of radioactive water. Tepco is building other tanks, but they will also be **full by mid-2022.**
Tepco must continue pumping water into the melted reactors and has decided to discharge, in agreement with the government, the water accumulated so far into the sea after filtering it to make it less radioactive (however, to what extent it is not known) with a process which will last 30 years. There is also radioactive sludge accumulated in the decontamination filters of the plant, stored in thousands of containers, and huge quantities of soil and other radioactive materials.
As Tepco admitted, **the melting in reactor 3 is particularly serious because the reactor was loaded with Mox, a much more unstable and radioactive mix of uranium oxides and plutonium.**
The Mox for this reactor and other Japanese ones was produced in France, using nuclear waste sent from Japan. Greenpeace has denounced the danger deriving from the transport of this plutonium fuel for ten thousand kilometers.
Greenpeace also denounced that Mox favors the proliferation of nuclear weapons, since plutonium can be extracted more easily and, in the cycle of uranium exploitation, there is no clear dividing line between civilian and military use of fissile material.
Up to now, around 240 tons of plutonium for direct military use and 2,400 tons for civil use (nuclear weapons can however be produced with them), were accumulated in the world (according to 2015 estimates), plus about 1,400 tons of highly enriched uranium for military use. A few hundred kilograms of plutonium would be enough to cause lung cancer to 7.7 billion inhabitants of the planet, and plutonium remains lethal for a period corresponding to almost ten-thousand human generations.
A destructive potential has thus accumulated, for the first time in history, capable of making the human species disappear from the face of Earth. The nuclear bombings of Hiroshima and Nagasaki; the more than 2,000 experimental nuclear explosions in the atmosphere, at sea and underground; the manufacture of nuclear warheads with a power equivalent to over one million Hiroshima bombs; the numerous accidents involving nuclear weapons and those involving civilian and military nuclear plants, all this has caused radioactive contamination that has affected hundreds of millions of people.

A portion of approximately 10 million annual cancer deaths worldwide – documented by WHO – is attributable to the long-term effects of radiation. In ten months, again according to the World Health Organization data, Covid-19 caused about 1.2 million deaths worldwide. This danger should not be underestimated, but it does not justify the fact that mass media, especially television, did not inform that over one million tons of radioactive water will be discharged into the sea from the Fukushima nuclear power plant, with the result that it will further increase cancer deaths upon entering in the food chain.

Manlio Dinucci *is a Research Associate of the Centre for Research on Globalization.*

Oxford University's ties to nuclear weapons industry revealed

Source: https://cherwell.org/2020/11/13/oxford-universitys-ties-to-nuclear-weapons-industry-revealed/

Nov 13 – Freedom of Information requests submitted by *Cherwell* have revealed that Oxford University accepted at least £726,706 from the Atomic Weapons Establishment (AWE), the designer and producer of the UK's nuclear warheads, during the years 2017-19 alone.

The majority of this money was awarded to the Oxford Centre for High Energy Density Science (OxCHEDS), which advertises AWE as one of its "national partners" on its website.

AWE's funding is mostly used by OxCHEDS to fund individual research projects and studentships, with a substantial portion (£82,863 in 2019) funding the department's William Penney Fellowship, named after the head of the British delegation for the Manhattan Project and 'father of the British atomic bomb'. According to the AWE website, William Penney Fellows "act as ambassadors for AWE in the scientific and technical communities in which they operate".

This fellowship is currently shared by two professors, Justin Wark and Peter Norreys, both of whom collaborate closely with US state laboratories that develop nuclear weapons, the Lawrence Livermore National Laboratory and the Los Alamos National Laboratory.

AWE donations have also funded projects at the University's Departments of Chemistry, Engineering, and Physics, a number of which are directly linked to the design of nuclear weapons. One AWE-funded paper, published in 2019, investigated fusion yield production, a vital way of testing the destructive power of a warhead prior to manufacturing, whilst another project researched methods used by nuclear weapons designers for simulating the interior of a detonating warhead.

This research also has civilian applications, and does not in itself point towards the development of nuclear weapons. A spokesperson from Oxford University stated: "Oxford University research is academically driven, with the ultimate aim of enhancing openly available scholarship and knowledge. All research projects with defence sector funding advance general scientific understanding, with a wide range of subsequent civilian applications, as well as potential application by the sector."

However, AWE is not a civilian organisation. As Andrew Smith of Campaign Against the Arms Trade told Cherwell, "the AWE exists to promote the deadliest weaponry possible. It is not funding these projects because it cares about education, but because it wants to benefit from the research and association that goes with it". Mr. Smith concluded: "Oxford University should be leading by example, not providing research and cheap labour for the arms industry".

Responding to *Cherwell*'s findings, Dr Stuart Parkinson, Director of Scientists for Global Responsibility, described Oxford University's ties with AWE as "shocking" and called for the work to be "terminated immediately". He said that the findings "point very clearly to Oxford University researchers being involved in the development of mass destruction".

In the face of this criticism, the University spokesperson claimed: "All research funders must first pass ethical scrutiny and be approved by the University's Committee to Review Donations and Research Funding. This is a robust, independent system, which takes legal, ethical and reputational issues into consideration."

However, there are growing concerns over the ethics and efficacy of this process, which has seen controversial donations from the Sackler family, Wafic Saïd, and Stephen Schwarzman given the green light despite internal and public protests. The committee's deliberations are frequently subject to Non-Disclosure Agreements, meaning that they are not accountable to members of the University and to the wider public. Moreover, Freedom of Information requests submitted earlier this year revealed that the committee accepts over 95% of the funding it considers, with congregation members describing the committee as a "smokescreen" and a "fig leaf".

In recent years, the University has faced increased opposition from student groups such as the Oxford Climate Justice Campaign and Oxford Against Schwarzman over the companies Oxford chooses to affiliate itself with through investments and donations. From this term onwards, a newly formed student group, Disarm Oxford, will be campaigning against the University's numerous ties with the arms industry. Oxford Amnesty International is working with Disarm Oxford on the global Campaign to Stop Killer Robots, and to strive for the disarmament of the University more broadly.

Dr Rowan Williams, the former Archbishop of Canterbury and Chair of the Trustees of the Council for the Defence of British Universities, told Cherwell: "The recent publicity around university divestment from fossil fuels has highlighted the need for university bodies to be transparent about the ethical standards they apply to their funding, and it is encouraging to see this crucial question being raised also in the context of armaments-related funds and research."
The combination of Brexit and the coronavirus pandemic has created a particularly difficult time for university research finances. In a marketised higher education system, seeking and welcoming money from industry partnerships seems like an inevitability. However, while some industries rely on academic research to save lives, others are predicated on taking them. With the UK confirmed this year as the world's second biggest exporter of arms, the University's significant ties to the development of weaponry has an alarming global significance which is now beginning to be called into question.

EDITOR'S COMMENT: This article reminds me the situation in Greece whenever an attempt is made for a collaboration between academia and armed forces. Until now, it is mainly the communist part that suffers severe allergic reactions with such evil intentions. As a result, armed forces buy technologies from abroad; technologies that very easily could have been developed domestically. It seems that there is a very think line between stupidity and democracy.

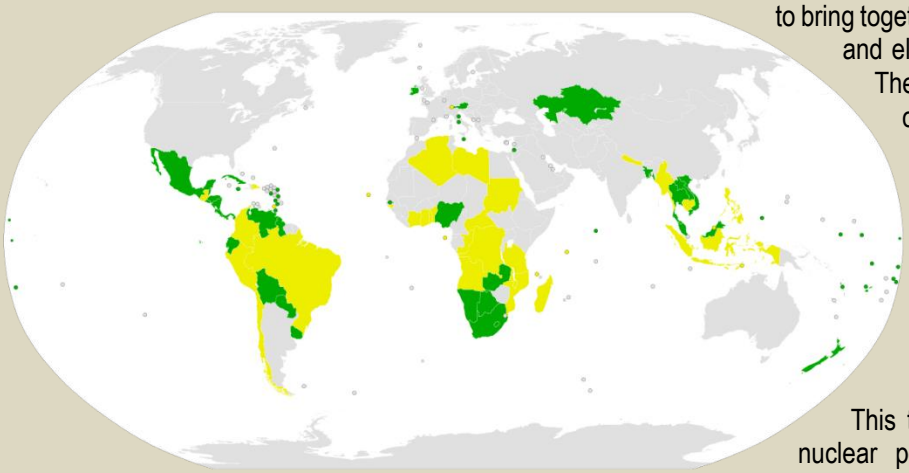
Kim Jong-un could 'carry out nuclear test to coincide with Joe Biden inauguration'

Former U.S. Department of State's top Asia expert, Mr Evans J.R. Revere, has warned that North Korean dictator Kim Jong-Un will be tempted to demonstrate his military might when Joe Biden finally becomes President of the USA.

Five Common Mistakes on the Treaty on the Prohibition of Nuclear Weapons

By Alicia Sanders-Zakre
Source: https://warontherocks.com/2020/11/five-common-mistakes-on-the-treaty-on-the-prohibition-of-nuclear-weapons/

Nov 16 – The Treaty on the Prohibition of Nuclear Weapons, the first international ban on nuclear weapons, will take full legal effect on Jan. 22, 2021. It joins the Chemical Weapons Convention and the Biological Weapons Convention as a treaty prohibiting weapons of mass destruction and follows the roadmap of the Mine Ban Treaty (known as the Ottawa Treaty) and Cluster Munitions Convention to bring together a coalition of civil society and diplomats to prohibit and eliminate weapons based on their humanitarian harm. The treaty has widespread support in the international community — 122 countries voted for its adoption in 2017, and these countries have continued to express their support for the treaty in subsequent statements to the U.N. General Assembly, in spite of resistance from nuclear-armed states and some of their allies, who have not joined the treaty.



Parties ■ | Signatories ■

This treaty is a big deal. And yet, political scientists and nuclear policy experts, largely from nuclear-armed states, repeatedly make mistakes in their analysis and interpretation of this treaty and international law. At a gathering of roughly 800 nuclear policy experts in Washington, D.C. in 2019, experts overwhelmingly and incorrectly predicted the treaty would not enter into force by March 2021. A French academic even misread the actual treaty text — a clear error that was not flagged by any of the article's expert reviewers, and was only corrected after publication.
I work at the International Campaign to Abolish Nuclear Weapons, which won the 2017 Nobel Peace Prize for its efforts to negotiate the ban treaty. Its work is informed by international lawyers, academics, technical experts, diplomats, survivors of nuclear weapon use and testing, and advocates with regional expertise. This diverse and rich foundation of knowledge

and experience informs our work to this day. But some academics and nuclear policy experts that haven't worked as closely on the treaty often make five key mistakes when analyzing this treaty and international law: that the treaty may be just symbolic, that NATO countries cannot join, that the treaty doesn't address compliance, that it won't have any impact on nuclear-armed and NATO states, and that the treaty will only affect democracies.

Mistake One: The Treaty Is Purely Symbolic

The legal impact of the Treaty on the Prohibition of Nuclear Weapons is clear: Once it enters into force, all states parties will need to comply with the treaty's prohibitions and implement its obligations. While some treaty articles reinforce existing obligations under other treaties, states parties do actually take on new legal obligations, contrary to what some have claimed. Even without any other states joining the treaty, from a strictly legal perspective, the treaty is not merely "symbolic."

The treaty prohibits states parties from developing, testing, producing, manufacturing, transferring, possessing, stockpiling, using (or threatening to use) nuclear weapons, or allowing nuclear weapons to be stationed on their territory. It also prohibits states parties from assisting, encouraging, or inducing states to engage in any of these prohibited activities. Some of these prohibitions are already enshrined in nuclear weapon-free zone treaties, but not all prohibition treaty states parties are members of these treaties. Given that the Comprehensive Nuclear-Test-Ban Treaty unfortunately has yet to enter into force, the Treaty on the Prohibition of Nuclear Weapons will be the only agreement in force banning nuclear testing internationally.

In addition to adhering to prohibitions, states parties must implement positive obligations, some of which echo previous agreements, but many of which are new to this treaty.

There are some technical requirements. For example, states parties must submit a declaration with the U.N. secretary-general on their nuclear weapon status. They must also bring into force a comprehensive safeguards agreement with the International Atomic Energy Agency on inspecting their peaceful nuclear program, or maintain a more intrusive inspections regime (an "additional protocol") if they have one in force already.

But the Treaty on the Prohibition of Nuclear Weapons also includes ground-breaking provisions on providing assistance to victims of nuclear weapons use and testing and remediating contaminated environments. This is the first time that international law has mandated that countries address the humanitarian devastation caused by decades of nuclear weapons testing and the U.S. bombing of Hiroshima and Nagasaki 75 years ago. It is a critical step forward to address the racist, colonialist, and unjust legacy left by these uniquely horrible weapons of mass destruction. Analysis of this treaty would do well not to ignore these historic articles.

Specifically, Article 6 of the treaty requires states to "provide age- and gender-sensitive assistance, without discrimination, including medical care, rehabilitation and psychological support," for victims of nuclear weapons use and testing "as well as provide for their social and economic inclusion." States must also "take necessary and appropriate measures" towards the remediation of contaminated environments. States with affected communities and contaminated environments under their jurisdiction are primarily responsible to structure and implement these obligations in order to respect these states' sovereignty and follow the legal precedent for victim assistance in other treaties. However, Article 7, which requires that all countries cooperate to implement the treaty's provisions, specifically calls on all states "in a position to do so" to provide assistance to other states as they carry out these initiatives. Such assistance can take many forms, including technical, financial, and material, so every state should be in a position to contribute.

These provisions will be at the center of the first meeting of states parties to the treaty, to take place within one year of the treaty's entry into force. Austria has already offered to host this meeting in Vienna. At this meeting, states will discuss routine logistics of international treaty meetings, such as costs and establishing the rules of procedure. Observer states, including signatory states, and some non-signatory states, including at least Sweden and Switzerland, will also attend and share the cost of the meeting. The extent of their participation will be determined by the rules of procedure. Civil society will also likely play an active role.

Mistake Two: NATO Countries Cannot Join the Treaty

One academic recently argued that membership in NATO and the Treaty on the Prohibition of Nuclear Weapons would be "mutually exclusive." While fully compliant membership in both treaties would require a few policy adjustments, it is certainly possible. There is no prohibition in the treaty for a member to be involved in military alliances or exercises with nuclear-armed states, as long as there is not a significant nuclear dimension to those alliances. NATO itself states, "NATO is committed to arms control, disarmament and non-proliferation, but as long as nuclear weapons exist, it will remain a nuclear alliance." However, legal experts explain that if a NATO state would like to join the treaty, they may certainly do so and remain in the alliance as long as that state renounces participation in the nuclear dimension of the alliance and indicates that it does not support activities prohibited by the treaty. There is a precedent of NATO members "footnoting" alliance documents to signal disagreement with certain policies. A NATO state could thus announce its change in policy and adjust its behavior accordingly to be in compliance with the treaty's provisions. Exactly how the NATO state would need to adjust its behavior to be in compliance with the treaty varies by country and could be determined in consultation with states parties.

Historically, different members of NATO can take different positions on controversial weapons without obliterating the alliance. Indeed, there are already divergent policies within NATO on the extent of participation in the nuclear aspect of the alliance: Some NATO countries go so far as to host U.S. nuclear weapons on their soil while others do not allow deployment on their territory under any circumstances. Opposition within NATO to banning landmines and cluster munitions did not stop those prohibitions from moving forward, even as the United States pressured countries to not even participate in the process to negotiate a treaty banning cluster munitions, and certainly did not destroy the alliance. Dozens of former leaders from NATO states, including two former NATO secretaries-general, recently called on their countries to join the Treaty on the Prohibition of Nuclear Weapons and certainly did not suggest that such a move would involve leaving NATO or that it would fracture the alliance. NATO's status as a nuclear alliance has evolved over time, and it could continue to adapt to shifting international norms.

Mistake Three: There Is No Mechanism to Address Compliance Concerns in the Treaty

If there are any concerns about compliance with the terms of the treaty, the treaty explains clearly what states should do in Article 11. When a state party has a concern about another state party's implementation of the accord, the two states may resolve the dispute amongst themselves or bring the matter to a meeting of states parties to discuss.

Concerns about compliance with an international treaty would certainly not be unique to this treaty and do not indicate that it is any less legitimate or valuable than other treaties with compliance disputes. States parties to the Nuclear Non-Proliferation Treaty regularly raise concerns about nuclear weapon-state compliance with their obligation to pursue nuclear disarmament under Article VI during meetings of states parties of that treaty. Likewise, states parties to the Chemical Weapons Convention condemn Syrian and Russian violations. These examples demonstrate the value of international treaties to reinforce norms and provide a forum to discuss and condemn violations of international standards for peace and security. Of course, given that the treaty has not yet entered into force, no state can currently be judged to be in non-compliance with the accord.

Mistake Four: The Treaty Will Only Impact Countries That Have Joined It

States parties' implementation of their obligation to assist victims of nuclear weapons use and testing will also have lasting impact beyond those countries themselves. There is currently no international standard for adequate victim assistance for those who have been impacted by nuclear weapons use and testing and no standard for how to judge that a nuclear-contaminated site has been adequately remediated. States parties' work on these provisions in the treaty will help to provide research and experience in these fields that can be applicable and useful even beyond countries that have joined the treaty.

Countries that are not part of the treaty can still contribute to these important measures. The United States, for example, is one of the largest donors to Mine Action, which facilitates mine clearance, despite not joining the Mine Ban Treaty. Mounir Satouri, a French member of the European Parliament, has expressed interest in encouraging European Union countries, including NATO members, to contribute to victim assistance and environmental remediation measures under the treaty, even if they have not yet joined as states parties.

The treaty will continue to grow and integrate into the international system well beyond its entry into force in January and first meeting of states parties. The norm established by previous weapons prohibitions impacted banks, companies, and government policies in countries that had not joined the treaty, and the same can be expected for the nuclear prohibition norm. The treaty's adoption has already caused a major Dutch pension fund to divest from companies involved in nuclear weapons, and more divestment can be anticipated once the treaty takes full legal effect.

Mistake Five: The Treaty Only Impacts Democracies

Countries that have not yet expressed support for the treaty are also expected to join in time. In many countries that do not officially support the treaty, polls show that domestic opinion is behind the ban and capitals in nuclear-armed and NATO states have adopted resolutions calling on their governments to join. Critics claim that domestic support may push Western democracies – in particular France, the United Kingdom, the United States, and NATO allies — to join the treaty, while more autocratic states — without a strong civil society to demand they adhere — remain unfazed by the new international law and norm.

That's not how international law works. International law applies to all countries, regardless of their governance structure, and all countries are influenced by the new norms advanced by international treaties. Pressure to join the treaty does not just come from an active civil society, but from other states, international organizations, and the changing norm established by the treaty itself. Article 12 of the treaty legally requires that all states parties urge other countries to join. This can be done in the form of public statements in international fora, like the United Nations, or privately in bilateral meetings. Pressure to adhere can even come from international figures like the U.N. secretary-general, the Dalai Lama, and the Pope who have all welcomed the Treaty on the Prohibition of Nuclear Weapons.

So far, the record shows that Western democracies are not necessarily more susceptible to pressure to support the treaty or to join it. While the United States and some NATO allies held a press conference outside the negotiations of the treaty in protest, China merely abstained on the resolution to start negotiations. When the treaty reached 50 states parties, a U.S. official Twitter account called the treaty "counterproductive," while the Chinese UN Mission on Twitter claimed its objectives were "in line with purposes of the TPNW." Of the states that have already joined the treaty, many have done so not because of civil society pressure, but due to their desire to adhere to international laws and norms against nuclear weapons.

Conclusion

In January, the treaty will take its rightful place among the other international treaties regulating nuclear weapons and other weapons of mass destruction, as an implementing instrument of the Nuclear Non-Proliferation Treaty's Article VI and complement to the Comprehensive Nuclear-Test-Ban Treaty. Most countries support the Treaty on the Prohibition of Nuclear Weapons as an important achievement for peace and security and towards a world free of nuclear weapons. As the risk of nuclear weapons use increases alarmingly, nuclear disarmament measures like this treaty are urgently needed.

The Treaty on the Prohibition of Nuclear Weapons will impact the norm against nuclear weapons and in the meantime will provide concrete assistance for victims of nuclear weapons use and testing and contribute to remediating radiologically contaminated areas. It is a powerful tool: important enough for leaders to ratify even in the midst of a global pandemic and influential enough that the United States actually called on countries to withdraw their instrument of ratification or accession. Analytical attempts to belittle or undermine the significance of this treaty may appease the minority of countries that cling to these weapons of mass destruction for now, but make no mistake — the Treaty on the Prohibition of Nuclear Weapons is a game-changer. And it is not going anywhere.

Alicia Sanders-Zakre *is the policy and research coordinator of the International Campaign to Abolish Nuclear Weapons. She is the author of over 100 news articles, editorials, academic articles, and reports on nuclear and chemical weapons, including many on the Treaty on the Prohibition of Nuclear Weapons.*

Students of Nuclear Security Have a Problem. Here's How to Help Them

Source: http://www.homelandsecuritynewswire.com/dr20201121-students-of-nuclear-security-have-a-problem-here-s-how-to-help-them

Nov 21 – Radioactive materials are attractive targets to thieves and other bad actors. These are rare finds, valuable on the black market and relatively easy to weaponize. New security professionals rarely learn practical skills for protecting these targets until they are on the job at nuclear power plants, research reactors, processing plants and other nuclear facilities.

"There is a need to have students who are technically trained in nuclear security before they work at a laboratory, a government agency, or at a commercial nuclear facility," said Alan Evans, a Sandia National Laboratoriesnuclear engineer.

Evans and his Sandia colleagues are teaming up with their counterparts at the University of New Mexico to create a new approach to teaching nuclear security. Their goal: create a one-of-a-kind, graduate-level program — one that has access to two national laboratories — that focuses on technical skills in education, research and professional development.

This program has financial backing from the National Nuclear Security Administration's Office of International National Security and has been bolstered by a memorandum of understanding signed in September between Sandia and UNM that outlines the program's development over the next five years.

Hyoung K. Lee, professor and chair of the UNM Department of Nuclear Engineering, said his hope with the new agreement is to create more robust opportunities for current and future nuclear engineering students at UNM.

"UNM has such a phenomenal resource right in its backyard with Sandia, so it makes sense to maximize that proximity by creating a partnership that will truly enhance students' education," he said. "We are very excited to be developing this program that we feel, with Sandia's collaboration, will offer UNM students an incredible advantage in the nuclear security field."

Future Program Built on University Partnership

At the core of the team's vision is a pedagogical shift toward engineering.

"There are other university programs in nonproliferation and nuclear security — some of which Sandia already works with — but a lot of these classes focus on policy and concepts," Evans said. "So, we had to ask ourselves: How can we better prepare the next generation of experts to apply traditional engineering capabilities to nontraditional challenges facing nuclear security for tomorrow?"

Adam Williams, a Sandia systems' engineer who has supported several educational initiatives, says the answer lies in forming the right team. He helped create the education program at the Gulf Nuclear Energy Infrastructure Institute at Khalifa University of Science

and Technology in Abu Dhabi, has served as a technical consultant on a nuclear security graduate program being piloted at Ukraine's Kiev Polytechnic Institute, and has lectured at multiple universities on security topics.

"We have a rare opportunity with UNM to create a robust, technical education program to bolster nuclear security around the world," Williams said.

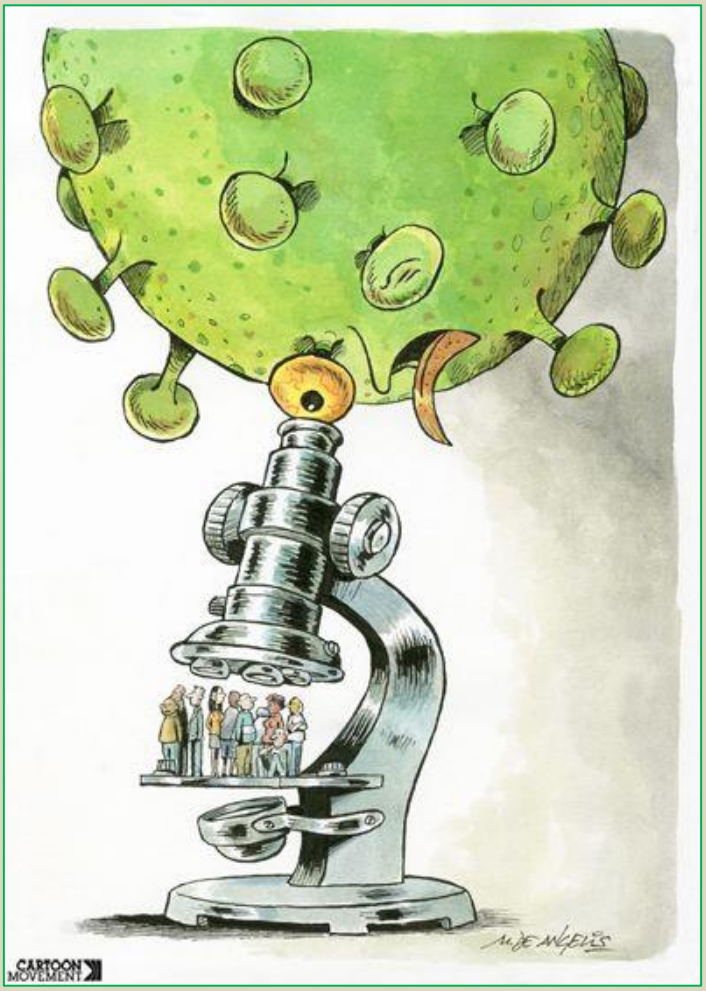
Nuclear security is one of Sandia's core research missions. For more than 70 years, the labs' primary work has been engineering the non-nuclear components of nuclear weapons. But corollary to this work, Sandia has had to keep these weapons and components secure. Through generations of research and practice, Sandia has grown into one of the world's foremost authorities on securing nuclear and radiological materials against would-be thieves or saboteurs.

"We are building on decades of expertise at both institutions to transform nuclear security from an art to a science," Williams said.

If successful, the new program will create a pipeline of professionals with knowledge, skills and abilities that shortcut years of on-the-job training — making their positive impact at nuclear facilities more immediate and long-lasting, and broadening their employment opportunities. Coursework also will better prepare nuclear engineering students to consider security when they design new energy, defense and medical technologies.

Additionally, Sandia will provide resources for the future Advanced Nuclear Security Summer School, a three-week, intensive professional development course to be hosted at UNM. The summer school will concentrate course materials for global industry executives and university professors and will be taught at a level appropriate for mid-career professionals.

"UNM is helping us create a new mechanism to enhance nuclear security capacity across the globe," Williams said.



ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

C²BRNE DIARY

EXPLOSIVE NEWS

Power Hawk – The 'Jaws of Life' for Bomb Squads

Source: https://www.hstoday.us/subject-matter-areas/emergency-preparedness/power-hawk-the-jaws-of-life-for-bomb-squads/

Oct 20 – Recently in Rhode Island, the Office of the State Fire Marshal was called in by local law enforcement to examine a possible pipe bomb. Once the area was secured and the public was at a safe distance, the bomb squad went to work assessing the device. When they determined that it was indeed a live pipe bomb, loaded with explosives and deadly shrapnel, the responders used a Department of Homeland Security (DHS) Science and Technology Directorate (S&T) developed tool called Power Hawk to carefully disable (or "render safe") the bomb.

"Our bomb technicians engaged the Power Hawk as a non-energetic means of remotely rendering the pipe bomb safe," reported Deputy Thomas Groff, Bomb Squad Commander with the Rhode Island State Fire Marshal's Office. "We were successful in doing so."

As dangerous as this scenario sounds to the general public, in listening to Groff's matter-of-fact description one might be tempted to think that this render safe operation was just another regular day at the office for bomb squad technicians. To a degree it is, but there was something different about this encounter.

Like many other bomb squad tools, Power Hawk enabled the bomb technicians to be at a safe distance from the explosive device during the procedure. However, what makes Power Hawk so special is that the bomb itself was not destroyed while being rendered safe. Since the components were left intact, the authorities were able to recover valuable forensic evidence that helped lead law enforcement to the arrest of the bomber.

S&T works with bomb squads to ensure they have tools to get the job done

Pipe bombs are the most commonly used Improvised Explosive Devices (IEDs) on American soil. Like the one used in Rhode Island, pipe bombs get their name from the casing of choice. Usually this means a section of steel water pipe. The inside of the pipe is packed with an easy-to-acquire explosive and often nails, bolts or other metal objects that will serve as shrapnel. The ends of the pipe are then sealed. When ignited, pressure builds up within the sealed pipe until it rips apart the casing—and that's what makes the weapon so devastating.

Making things worse, due to the nature of the explosive mixtures used in them, pipe bombs are notoriously unstable and prone to premature detonation. This can happen from seemingly innocent events that initiate internal pressure, friction, static electricity or other forces.

Unfortunately, the science and construction behind the development of IEDs is constantly evolving and will continue to threaten lives and property. However, S&T is dedicated to defeating that threat through the Response and Defeat Operations Support (REDOP) program, which leads the charge in helping to ensure public safety bomb technicians have the tools and solutions to do their jobs faster and safer.

"Our mission is to support state and local bomb squads (SLBSs) by focusing on collaboratively addressing the homeland's IED capability gaps, helping develop the best

solutions and connecting those solutions to the technicians in the field," said REDOPS Program Manager Byung Hee Kim.

Modifying traditional response gear for a more 'RAPID' response

Power Hawk was originally developed as a miniature version of the very well-known "**Jaws of Life**" (photo below) rescue tool that firefighters have been using to free trapped victims from car crashes and other dangerous situations for the last fifty years.

However, several years ago, REDOPS discovered that both the Michigan State Police (MSP) and the New Jersey State Police were using Power Hawk tools on pipe bombs with great success. Kim pointed out that "This is exactly the type of innovative thinking that REDOPS is always looking to bring to the broader SLBS community."

Under a branch of REDOPS called RAPID (Research and Prototyping IED Defeat) the Federal Bureau of Investigation (FBI) led independent testing, assessment and validation of Power Hawk's IED defeat capabilities. The Power Hawk passed with flying colors.

Subsequently, REDOPS and the FBI wrote a report detailing exactly how to use Power Hawk to defeat pipe bombs. That report was disseminated to all SLBSs across the county, and Power Hawk has been widely used ever since.

The Power Hawk has two major component parts to it: an extremely powerful hydraulic engine and a pair of scissor-like jaws.

The jaws are studded with metal teeth that clamp down and hold the pipe bomb steady. One of the reasons Power Hawk is so effective at rendering pipe bombs safe is that when the jaws engage, they slowly and smoothly crush the pipe. This causes small fractures that release pressure inside the pipe and prevent the buildup of gases that would power an explosion.

Overall, the tool is about two-and-a-half feet long and weighs about 40 pounds. Power Hawk is smaller and lighter than its big brother used in rescues, but it is still heavy and somewhat cumbersome. This is especially true for bomb technicians working with the added physical stress of wearing an 80-pound Kevlar bomb suit.

Precision and control are obviously important when dealing with explosives. The original solution to the awkward weight issue presented by the Power Hawk was to attach it to a large robot. However, this puts a very expensive robot at risk when rendering safe an IED. It also further limited the use of the Power Hawk to well-funded teams with larger robots.

To overcome this hurdle, MSP bomb squad technicians figured out another ingenious solution. Using components that were inexpensive and easily found in commercial stores, the techs constructed a mobile mounting stand to which Power Hawk can be attached. The stand (similar to a 2-wheel furniture moving dolly) can be pulled by a relatively small and inexpensive robot.

Once affixed, the robot can then transport Power Hawk to the IED. Alternatively, Power Hawk can be placed in a safe area and the pipe bomb can be delivered to Power Hawk. Either way, this cost-conscious workaround means that Power Hawk can be used by even more bomb squads around the country.

The MSP bomb techs didn't stop there. They also devised a remote controller to operate the Power Hawk. That way, the bomb tech doesn't have to manually handle Power Hawk and be in direct blast proximity to the bomb while rendering it safe. By using the new controller, the bomb tech and the robot can be protected.

All this is no surprise to Kim. "Bomb squad members are very inventive. Very technical. If they see a problem, they just figure out a way to solve it. Many times, that means inventing something new … . That's why we go out and visit bomb squads across the county and literally look through their trucks to find do-it-yourself tools that they built with off-the-shelf parts. Sometimes, they are so humble, they don't even know how brilliant their inventions are or how many other SLBSs they could help. That's one of the reasons we do what we do."

Groff expressed his gratitude to the REDOPS team for helping share Power Hawk with his bomb squad, "I just wanted to be sure you all saw the 'real' result of all your work. To be

completely frank … this stuff matters. It matters because it creates distance between us and a bad day. It also mattered because we recovered the forensics."

Filling bomb squad capability gaps with solutions big and 'micro'

REDOPS maintains a list of capability gaps for various IED scenarios and when the teams find innovative tools being used by SLBSs that help fill gaps across the community, REDOPS initiates a Micro Research and Development (R&D) Project.

In many cases, SLBSs don't have the funds to do their own extensive R&D on defeat products. This can put them at a disadvantage because those who wish to do harm are always looking for new ways to inflict damage. In this continuously evolving pipe bomb arms race, SLBSs must always stay at least one step ahead of the bad guys. If they don't, the results could be disastrous.

In support of SLBSs, REDOPS mines great ideas, do-it-yourself creations and workarounds created by technicians in the field from around the country. But its mission doesn't stop there. REDOPS then helps to refine the product and begins testing them extensively with the help of other SLBSs. If the invention passes the RAPID criteria, they not only create and disseminate the report about it, they write the product assembly manual. These instructions detail exactly how to build the product from those inexpensive and easy to find parts.

Another function within Micro R&D testing, is that once REDOPS writes up the instruction manual, they send it to a pre-selected group of SLBSs so they can try to build it from scratch. The SLBSs will need to find the pieces (at stores or online) and build the tool, using only the instruction manual. The users then give feedback directly to REDOPS on if they were able to find, buy and build a working tool. That feedback is incorporated into the final manual.

If only some of the big box stores would implement as comprehensive a system for developing their assembly instructions as the Micro R&D team has!

Power Hawk is a force multiplier

Kim says, "In the past, bomb squad techs would need to go down range and into harm's way to operate the Power Hawk by hand. They would be in close proximity to the explosives, putting their lives in danger, but now, the robot via remote control can bring the Power Hawk to the bomb (or vice versa) while staying at a safe distance."

REDOPS represents a technological force multiplier effect in the battle against pipe bombs. It works as both a full-service tech incubator and as a tech bridge between SLBSs across the country. Without REDOPS, the bomb technicians in Rhode Island would have never used Power Hawk, the mobile stand or its remote control. They would have had to place themselves in greater danger, as well as potentially risk losing the forensic evidence.

Kim summed up the impact saying, "We are providing new capabilities to the bomb squads. They are fully informed about the technology, and they know it is fully tested."

Military working dogs in Iraq get a blood bank like their humans have

Source: https://www.stripes.com/news/military-working-dogs-in-iraq-get-a-blood-bank-like-their-humans-have-1.649492

Oct 22 – Military working dog handlers in Iraq have set up a "walking blood bank" for their four-legged partners who help secure bases, hunt explosives and assist in combat missions such as the raid that killed Islamic State leader Abu Bakr al-Baghdadi last year.

"The bank will allow for rapid treatment of injured working dogs," Operation Inherent Resolve, the U.S.-led coalition battling ISIS in Iraq and Syria, said on Twitter Wednesday.

Boni, Bubo and Rexo, all patrol explosive detector dogs at Al Asad Air Base, were among the pups who had their blood drawn and tested earlier this month to identify their blood types, online photos show.

"This is the first time [Operation Inherent Resolve] has established a mobile blood bank for military working dogs ... and multi-purpose canines," said Army Col. Wayne Marotto, a coalition military spokesman.

The canine blood bank was started in response to a policy the Army Medical Command surgeon general's office issued that requires the service's veterinarians to record blood types for all working dogs, Marotto said. For human casualties in Iraq and Afghanistan, the military has long relied on "walking blood banks" in which prescreened donors can be called up to give blood at a medical facility in case of a mass casualty event or a trauma patient in need of numerous transfusions.

Blood loss is one of the top preventable causes of combat death. Earlier this year, the Marine Corps also began testing a program in the Middle East modeled on one used by Army Rangers in Afghanistan last year that enables lifesaving transfusions on the battlefield.

The 994th Medical Detachment Veterinary Services Support and medical personnel has set up emergency response capabilities and trained health care providers to ensure the animals receive "the highest level of emergency care," Marotto said. Inherent Resolve did not have military canine casualty data, he said. But at least two working dogs in the U.S. Central Command area of operations were medically evacuated following injuries this year, including one from Iraq that suffered cardiac arrest, according to military statements.

Military working dogs like Conan, a Belgian Malinois who was wounded during the mission that killed ISIS leader Baghdadi last October, are "critical members of our forces," U.S. Central Command boss Gen. Frank McKenzie said last year. Conan had accompanied special operations troops on some 50 missions.

In hot Middle Eastern weather, the availability of donor blood also can be critical for canines off the battlefield. In June, an Air Force pup named Cvoky was rushed by helicopter from Prince Sultan Air Base in Saudi Arabia to Kuwait's Camp Arifjan after its body temperature reached nearly 110 degrees.

At 104 degrees, dogs begin suffering heat stroke, the Humane Society of the United States website says. Heat injuries can cause internal organ damage and hemorrhage, and few dogs survive if they reach as high a body temperature as Cvoky, a military veterinarian said in a statement after the incident.

But in that case, a pint of blood from a Navy dog named Army helped save his life, the statement said. "We got the call that my dog, Army, might be a match," it quoted dog handler Petty Officer 2nd Class Sera Tamez as saying. "It feels really good to help one of our own!"

Electronic Security Technology to Replace Sniffer Dogs

Source: https://i-hls.com/archives/105087

Nov 07 – **A novel technology based on machine learning could replace sniffer dogs in finding explosives. High-tech sensors made from genetically-modified living cells can detect odors in the air and will be able to provide airports and airlines with situational awareness on the chemical, explosive, bacteriological threat. The cells are fused with a silicon chip that processes odor signals and passes them through a machine learning system for classification, performance improvement and error correction. If a smell is identified as a security threat, the purple, jelly-like device — called a Konikore — lights up.**

The US startup Koniku, in collaboration with Airbus, will start field trials of the devices in December, at Changi Airport in Singapore and San Francisco International Airport.

Weighing less than 350 grams and about half the size of a smartphone, the devices could be installed in multiple locations: on the revolving doors at the entrance to a terminal, at check-in desks, or at the entrance to an aircraft. This would not only make them easier to deploy than their canine counterparts, but more cost-effective.

"Dogs work for 20 minutes maximum, they can be easily distracted, and they are very, very expensive to train — it's an average cost of $200,000 per dog," says Julien Touzeau, head of product security for Airbus America.

Potential uses for the device do not stop at security, Koniku has been investigating whether the same technology could be used to detect viruses like Covid-19, following reports that

dogs may be trained to sniff it out. While they cannot detect the actual virus, respiratory diseases cause a change in the body odor of sufferers, which dogs — or "electronic noses," devices that can detect odors — may be able to pick up on.

However, some scientists specializing in electronic noses are skeptical of the technology.
Timothy Swager, a chemistry professor at the Massachusetts Institute of Technology, says that to pull off what Koniku claims would require "some technical miracle."
Integrating natural proteins into silicon circuits is extremely difficult, he says, and the fragility of cells and the complexity of their interactions with chemical substances makes them hard to work with.

Attack Methodology: Vehicle bombs

Published 2 November 2020
Source: https://www.gov.uk/government/publications/crowded-places-guidance/attack-methodology-vehicle-bombs

1. Introduction – Vehicle-borne Improvised Explosive Device (VBIED)
A VBIED is a vehicle which contains and delivers an explosive device to a target. The vehicle may be old or new, inexpensive or valuable, liveried or plain, blend into most situations and / or be modified to prevent detection. VBIEDs may range in size e.g. bicycles, cars, trailers, vans and large goods vehicles and have historically caused significant casualties when detonated near to or within crowded places or buildings. Injuries and fatalities are often greater when additional items are added to the device such as nails, nuts or bolts, or when structures / objects near the explosion shatter or fragment. It is likely that terrorists will continue to try and carry out such attacks in the UK. Such attacks may be multi-layered, including firearms, weapons (including 'fire as a weapon'), or any multiple combination.
The following examples may indicate unusual or suspicious behaviour:

- Unusual behaviour of the driver / rider
- Unusual characteristics of the vehicle

1.1 Behaviour of the driver / rider is unusual

This may include:

- Buying or renting a vehicle for cash, or without identity documents, or using false or forged identity documents. Can your staff readily identify forged documents such as driving licenses?

- Rapidly parking and the occupants leaving the vehicle. Do your staff monitor their surroundings? How good is their situational / environment awareness?
- Showing signs of stress, or concealment of their physical features when buying, renting, or parking the vehicle, or when obtaining potential IED components. Could staff readily recognise and more importantly respond and report suspicious customers at your premises?
- Conducting hostile reconnaissance before the event. Terrorists will regularly carry out hostile reconnaissance and undertake 'dry-runs' to test the security response. How might your staff identify such activity in your workplace?

1.2 characteristics of the vehicle are unusual

This may include:

- The vehicle appearing out of place or potentially abandoned. It may be illegally parked, have hazard lights or the headlights left on.
- The vehicles contents appearing out of place, such as visible gas canisters, wires, or modified electrical items such as alarm clocks and mobile phones.
- The registration details differing between the licence plate and the windscreen permit(s).
- The licence plates appearing newly attached, or with obscured characters to avoid recognition.
- A modified vehicle shell, such as a different body structure or patched paintwork.
- The vehicle sitting low on the rear axle (indicative of a heavy load in the boot or under the back seat).
- The vehicle emitting smells such as gas or fuel.
- The presence of smoke within the vehicle.

Trust your instincts. If you suspect it, report it.

2. Under vehicle improvised explosive device (UVIED) guidance

Under Vehicle Improvised Explosive Devices (UVIEDs) are small explosive devices, typically attached to, or placed underneath a vehicle, intended to kill or seriously injure the vehicle's occupants. Depending on the design, size and placement of the device, they may also result in the injury or death of others in the immediate vicinity and / or cause damage to the surrounding infrastructure.

Any individual or organisation likely to be targeted by terrorists or extremists should consider their risk and vulnerability against this attack methodology.

UVIEDs are improvised and therefore come in a variety of shapes and sizes. Different containers and camouflage have been used and attempted, including, but not exclusively, the use of plastic lunchboxes, metal piping or wooden boxes. Paint and grease may be used in an attempt to conceal or disguise the UVIED and such devices could be constructed to resemble a legitimate car part.

UVIEDs are likely to be placed in reasonably accessible locations, as those placing them will typically be keen to install and leave the device as quickly as possible.

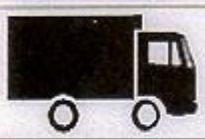
Historically, UVIEDs have been placed as follows:

- to the underside of a vehicle
- in front, on top of, or behind a wheel
- attached to a wheel arch
- tied to an exhaust
- on the ground under a vehicle

This is not an exhaustive list. UVIEDs are most frequently attached using magnets or adhesives due to the need to deploy the device quickly. UVIEDs can feature a number of different triggers to devices.

2.1 Mitigation

Wherever possible, park your vehicle securely. Make use of a lockable garage where available. Should a garage not be available, park your vehicle in a well-illuminated location where you and / or your neighbours can see it and where any suspicious behaviour is easily detectable. Avoid a set pattern in daily business that could aid the prediction of your vehicle's location wherever possible. This includes routes to / from work and times / days for shopping. Consider installing movement-based lighting systems, CCTV and / or fencing as deterrents. When out and about, consider parking in areas where there is high footfall, or where there are effective security measures or regimes in place.

ATF	VEHICLE DESCRIPTION	MAXIMUM EXPLOSIVES CAPACITY	LETHAL AIR BLAST RANGE	MINIMUM EVACUATION DISTANCE	FALLING GLASS HAZARD
	COMPACT SEDAN	500 Pounds 227 Kilos *(In Trunk)*	100 Feet 30 Meters	1,500 Feet 457 Meters	1,250 Feet 381 Meters
	FULL SIZE SEDAN	1,000 Pounds 455 Kilos *(In Trunk)*	125 Feet 38 Meters	1,750 Feet 534 Meters	1,750 Feet 534 Meters
	PASSENGER VAN OR CARGO VAN	4,000 Pounds 1,818 Kilos	200 Feet 61 Meters	2,750 Feet 838 Meters	2,750 Feet 838 Meters
	SMALL BOX VAN *(14 FT BOX)*	10,000 Pounds 4,545 Kilos	300 Feet 91 Meters	3,750 Feet 1,143 Meters	3,750 Feet 1,143 Meters
	BOX VAN OR WATER/FUEL TRUCK	30,000 Pounds 13,636 Kilos	450 Feet 137 Meters	6,500 Feet 1,982 Meters	6,500 Feet 1,982 Meters
	SEMI-TRAILER	60,000 Pounds 27,273 Kilos	600 Feet 183 Meters	7,000 Feet 2,134 Meters	7,000 Feet 2,134 Meters

2.2 Search and Detection

Avoid relying solely on the above measures. Additional checks should still be made. You may consider that checking your vehicle will draw attention; this is a possibility, but needs to be weighed against the potential impact of a UVIED attack.

There are other ways attention can be drawn to you, but there are no other ways to check for a UVIED.

- Check your vehicle after each occasion it is left unattended in an area that you cannot be certain is secure. Checks should be undertaken at your home first thing each morning; night time is when the vehicle is most vulnerable to tampering.
- Check if the vehicle has been left unattended at any time during the day; it can take only a few seconds to plant a device.
- Check the ground for any disturbance; this may indicate that the car has been approached or a device buried below.
- Park / orientate your vehicle to help you to inspect it. Avoid parking in a poorly lit area and where there are kerbs and puddles which would hinder your inspection.

Do not allow friends or family near the vehicle before you have checked it thoroughly and are satisfied in your own mind that there is nothing untoward or suspicious. Be familiar with the underside of your vehicle, as this will help you to detect anything suspicious. This is particularly important for larger vehicles where the underside may be more complex and provide greater opportunities for the concealment of devices. Photographs may assist memory if they are available at the time of inspection.

2.3 Response to a vehicle bomb

If something suspicious is found, stay calm. Do not touch it or any part of the vehicle. Move yourself and anyone else well away from the vehicle. Keep others from approaching the vehicle if possible and it is safe to do so. Once at least 15m away, call 999, ask for the police and explain what has happened. Take cover behind a substantial structure such as a wall or building, avoiding glazed areas. Trust your instincts.

2.4 Considerations for site security managers

Understand the threat posed by vehicles entering or in close proximity to your site. Whilst the principal risk is likely to be posed by VBIEDs with the potential to cause catastrophic damage to structures and mass casualties, the vulnerability of your staff to UVIEDs should

also be considered. To mitigate these risks, consider limiting and controlling vehicle access to your site as far as possible. For those vehicles requiring access, consider screening vehicles in accordance with your risk assessment, with staff proactively looking inside vehicles at vehicle access control points in order to identify any suspicious items. A general increase in vigilance around your site will also assist in deterring any hostile activity.

There are various methods of sophistication with regards to vehicle screening. These include pole-mounted mirrors and cameras, permanent or temporary drive-over inspection systems (for use at site entrances) and vehicle mounted detection systems (for specific, high-risk vehicles). It is advised equipment solutions only be procured as a result of a robust risk assessment and analysis of the operational requirement as a part of a holistic approach to security.

It is important to take advantage of the existing topography in creating 'stand-off' distance between premises / staff and vehicle access and parking points.

Remember - Every Metre Matters - The greater the distance between any such device and staff members or property, the less impact any such device is likely to have.

FBI "Actively Pursues" a Possible Hezbollah '94 Plane Bombing

By Todd Bensman

Source: https://www.meforum.org/61757/fbi-renews-probe-of-94-panama-plane-bombing

Nov 09 – For the first time in a quarter century, forward motion has been detected in the moribund investigation into one of the world's most enduring, unsolved terrorist bombings: the 1994 downing of **Panamanian** airliner Alas Chiricanas Flight 901.

The mid-air, apparent suicide bombing killed all 22 people aboard the short commuter flight from Colon to Panama City, 12 of them leading local Jewish businessmen. Coming just one day after the more catastrophic attack on the Argentine Israelite Mutual Association (AIMA) that left 85 Jews dead, Chiricanas Flight 901 drew less media interest or a similarly muscular investigative effort that eventually led Argentina to indict Iranian leaders and Iran's proxy, the U.S.-designated foreign terrorist organization Hezbollah. The bombing of Flight 901 has remained unattributed after some initial investigation vaguely suspected Hezbollah, the affiliated Sidon, Lebanon-based Shia group Ansar Allah, or a local drug and weapons trafficking cartel.

▶▶ Read the full article at source's URL.

Todd Bensman *is a fellow at the Middle East Forum and a senior national security fellow for the Center for Immigration Studies. He previously led counterterrorism-related intelligence efforts for the Texas Intelligence and Counterterrorism Division.*

ICI International CBRNE INSTITUTE

HOTZONE SOLUTIONS GROUP

CBRNE-Terrorism Newsletter

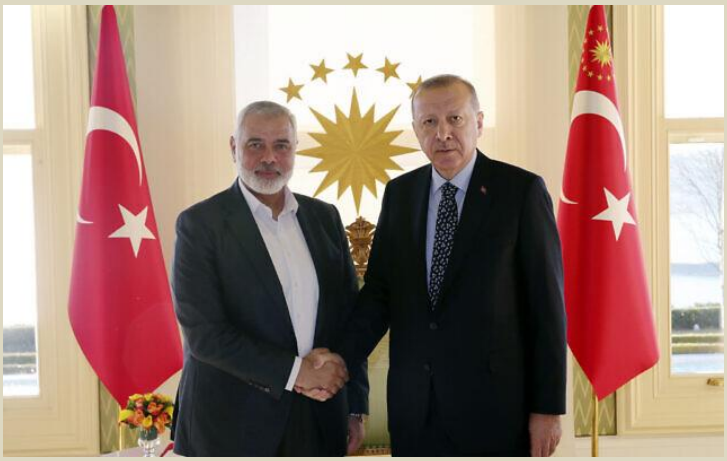
C²BRNE DIARY

CYBER NEWS

Hamas said to be secretly operating cyber, counterintelligence HQ in Turkey

Source: https://www.timesofisrael.com/hamas-secretly-operating-cyber-counterintelligence-hq-in-turkey-report/

Oct 23 – The Palestinian terror group Hamas is secretly operating a facility in Turkey where it conducts cyberattacks and counterintelligence operations, according to a British newspaper report Thursday.
Citing Western intelligence sources, the Times of London said the headquarters was set up two years ago and is overseen by Hamas military leaders in the Gaza Strip.



The headquarters, which is separate from Hamas's official offices in the city, was set up without the knowledge of Turkish authorities, the report said.

Turkey's President Recep Tayyip Erdogan, right, shakes hands with Hamas terrorist movement chief Ismail Haniyeh, prior to their meeting in Istanbul, February 1, 2020. (Presidential Press Service via AP, Pool)

The facility is reportedly overseen by Samakh Saraj, a senior member of the terror group who reports directly to Yahya Sinwar, the head of Hamas in Gaza.
The report said the headquarters' missions included obtaining "dual-use" equipment for producing weapons; coordinating cyberattacks against Hamas's enemies, including the Ramallah-based Palestinian Authority; and conducting counterintelligence operations against members of the terror organization suspected of disloyalty. There was no Turkish response to the report.
In August, the British daily The Telegraph reported that Turkey was granting citizenship to a dozen high-ranking Hamas members involved in coordinating terror attacks, which was later confirmed by the chargé d'affaires at Israel's embassy in Ankara.
Hamas is feared to be planning attacks against Israelis in Europe, The Telegraph said, and Turkish citizenship would enable its members to travel more easily.
Turkey sees Hamas as a legitimate political movement. The country has long maintained warm ties with Hamas, which have grown more overt as relations with Israel have chilled over the last decade. Israel has complained to Ankara about its ties to Hamas, but to no avail, according to the report.
In August, Turkish President Recep Erdogan met with a Hamas delegation that included politburo chief Ismail Haniyeh and the terror group's No. 2, Saleh al-Arouri — a top military commander who has a $5 million US bounty on his head.
The meeting was harshly condemned by the US State Department, but the Turkish Foreign Ministry rejected the criticism, accusing Washington of "serving Israel's interests."
In December 2019, The Telegraph cited Israeli sources as saying that Turkey is allowing Hamas members to plan attacks on its soil. Israeli officials told the paper at the time that Turkey has reneged on its 2015 commitment, negotiated by the US, not to allow Hamas officials to plot terror attacks against the Jewish state from its territory. Hamas and Erdogan's AKP party are linked politically. Both have close ideological ties to the Egyptian Muslim Brotherhood movement.

EDITOR'S COMMENT: "… secretly" – really?

Predicting the Likelihood of Cyberattacks Between Nations

Source: http://www.homelandsecuritynewswire.com/dr20201026-predicting-the-likelihood-of-cyberattacks-between-nations

Oct 26 – Where in the world might the next cyberattack between nations take place?
A new online database developed by a team of Johns Hopkins University computer scientists and international studies students predicts that there is an "extremely high likelihood" of a Russian cyberattack on Ukraine.
The second most likely? The United States against Iran.
The Cyber Attack Predictive Index (CAPI) devised by computer science professor Anton Dahbura along with cybersecurity lecturer Terry Thompson and former undergraduate Divya Rangarajan provides a predictive analysis of nations most likely to engage in the

surreptitious strategy waged with keyboards, code and destructive malware rather than soldiers, tanks and airplanes.
"The site attempts to anticipate and predict where the next major cyber conflict could break out based on existing data from past attacks," said Dahbura, executive director of the Johns Hopkins Information Security Institute and co-director of the new Johns Hopkins University Institute for Assured Autonomy. "It's a very good approximation of what's hot and what's not."
In 2019 as the rhetoric and record around deploying the malware menace grew more threatening, Dahbura began developing the site with Thompson when he was a lecturer in the Information Security Institute and Rangarajan before she graduated in May. Thompson worked for three decades at the National Security Agency and other federal agencies before moving to the private sector as a vice president at Booz Allen, and teaches graduate courses in global cybersecurity, cyber policy and cybersecurity risk management.
"This is going to be a much more common form of conflict in the future," Dahbura said.
The team devised a methodology for grading nations based on five common elements identified in all of the national cyberattacks over the past 15 years. Scored on a 1 to 5 scale, they are:

1. The strength and sophistication of the attacker's cyber force (from none to most advanced);
2. The severity of the grievance motivating the attacker against its target (from none to extremely aggrieved);
3. The attacker's lack of fear of serious repercussions (from extreme fear to none)
4. The consistency of an attack with the attacker's national security policy (from no policy to extremely consistent)
5. The degree of technological vulnerabilities within the target (from none to many).

The higher the total score the more likely a nation is to attack. The 12 nation-on-nation scenarios scored on the website range from the very low likelihood of India attacking China to four tied as the third most likely situations: China against the United States, Israel against Iran, Russia against the United States and the United States against Russia.
Dahbura and Thompson have formed a CAPI Advisory Board of project stakeholders that meets regularly to discuss hot-spots around the world that have implications for likely cyber conflict and to update the online CAPI Heat Index.
The website also provides several case studies used to devise the scoring system. The two highest scoring incidents were the cyberattack Russia simultaneously launched with its 2008 invasion of neighboring Georgia, and the STUXNET malware the United States and Israel unleashed on an Iranian nuclear facility.

▶▶ The project website can be found at https://cyberheatmap.isi.jhu.edu/.

Huge, Sophisticated Black Market for Trade in Online "Fingerprints"

Source: http://www.homelandsecuritynewswire.com/dr20201026-huge-sophisticated-black-market-for-trade-in-online-fingerprints

Oct 26 – Security on the internet is a never-ending cat-and-mouse game. Security specialists constantly come up with new ways of protecting our treasured data, only for cyber criminals to devise new and crafty ways of undermining these defenses. A thriving black market for user profiles is used by criminals to circumvent authentication methods that secure our online secrets.

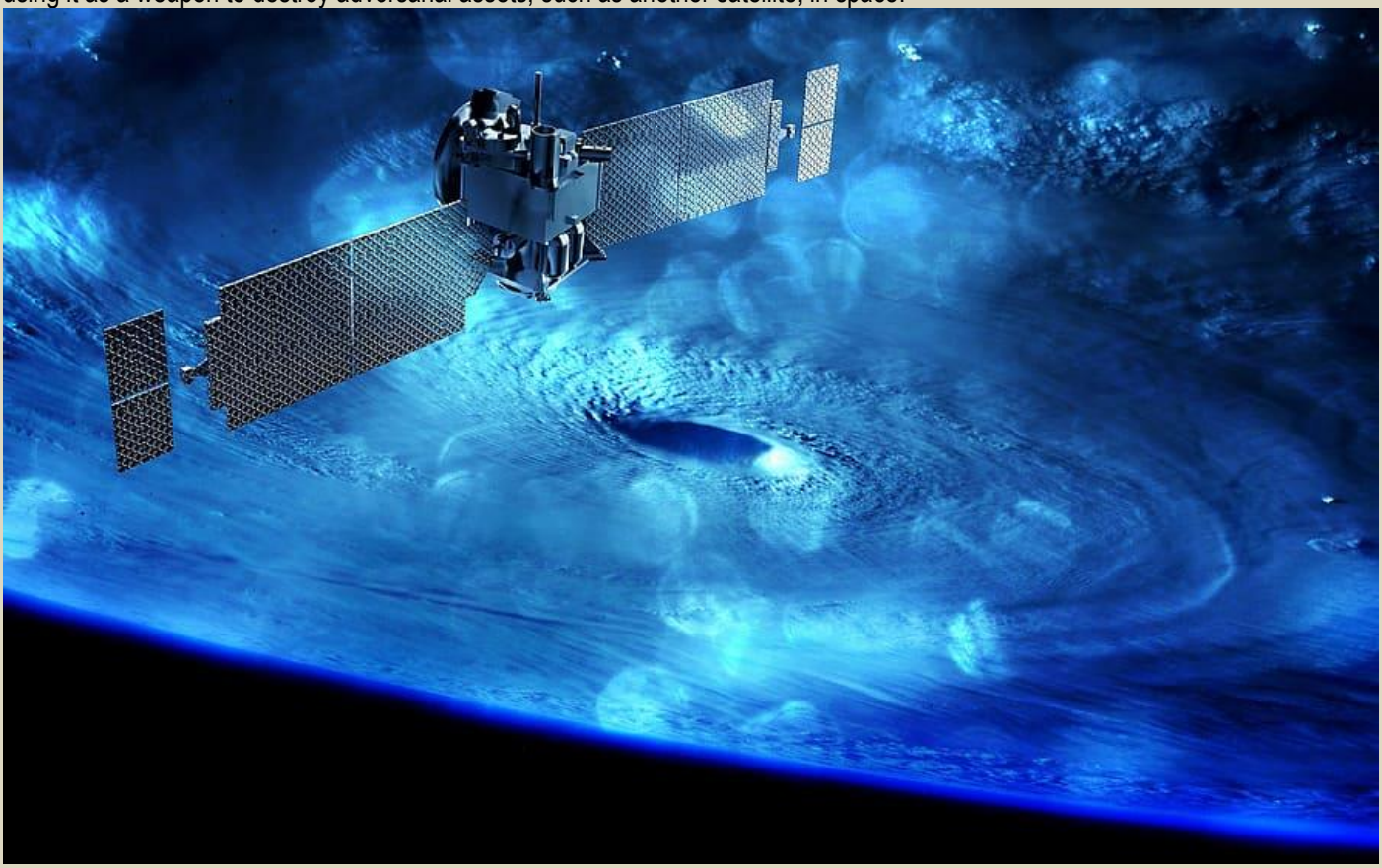
Why Satellite Hacking Has Become The 'Biggest Global Threat' For Countries Like US, China, Russia & India?

Source: https://eurasiantimes.com/why-satellite-hacking-has-become-the-biggest-global-threat-for-countries-like-us-china-russia-india/

Oct 24 – The US Air Force in April this year organised a hackathon to test the vulnerabilities of its military satellites in orbit. The competitors were asked to hack into an actual US satellite orbiting the earth, during Defcon, one of the world's largest hacker conferences.
The finale for the satellite hacking challenge, which offered hefty cash prizes, was held virtually to expose cyber-security issues and vulnerabilities in space assets and ground control systems.
"We need to embrace this external community to help us understand how to use … bug bounties and hacking events to deal with security issues before we take (systems) onto the battlefield," Will Roper, the Air Force's assistant secretary for acquisition, technology and logistics told reporters in May.
The pace at which the cyber-security and electronic warfare capabilities of different nations and non-state actors are advancing poses a monumental challenge to owners of the space assets in orbit. Taking control of a satellite by rogue elements could have dire consequences. Interfering with control systems of a satellite could render it non-functional in orbit, or even

deny access to its services. The possibilities involve jamming or spoofing the signals from satellites, destroying critical infrastructure such as electric grids, water networks and transportation systems.

Some satellites make use of thrusters to manoeuvre in orbit and to change speed, which if tampered with can alter the course of the satellite and send it crashing down to earth. These steerable satellites have most vulnerabilities, most disastrous of which could be using it as a weapon to destroy adversarial assets, such as another satellite, in space.



The country's possessing assets in space, particularly, the US, China and Russia, are increasingly worried about conflicts in space, where their vulnerabilities could be exploited.

China and Russia are believed to be working on the development of directed-energy weapons, signal jammers, anti-satellite missiles, satellites that can go close enough to other satellites in orbit and robotically mess with them, and, yes, cyber skills.

Experts warn the threats of satellite hacking are growing with increasing cyber warfare capabilities and the global arms race. The Defence One portal quoting Brian Weeden, Director of program planning for Secure World Foundation, said:

"Satellites and their ground systems are increasingly just computers running some specialized software, but they often run common OSes like Unix or Linux. They are vulnerable to many of the same cyber attacks as every other computer system out there."

"You generally need access to a specialised ground antenna and wait for the satellite to pass overhead before sending it commands. But if you can hack into the computers controlling that antenna, then you could be in business," he added.

The portal quotes Bill Malik, the vice president of infrastructure systems at cybersecurity firm Trend Micro, saying:

"So-called "control hacking" of a satellite isn't as easy as trying to steal someone's email, but it can be done. The hackers can easily get into the systems of the ground station controlling the satellite, after which gaining access to the satellite is a cakewalk, the experts believe.

The US intelligence agencies estimate that there were six known examples of hackers successfully interfering with or even commanding unauthorised manoeuvres of NASA satellites before 2011, many of which took place in 2007 and 2008.

Recognising these challenges, the White House last month issued directions to satellite makers and operators to harden their spacecraft against hackers and hijackers.

The directive asks the makers to design their hardware and software so that operators can monitor and adapt to "activities that could manipulate, deny, degrade, disrupt, destroy, surveil, or eavesdrop on space system operations.

The directive urges the manufacturers to ensure they also have plans and tools in place to recapture control of satellites that get jammed, spoofed, hacked, or hijacked. It also asked

satellite makers and operators to also better manage the security of ground stations and address "supply chain risks that affect cybersecurity of space systems."

Satellite hacks in the past

A US-German ROSAT X-Ray satellite was rendered useless in 1998 when hackers took control of the craft, directing it to aim its solar panels directly at the Sun. They managed to hack the satellite by getting into computers at the Goddard Space Flight Center in Maryland. The satellite's batteries were fried and it eventually crashed back to Earth in 2011.

In 1999, the hackers took control of the UK's SkyNet satellites and asked the government for ransom.

In 2007-08, the US Air Force accused Chinese hackers of using the connection from a ground station to affect the operation of the earth observation Landsat 7 and Terra (EOS AM-1) satellites. The Chinese government was suspected of sponsoring the hackers trying to find out how vulnerable the satellite control systems were to cyber-attack.

The Chinese hackers were again alleged to have been involved in a 2014 US weather systems and satellite network tampering. The hackers reportedly breached the federal weather network recently, forcing cybersecurity teams to seal off data vital to disaster planning, aviation, shipping and scores of other crucial uses.

The Chinese government officials denied any involvement in the incident.

The Chinese were suspected to have been also involved in the interception of a conversation happening through video chat via satellite, of a high-profile Indian government meeting in October 2017. The hackers continued to intercept the link for almost 4-5 minutes before a counter-offensive was launched to neutralise it, the Indian media reported.

However, hacking into space objects is not the same as hacking web systems. To successfully master a space system hack, one needs at least a basic understanding of things like orbital mechanics, ground stations functioning, the complex radio-frequency protocols, and more importantly, knowing what circuit board side of a satellite actually looks.

Launching such a daunting hack is, therefore, not everybody's cup of tea.

Today, numerous countries possess capabilities that could be used against space systems; however, there is limited evidence of cyber attacks in the public domain. The nations like the United States, Russia, China, North Korea, and Iran are known to have the capabilities to engage in offensive cyberattacks against non-space targets.

Although the efforts to address space cybersecurity are gaining momentum, the pace is still slow. The electronic warfare analysts lament the lack of any cybersecurity standards for satellites, with no governing body to regulate and ensure their cybersecurity. The responsibility for cyber safety of the satellites currently falls on the individual companies that build and operate them.

Satellites are becoming more and more important for the modern world, and their presence in lives is becoming indispensable.

The defence networks, such as the US defence and intelligence operations almost wholly depend on satellites today. From imaging and surveying every part of the earth, ensuring global communications, helping in transportation and tracking of ships and planes, gathering weather data, to providing location, timing, and navigation information, satellites are infiltrating every part of human functioning.

It's safe to say the modern world can't function without the operation of satellites. And their number is increasing around the earth every year, and so is their role in our lives.

French Jihadism on the Internet: A Quantitative Overview

By Dr. Antoine Jardin

Source: https://gnet-research.org/2020/10/19/french-jihadism-on-the-internet-a-quantitative-overview/

Oct 19 – France has been one of the most-targeted Western countries by jihadist organisations in the past 5 years and one of the most concerned by its recent development (40% of Europeans who joined IS are French). France has first been attacked by groups operating in the civil war in Algeria, like the GIA in the 1990s, before being targeted by al-Qaeda's global jihad networks in the 2000s. Since that date though, the country has increasingly faced homegrown activism and the threat of burgeoning national and local subgroups. Of course, these developments echoed major international events such as 9/11 in the U.S., 7/7 in the U.K., the war in Iraq, the rise of al-Qaeda in Mesopotamia and North Africa, and the outbreak of the Syrian civil war in 2011.

This experimental paper offers an overview analysis of requests related to jihadism on the French Google search engine.

1. Approach

We used French Google's 'Trends platform' in order to identify historical evolution on how French relates to this matter. We examined the frequency of about twenty keywords referring to jihadi and radical Islam activism on Google searches between January 2004 to October 2020 (the longest period available).

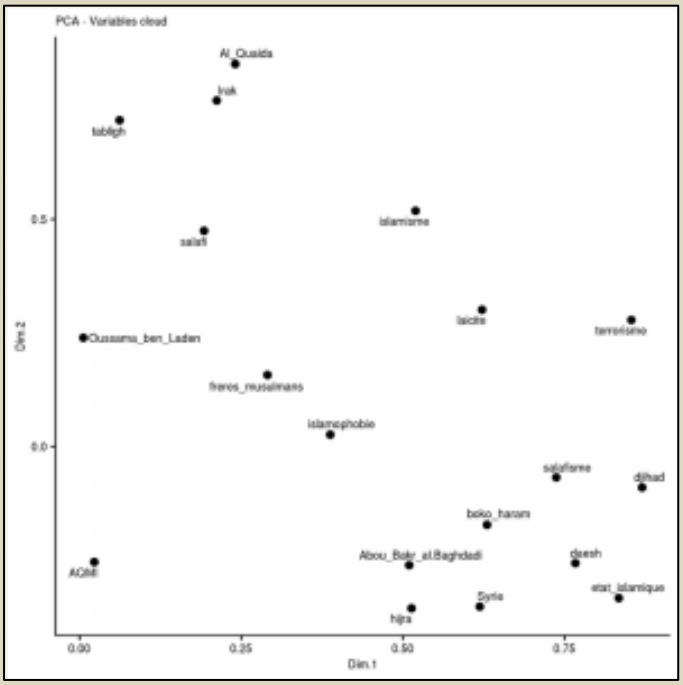
We also looked for terms indirectly linked to these topics in the public debate such as the concept of French secularism or 'laïcité' and the use of the word 'islamophobia'.
We tried to respond to the following questions:
1) What are the historical trends and the big picture of overall interest in Islamist terrorism in France? 2) Can we identify different phases in the way French Google users address jihadism and how this relates to different periods of jihadi activism?
3) Can we draw a statistical relationship between terrorism and jihadi-related events, on the one hand, and the increase in polarising public debates around 'secularism' and 'islamophobia' on the other?

2. Data

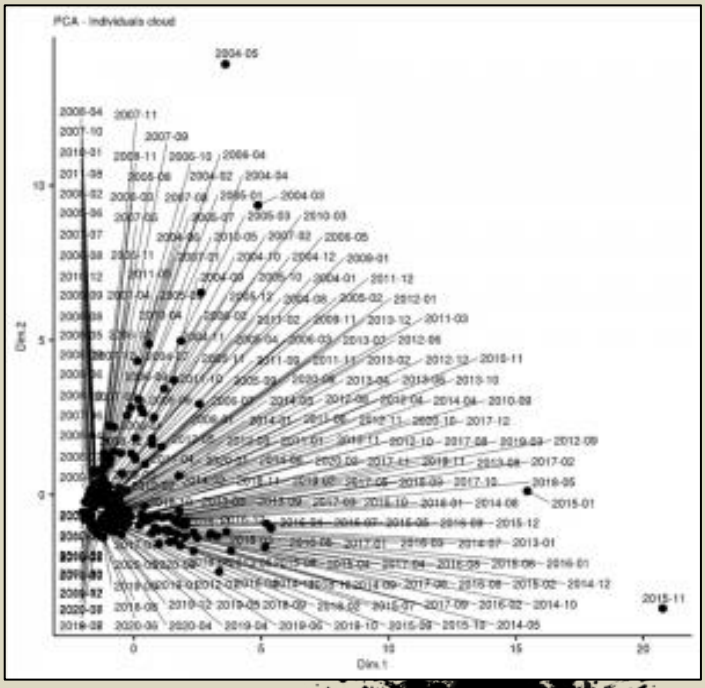
In order to do so, we looked at the frequency of the use of the following terms in French (here translated into English) in the Google search engine for the past sixteen years:
'jihad', 'islamism', 'salafi',' salafism','boko_haram","hijra","tabligh", "muslim_brothers", "islamophobia", "al_qaeda", "AQIM", "terrorism", "isis", "daesh", "islamic_state", "laicité", "iraq", "syria", "abu_bakr_al_baghdadi", "osama_bin_laden".
These data have been collected on a monthly basis following two multivariate analysis methods: a principal component analysis (PCA – which is a type of statistical treatment) and a manifold learning approach (UMAP).

3. Results

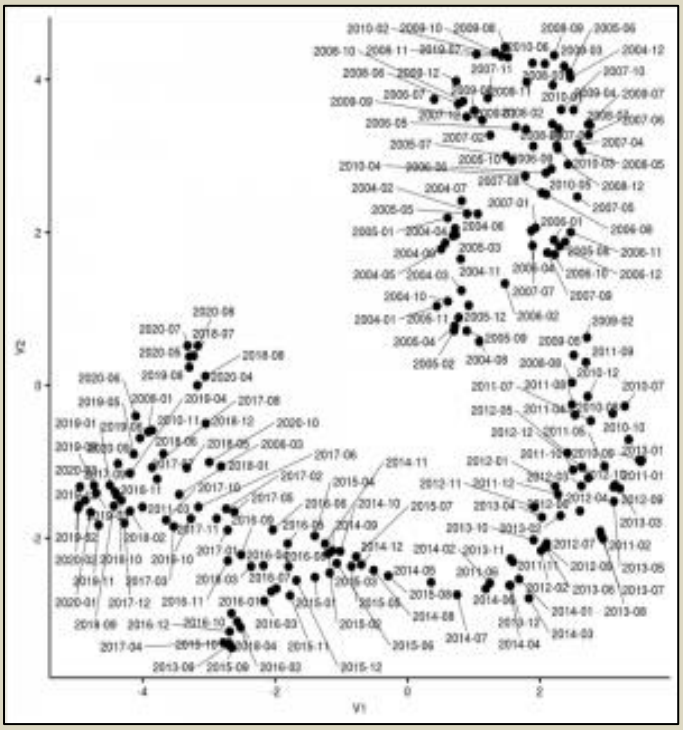
The PCA variables cloud shows a polarisation between two periods corresponding to two axes, one vertical concentration of the variables in the top-left-hand side) and the other horizontal (concentration in the bottom-right-hand side).
The vertical axis represents the prime dimension of PCA and is characterised by an interest for 'tablighi' movements and the relatively old and rare use of the word 'salafi'. These occurrences are associated with searches on al-Qaeda, Iraq, Osama bin Laden and to a lesser extent, AQIM. The second sub-group of words which appears on the horizontal axis underlines a strong concern about daesh, the Islamic State, hijra, Salafism and the situation in Syria. During this period, the jihadi leader who channels the biggest interest is Abu Bakr Al Baghdadi. One can note that 'laïcité' and 'islamophobia' are not fitting into this double-axis pattern. This indicates that concerns for Islam and the place of Muslims in the French society are not linked with concerns about jihadi groups. Both issues seem addressed independently from each other and following their own dynamics on the web search engine.



The PCA individuals cloud confirms a polarisation between two periods. It shows an early time, during which interests were focusing on the situation in Iraq, al-Qaeda, with little use of specific jihadi terms. On the opposite side of the spectrum, the period corresponding to the January 2015 'Charlie Hebdo and the hypercasher' onslaughts and the November 'Bataclan' massacres, underscores two peaks of requests about IS specificities and jihadi motives. Between these two episodes, the number of requests is close to normal. Moreover, in sharp contrast the Bastille Day 2016 Nice truck attack did not trigger the same amount of interest for French Internet users than those of 2015. Quite surprisingly, the data structure seems to imply that interests for these issues fluctuate significantly over time, skyrocketing after the first attacks and then falling rapidly afterwards and over the long run.



These preliminary results are then interpreted using UMAP technique or manifold learning approach which takes into account the data overall variations.
The UMAP individuals cloud provides complimentary insights. We clearly distinguish four different periods in the structure of requests on Google.
The first one goes from 2004 to 2010. Jihadism appears as an external and international issue taking shape around the struggle against al-Qaeda and the U.S. military intervention in Iraq and its offspring.



A second period stems from 2011 to summer 2014. It is marked by a decline in the search for terrorism-related issues, despite the Toulouse and Montauban attacks in March 2012, the first purported by a jihadi on French soil since 1996. At the same time, hundreds of French joined the jihad in Syria and Iraq, without this seeming to attract peculiar attention on the web.
A third 'wake-up call' sequence spreads from 2014 to 2017. It corresponds to the rise of IS in the Levant and the subsequent terror campaign in France that deeply impacted French society. Searches are characterised by words expressing resilience and anger but also anxiety and nervousness that have so far been latent.
The clash around Charlie Hebdo's editorial lines takes shape during this phase and remains to this day very vivid (especially since airings for the trial are taking place in France). Meanwhile jihadi-supporting groups are using this debate to mobilise sympathisers.
The last and ongoing period starts at the end of 2017 and is marked by a new decline for terrorism-related features. This can be explained by the fall of IS's self-proclaimed caliphate in the Levant and the rise of other issues debated on the Internet, such as the Yellow vest movement and the Covid-19 crisis. They have relegated radical Islam issues in the background, for an uncertain period of time.

Conclusion

This preliminary overview and analysis of Google Trends Data show different ruptures in French approaches and relations to jihadism. Although a homegrown deeply rooted jihadism was operating in France since the early 2000s, this phenomenon was first perceived as an international and distant issue. It only became of major domestic concern after it manifested violently and bluntly on French soil in 2015, and for a relatively short period of time afterwards.
By the end of 2017, it has been degraded to a secondary concern in a context of social and sanitary crisis. Yet, an indirect understanding of these results is that the study of jihadism must be consistent in relatively untroubled times, which tends to correspond to internal transitional phases within European jihadi movements.

Detecting "Deepfake" Videos by Checking for the Pulse

Source: http://www.homelandsecuritynewswire.com/dr20201029-detecting-deepfake-videos-by-checking-for-the-pulse

Oct 29 – With video editing software becoming increasingly sophisticated, it's sometimes difficult to believe our own eyes. Did that actor really appear in that movie? Did that politician really say that offensive thing?
Some so-called "deepfakes" are harmless fun, but others are made with a more sinister purpose. But how do we know when a video has been manipulated?
Researchers from Binghamton University's Thomas J. Watson College of Engineering and Applied Science have teamed up with Intel Corp. to develop a tool called FakeCatcher, which boasts an accuracy rate above 90 percent.
FakeCatcher works by analyzing the subtle differences in skin color caused by the human heartbeat. Photoplethysmography (abbreviated as PPG) is the same technique used for a pulse oximeter put on the tip of your finger at a doctor's office, as well as Apple Watches and wearable fitness tracking devices that measure your heartbeat during exercise.

"We extract several PPG signals from different parts of the face and look at the spatial and temporal consistency of those signals," said Ilke Demir, a senior research scientist at Intel. "In deepfakes, there is no consistency for heartbeats and there is no pulse information. For real videos, the blood flow in someone's left cheek and right cheek — to oversimplify it — agree that they have the same pulse."

Working with Demir on the project is Umur A. Ciftci, a PhD student at Watson College's Department of Computer Science, under Professor Lijun Yin's supervision at the Graphics and Image Computing Laboratory, part of the Seymour Kunis Media Core funded by donor Gary Kunis '73, LHD '02 It builds on Yin's 15 years of work creating multiple 3D databases of human faces and emotional expressions. Hollywood filmmakers, video game creators and others have utilized the databases for their creative projects. At Yin's lab in the Innovative Technologies Complex, Ciftci has helped to build what may be the most advanced physiological capture setup setup in the United States, with its 18 cameras as well as in infrared. A device also is strapped around a subject's chest that monitors breathing and heartrate. So much data is acquired in a 30-minute session that it requires 12 hours of computer processing to render it.

"Umur has done a lot of physiology data analysis, and signal processing research started with our first multimodal database," Yin said. "We capture data not just with 2D and 3D visible images but also thermal cameras and physiology sensors. The idea of using the physiology as another signature to see if it is consistent with previous data is very helpful for detection."

Deepfakes found "in the wild" are many steps below the kind of quality that Yin's lab generates, but it means that manipulated videos can be much easier to spot.

"Considering that we work with 3D using our own capture setup, we generate some of our own composites, which are basically 'fake' videos," Ciftci said. "The big difference is that we scan real people and use it, while deepfakes take data from other people and use it. It's not that different if you think about it that way.

"It's like the police knowing what all the criminals do and how they do it. You understand how these deepfakes are being done. We learn the tricks and even use some of them in our own data creation."

Since the FakeCatcher findings were published, 27 researchers around the world have been using the algorithm and the dataset in their own analyses. Whenever these kinds of studies are made public, though, there are concerns about telling malicious deepfake makers how their videos have been shown to be false, allowing them to modify their work to be undetectable in the future.

Ciftci is not too worried about that, however: "It's not going to be easy for someone who doesn't know much about the science behind it. They can't just use what's out there to make this happen without significant software changes."

Intel's involvement in the FakeCatcher research is connected to its interests in volumetric capture and augmented/virtual reality experiences. Intel Studios operates what Demir calls "the world's largest volumetric capture stage": 100 cameras in a 10,000-square-foot geodesic dome that can handle about 30 people simultaneously — even a few horses once.

Future plans include volumetric-capture technology to be included in mainstream television shows, sports and augmented-reality applications, where the audience can immerse in any scene. Films in 3D and VR also are in the works, with two VR projects recently premiering at the Venice Film Festival.

By compiling the FakeCatcher data and reverse-engineering it, Intel Studios hopes to make more realistic renderings that incorporate the kind of biological markers that humans with real heartbeats have.

"Intel's vision is changing from a chip-first company to putting AI, edge computing and data first," Demir said. "We are making a transformation to AI-specific approaches in any way we can."

(Interesting to note: Intel's CEO is Bob Swan, MBA '85, who last year told the School of Management magazine *Reaching Higher* that "intellectual curiosity is a wonderful and powerful thing to help you grow and develop and evolve over time.")

Future research will seek to improve and refine the FakeCatcher technology, drilling further down into the data to determine how the deepfakes are made. That capability has many implications, including cybersecurity and telemedicine, and Yin also hopes for further collaborations with Intel.

"We're still in the brainstorming stage," he said. "We want to have an impact not only in academia but also to see if our research would have a role in industry."

Facial Recognition will Outlast COVID-19

By Alejandra Bringas and Kevin Kohler

Source: https://isnblog.ethz.ch/technology/facial-recognition-will-outlast-covid-19

Image courtesy of StockSnap/Pixabay

Sep 30 – The COVID-19 pandemic has led to an unprecedented spread of facial coverings while simultaneously accelerating the adoption of digital surveillance tools, including facial recognition systems (FRS). However, whereas the facemasks will disappear again, FRS are not only poised to stay, but to keep on expanding. Consequently, governments should address the issues of bias and robustness by testing and certifying FRS. Even more importantly, there is a need to explore and discuss acceptable socio-technical configurations (cultural norms, technical standards, infrastructure, laws, etc.) around the increased legibility of citizens to the state.

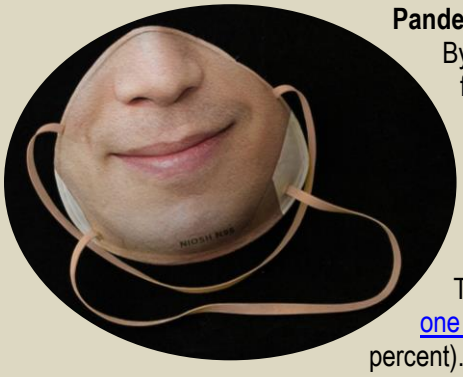
Faces are the most common patterns used by humans to identify others in everyday life. Consequently, faces are a part of governmental identity documents, such as passports or driver's licenses, as well as more informal ones, such as membership cards or social media profiles. In Western societies, there is an implicit agreement to reveal our face as a prerequisite to social relationships. However, because the face is such a central feature of identity and identification, we want to control it and its use. Hence, most of us would find it unacceptable if a stranger were to take a photograph of our face in the street without any further explanation.

FRS detect human faces in image data and match them with facial structures in a databank. Facial authentication or verification matches a captured face with the stored unique facial characteristics of an individual to verify that a person is who he or she claims to be (1:1). Facial recognition or identification is capable of uniquely identifying a person based on sensor data of facial contours (1:N). FRS have made significant progress in the last years due to the adoption of deep neural networks. More specifically, the lowest false negative identification rate in tests by the National Institute of Standards and Technology (NIST) has decreased about 27-fold since 2014. At the same time, the global number of surveillance cameras is growing by about 300'000 per day and is expected to surpass 1 billion in 2021.

The Visual Cortex of Leviathan

As James Scott argues in *Seeing Like A State*, governments have a long history of trying to make their citizenry more legible to them. As an example, even last names were originally forced onto people to make it easier to collect taxes and draft individuals into the armed forces. FRS can be seen as a continuation of this trend and framed as part of the metaphorical "visual cortex" of the state, allowing it to make sense of the exponentially growing input from its "eyes", turning Hobbes' Leviathan increasingly into Argus Panoptes, the many-eyed giant. Unlike other biometric technologies, such as DNA tests or fingerprint scanners, FRS neither require the active participation nor the consent of the subject. They

are non-intrusive, contact-free processes and relatively inexpensive, which makes them an increasingly effective and widespread surveillance tool.
Pushing back against this, in 2019, protesters against governments in places such as Hong Kong and Chile have not only masked their faces but actively tried to interfere with and disable surveillance cameras in order to protect their anonymity. In return, Hong Kong's Chief Executive Carrie Lam invoked emergency powers in October 2019 to prohibit all kinds of facial coverings at public gatherings. Violations of the ban were punished with a hefty fine and up to a year in prison.



Pandemic Adaption and Adoption

By early 2020, following the spread of COVID-19, nearly everyone in Hong Kong wore facemasks and, eventually, in July, the government made their use mandatory in public places. This 180-degree turn is emblematic for the worldwide shift towards masking faces during the pandemic. Accordingly, the symbolic meaning of masks was also temporarily reversed, changing an anonymity tool worn by revolutionaries into a symbol of conformism. However, this reversal is unlikely to last for long, and it hasn't stopped governments from using FRS to identify citizens in public spaces.
The false non-match rate of pre-COVID-19 face verification algorithms is on average around one order of magnitude higher on masked faces (ca. 5 percent) than on unmasked ones (ca. 0.3 percent). However, suppliers such as SenseTime, Baidu, or FaceGo have been very quick to retrain their algorithms on masked faces. As governments have adopted a large variety of digital tools to monitor and enforce compliance with social distancing and quarantine rules, they have also turned to facial recognition. For example, the city of Shanghai even installs the technology at gates and in the elevators of residential buildings to reduce contact with shared physical surfaces, and FRS partnered with temperature checks are used widely across China. Furthermore, several countries have used FRS to monitor quarantined citizens, either to identify their faces in citywide CCTV networks, such as in Moscow, or to verify that they are at their homes via their smartphones, such as in Poland and India.

Tech Backlash

Whereas the pandemic has led to calls to double down on FRS and surveillance systems in China, there has been a massive backlash against the technology in the US in the wake of COVID-19 and the George Floyd protests. Specifically, citizens criticized the use of FRS for contact tracing at the protests, its use for border control, and the supposedly discriminatory effects on law enforcement due to a *lower* ability to identify women and people of color. Subsequently, in June 2020, IBM decided to abandon its research in this field, whereas Microsoft and Amazon halted their collaboration with law enforcement. The EU had mulled a moratorium on FRS as well, but eventually recommended in its AI whitepaper that FRS "should be only used when subject to adequate safeguards" as "by analyzing large amounts of data and identifying links among them, AI may be used to de-anonymize data […] creating new personal data protection risks".
In democracies, such an approach is preferable to a wholesale moratorium, as FRS unquestionably has applications that create social value, such as finding missing children. At the same time, there is a need to build up capacities to test, and possibly certify, FRS in terms of accuracy, including for different demographics. This would help the population to trust that the technology is working properly and would show that gender and racial biases are less pronounced and more solvable than the public discourse on the subject might indicate.
The larger and more challenging questions arise from the new possibilities that a loss of anonymity in public spaces gives to different actors. It is easy to see how a technology that helps to track individuals in public spaces in real time could favor the centralization of power and allow for more stringent enforcement of norms and laws, as well as the targeted surveillance and suppression of dissenters. This is of course particularly problematic in places that have no rule of law or respect for human rights. For example, there are still countries with massive discrimination against homosexuals, including capital punishment. Hypothetically, they might use FRS to predict the sexual identity of individuals. In an example that is already a reality, China has specifically trained FRS to detect members of its persecuted Uighur minority in public spaces, "ushering in a new era of automated racism".
Consequently, legally binding rules are needed to protect citizens' rights and avoid disproportionate surveillance actions. Specifically, there should be transparency regarding how and for what purpose authorities use FRS and CCTV networks. However, the domestic and international debates on which norms and legislation around FRS are needed specifically to keep public authorities and private companies accountable will take time. Hence, in democracies, it is also up to civil society to check that the FRS that are now being developed and deployed – in part due to the extraordinary circumstance of controlling a global pandemic – will still be subject to proportionate and necessary measures in a post-COVID era. Unfortunately, the autocratic

systems that embrace this technology already have little to no civil society, and those individuals that remain part of it might soon wake up to an FRS installed on their door.

Alejandra Bringas *has an International Master in Security, Intelligence and Strategic Studies by the University of Glasgow, Dublin City University and Charles University.*
Kevin Kohler *is a researcher in the Cyber Defense Team at the Center for Security Studies (CSS) at ETH Zurich.*

New Way to Secure Critical Infrastructure

Source: https://i-hls.com/archives/104949

Oct 31 – A new project launched in Japan aims at improving the security of critical infrastructure using artificial intelligence (AI) solutions. The non-profit organisation IOTA Foundation, developing next generation protocols for the connected world, is partnering with the Japanese government and the New Energy and Industrial Technology Development Organisation (NEDO), Japan's national research and development agency.
The goal of the project is to develop technology to strengthen the security, longevity, and durability of critical infrastructure assets in Japan and abroad. By adding AI and distributed ledger technology to Risk Based Maintenance (RBM) Systems deployed in power plants, energy plants, industrial plants, petrochemicals and oil refining plants.
This type of predictive maintenance system that shares industry data using a distributed database is set to be the first of its kind in the world. While damage prediction assessment based on the current RBM standards exists, most processes are still left up to field workers to do manually.
To further optimise these systems, maintenance data will be digitised and processed by an artificial intelligence system to predict when and which parts of a plant are going to require maintenance. This will reduce unplanned outages, improve plant availability and lower costs by reducing unnecessary inspections and repairs.
The project will develop a cloud-based SaaS software. It will be based on a decentralised database using IOTA's distributed ledger technology.
Distributed ledger technology (DLT) is a digital system for recording the transaction of assets in which the transactions and their details are recorded in multiple places at the same time. Unlike traditional databases, distributed ledgers have no central data store or administration functionality. Blockchains are one form of distributed ledger technology.
Centralised databases are vulnerable to accidents, tampering and leakage. By building an RBM using IOTA, maintenance companies are able to provide a solution to infrastructure partners that is resistant to cyber-attacks while protecting sensitive data.
Thanks to the artificial intelligence system created, information can be captured, shared, and acted upon by distributed teams across the world, according to smart-energy.com.

US hospital systems facing 'imminent' threat of cyber-attacks, FBI warns

Source: https://www.theguardian.com/society/2020/oct/28/us-healthcare-system-cyber-attacks-fbi

Oct 30 – Federal agencies have warned that the US healthcare system is facing an "increased and imminent" threat of cybercrime, and that cybercriminals are unleashing a wave of extortion attempts designed to lock up hospital information systems, which could hurt patient care just as nationwide cases of Covid-19 are spiking.
In a joint alert on Wednesday, the FBI and two federal agencies warned that they had "credible information of an increased and imminent cybercrime threat to US hospitals and healthcare providers". The alert said malicious groups are targeting the sector with attacks that produce "data theft and disruption of healthcare services".
The cyber-attacks involve ransomware, which scrambles data into gibberish that can only be unlocked with software keys provided once targets pay up. Independent security experts say it has already hobbled at least five US hospitals this week, and could potentially affect hundreds more.
The offensive by a Russian-speaking criminal gang comes less than a week ahead of the election, although there is no immediate indication they were motivated by anything but profit.
"We are experiencing the most significant cybersecurity threat we've ever seen in the United States," Charles Carmakal, chief technical officer of the cybersecurity firm Mandiant, said in a statement.
Alex Holden, CEO of Hold Security, which has been closely tracking the ransomware in question for more than a year, agreed that the unfolding offensive is unprecedented in magnitude for the US, given its timing in the heat of a contentious presidential election and the worst global pandemic in a century.

The federal alert was co-authored by the Department of Homeland Security and the Department of Health and Human Services.
The US has seen a plague of ransomware over the past 18 months or so, with major cities from Baltimore to Atlanta hit and local governments and schools hit especially hard.
In September, a ransomware attack hobbled all 250 US facilities of the hospital chain Universal Health Services, forcing doctors and nurses to rely on paper and pencil for record-keeping and slowing lab work. Employees described chaotic conditions impeding patient care, including mounting emergency room waits and the failure of wireless vital-signs monitoring equipment.
Also in September, the first known fatality related to ransomware occurred in Duesseldorf, Germany, when an IT system failure forced a critically ill patient to be routed to a hospital in another city.
Holden said he alerted federal law enforcement on Friday after monitoring infection attempts at a number of hospitals. He said the group was demanding ransoms well above $10m per target and that criminals involved on the dark web were discussing plans to try to infect more than 400 hospitals, clinics and other medical facilities.
"One of the comments from the bad guys is that they are expecting to cause panic and, no, they are not hitting election systems," Holden said. "They are hitting where it hurts even more and they know it."
Carmakal described the eastern European group as "one of most brazen, heartless, and disruptive threat actors I've observed over my career".
The cybercriminals launching the attacks use a strain of ransomware known as Ryuk, which is seeded through a network of zombie computers called Trickbot that Microsoft began trying to counter earlier in October.
While no one has proven suspected ties between the Russian government and gangs that use the Trickbot platform, Holden said he has "no doubt that the Russian government is aware of this operation – of terrorism, really". He said dozens of different criminal groups use Ryuk, paying its architects a cut.

U.S. Bracing for Attacks Before and After Election Day

Source: http://www.homelandsecuritynewswire.com/dr20201031-u-s-bracing-for-attacks-before-and-after-election-day

Oct 31 – U.S. intelligence officials have already confirmed attacks on the election have been underway for some time, with Russia, China and Iran all waging operations designed to influence the way voters cast their ballots. And more recently, intelligence officials warned that Russia and Iran managed to acquire voter registration data while hacking into U.S. databases. In another significant difference from the 2016 and 2018 elections, intelligence and election security officials warn that, this time, the assault on the election will not end when the polls close. Instead, they say the attacks will persist, likely until at least the presidential inauguration on January 20, 2021.

Four Years Since the Mirai-Dyn Attack: Is the Internet Safer?

Source: http://www.homelandsecuritynewswire.com/dr20201102-four-years-since-the-miraidyn-attack-is-the-internet-safer

Nov 02 – On 21 October 2016, millions of household IoT devices were infected with the malware Mirai and instructed to send data requests to Dyn, a widely used Domain Name Server (DNS) that acts like a switchboard for the Internet. This tidal wave of requests crashed over 175,000 domains—including Twitter, PayPal, and other web giants—for several hours, affecting tens of millions of users.
Four years later, is the Internet more resilient? A team of Carnegie Mellon University CyLab researchers are presenting a new studyaimed at answering that very question at this week's Internet Measurement Conference.
"It seems that the lessons learned from the 2016 Dyn attack have only been acted upon by a handful of websites that were directly impacted," saysAqsa Kashaf, a Ph.D. student in Electrical and Computer Engineering (ECE)Opens in new window and lead author of the new study (view a video of Kashaf's presentation).
The Mirai-Dyn attack in 2016 was successful because of what Kashaf and her team refer to as critical dependencies. The domains affected by the Mirai-Dyn attack were critically dependent on Dyn, a third-party DNS. In other words, they relied solely on Dyn, so when Dyn went down, so did they.
To assess how websites have (or have not) changed since the 2016 attack, Kashaf and her co-authors analyzed 100,000 of the most popular websites as ranked by Alexa Internet, a web traffic analysis company. They looked at the dependencies of those websites in 2016 and then compared them with dependencies in 2020.
"Since the Dyn attack had such a huge impact, you would think websites would adapt as a result," says Kashaf.

Turns out, overall, critical dependency on DNS providers has in fact increased around five percent in 2020 compared to 2016. However, the researchers note, more popular websites have adapted to decrease their critical dependency.

"We interpret this to mean that the most popular websites care more about availability than the less popular ones," says Kashaf.

The researchers also focused on dependencies of two other services associated with delivering content to users online, both of which are performed in the blink of an eye when a user navigates to a website: content delivery networks, which host and deliver the content a user sees (e.g., video content for streaming), and certificate validation from a certificate authority, which confirms a secure connection.

The researchers found similar results: they observed little to insignificant changes in critical dependencies relative to 2016, but the most popular websites had decreased their dependencies.

This problem of critical dependencies isn't unique to websites, the researchers say. They ran two preliminary case studies of two other sectors—hospitals and smart home companies—and found that third-party dependencies leave these sectors vulnerable to Mirai-Dyn-like attacks as well.

"One obvious recommendation for websites is that they should build in more resilience and redundancy when using third party services," says Kashaf. "…and service providers need to support and encourage this redundancy. You can't have just a single point of failure."

Moving forward, the researchers envision building a tool that would allow web administrators to easily analyze and inspect their own website's dependency structure, empowering them to make informed decisions in choosing new service providers.

5G Is Here: Get Ready for the Cybersecurity Battles of Tomorrow

By Paul Ferrillo and Chuck Brooks

Source: https://www.hstoday.us/subject-matter-areas/infrastructure-security/5g-is-here-get-ready-for-the-cybersecurity-battles-of-tomorrow/

Nov 04 – The worldwide rollout of 5G will create innumerable benefits for the enterprise business community and the U.S. economy. Advanced 5G and wireless networks will bring a huge selection of benefits, including higher traffic capacities, lower latency, and increased reliability. It will empower millions by broadband connectedness. It will impact commercial verticals such as retail, health, and financial by enabling processing and analytics in real time. In essence, 5G will function as a data superhighway.

Although 5G is in the initial stages of deployment, connectivity is already exponentially expanding. The industry trade group 5G Americas cited an Omdia report that counted more than 17.7 million 5G connections at the end of last year, including a 329 percent surge during the final three months of 2019. Omdia is also predicting 91 million 5G connections by the end of 2020. (1)
The 5G ecosystem is gathering a wide range of investments and it will have financial implications. A GSMA industry report (GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with almost 400 companies in the broader mobile ecosystem) predicts 5G technology will add $2.2 trillion to the global economy over the next 15 years. And operators are expected to spend more than $1 trillion on mobile capex between 2020 and 2025, with 80 percent of that spend directed at their 5G networks. (2)

Security and 5G

5G speed, performance, capacity, and connectivity will necessitate the need for better security. As with any new technology 5G is not without its security concerns. Many of these issues have been out front in security discussions due to our highly charged political environment regarding 5G's supply chain roots and controls emanating from China. But there are also significant risks from an increased attack surface that 5G will foster.
A Brookings Institution report, "Why 5G Requires New Approaches to Cybersecurity," written by former FCC Chairman Tom Wheeler and Rear Adm. David Simpson (ret), former chief of the FCC's Public Safety and Homeland Security Bureau, outlines five clear security challenges of 5G. They note that:

1. "The network has moved away from centralized, hardware-based switching to distributed, software-defined digital routing. Previous networks were hub-and-spoke designs in which everything came to hardware choke points where cyber hygiene could be practiced. In the 5G software defined network, however, that activity is pushed outward to a web of digital routers throughout the network, thus denying the potential for chokepoint inspection and control.
2. 5G further complicates its cyber vulnerability by virtualizing in software higher-level network functions formerly performed by physical appliances. These activities are based on the common language of Internet Protocol and well-known operating systems. Whether used by nation-states or criminal actors, these standardized

building block protocols and systems have proven to be valuable tools for those seeking to do ill.

3. Even if it were possible to lock down the software vulnerabilities within the network, the network is also being managed by software—often early generation artificial intelligence—that itself can be vulnerable. An attacker that gains control of the software managing the networks can also control the network.
4. The dramatic expansion of bandwidth that makes 5G viable creates additional avenues of attack. Physically, low-cost, short range, small-cell antennas deployed throughout urban areas become new hard targets. Functionally, these cell sites will use 5G's Dynamic Spectrum Sharing capability in which multiple streams of information share the bandwidth in so-called "slices"—each slice with its own varying degree of cyber risk. When software allows the functions of the network to shift dynamically, cyber protection must also be dynamic rather than relying on a uniform lowest common denominator solution.
5. Finally, of course, is the vulnerability created by attaching tens of billions of hackable smart devices (actually, little computers) to the network colloquially referred to as IoT. Plans are underway for a diverse and seemingly inexhaustible list of IoT-enabled activities, ranging from public safety things, to battlefield things, to medical things, to transportation things—all of which are both wonderful and uniquely vulnerable." (3)

Security requirements to mitigate threats are being prioritized by both the public and private sectors. In government, 5G communications technology has been recognized as a foundational enabler for all U.S. defense modernization programs. The Department of Defense (DOD) is engaged at the forefront of cutting-edge 5G testing and experimentation. DOD is committed via new research and development budgets and programs to exploring a wide range of potential applications and dual-use opportunities that can be built upon 5G next-gen networks. Recently DOD selected five locations and $600 million in awards for 5G testing that represents the largest global full-scale 5G test for dual-use applications. (4)

On the civilian side of the federal government the Department of Homeland Security (DHS) and the nation's risk advisor, CISA, has determined that 5G implementation will introduce vulnerabilities. A summary of their findings in critical areas includes:

- **Supply Chain**: Risks of malicious software and hardware, counterfeit components, and poor designs, manufacturing processes, and maintenance procedures.
- **Deployment:** Improperly deployed, configured, or managed 5G equipment and networks may be vulnerable to disruption and manipulation.
- **Network Security**: Legacy vulnerabilities, such as Distributed Denial of Service attacks and SS7/Diameter challenges.
- **Competition and Choice**: Lack of interoperability with other technologies and services limits the ability of trusted ICT companies to compete in the 5G market. (5)

Cybersecurity Measures: Preparing for 5G

Because of myriad technological and policy challenges, it is critical that enterprises create a sense of urgency to prepare for the implementation and assimilation of 5G technologies. There are some things that enterprises should concentrate on to help deal with these security concerns. Yes, many of the below are "old friends" but they are needed still in light of the security challenges that 5G potentially creates:

Action Items:

1) Monitor your external supply chain to check what your providers are doing to keep secure – supply chain risk management was the focus of NIST cybersecurity framework 1.1. It should still be a concern today given 5G as many businesses are going to be sending huge amounts of data to cloud service providers, co-location centers, and other third parties via wireless transmissions. What are these providers doing as far as data security? What standards *do* they adhere to? What standards *should* they be adhering to given business needs (like HIPAA or SEC OCIE standards)? Much depends upon the strength of your own supply chain risk management program. Some companies can evaluate the cybersecurity of other entities on a regular and somewhat comprehensive basis. Others have less ability and fewer resources to do so. Here it is suggested that companies demand SOC 2 Type 2 reports that "define criteria for managing customer data based on five 'trust service principles' – security, availability, processing integrity, confidentiality and privacy." (6)

2) Know what is on your network — time to clean up your network and your data. Given that 5G does not erase traditional security concerns, it is time to make sure all OS and other cybersecurity solutions are updated and patched regularly to make sure as many security holes as possible get closed. This includes not only network devices, but laptops and other personal, smart devices like iPads and iPhones. Know where on your network your most critical data is. Protect it like it was sitting in Fort Knox.

3) Data in, Data out? 5g will move a lot of data. Faster than ever before. An attacker could do that just as easily as your company. Figure out first: (a) where your data is going on a regular basis (i.e. the cloud) so that when you are reviewing your logs you understand "normal activity," in terms of location but in terms of amounts as well too, so that you can then, (b) figure out where your data should NOT be going (i.e. China or Russia), and what amounts of data in transit are usual or not usual to

better understand potential data exfiltration issues. Accurate and timely log review will continue to be critical in a 5G environment.
4) Make sure your endpoints are updated, patched and monitored. In today's pandemic/COVID-19-filled world, the endpoint has taken on an increased focus as more and more people continue to remotely work from home. People are using all sorts of devices to connect, and more and more are coming to the market each week. Obviously, this creates thousands or more endpoints (if not millions more) than we ever had before. What is your company doing to monitor your employee when he or she logs in from home? Is that employee using his home internet, a VPN or wireless services? There are lots of questions here that need to be answered. But if "data is the new cash" your endpoint could be the attacker's cash register.
5) Encrypt or tokenize all data transmitted wirelessly. There are many telecoms that will be pursuing encryption of data that you push to them/through them. Anti-tracking and spoofing features that make it harder for bad actors on a network to track and manipulate individual device connections. To do this, 5G encrypts more data, so less is flying around in the clear for anyone to intercept. 5G is also a much more software- and cloud-based system than previous wireless networks, which will allow for better monitoring to spot potential threats. (7)
One of the missing links here: Why not encrypt or tokenize all data in transit before it hits the wireless tower? We should be doing this anyway but the encryption discussion in the U.S. has taken several left turns even though more and more individuals and businesses are using encryption to secure their data.
6) You have heard it before: Pay attention to the basics. You have heard it before from groups like The CyberAvengers: The Foundation of Good Cybersecurity is paying attention to the basics both at the employee level (through a solid and regular training program) and at the enterprise level. (See Back to Basics: Creating a Culture of Cybersecurity at Work.) Make sure your basic cybersecurity policies and procedures, e.g. your incident response, business continuity and crisis management policies, along with your privacy policy and your updating/patching policies, are fully up to date and recently reviewed. 5G does not mean you will not be breached; 5G does not mean you will not be hacked. An effective and practiced incident response plan is your best defense.
Finally, you have also read it here before that with an increased amount of internet traffic, and now with the increased speed of 5G, it is important to consider whether you have sufficient personnel or bandwidth to detect anomalous behavior on your network. It might be time to consider some sort of machine learning solution to both check and affirm an employee's access to the network (e.g. identity and access management), and to automatically monitor anomalous network behavior.
The above list is not mutually exclusive of other steps you might take to secure your network, but it's a start. As with any new technology, there will be new behaviors and new patterns of activity. Things will change. Things do change. But we know three things: there will be more network traffic, there will be more and faster network wireless traffic, and there will be many more IoT devices. This creates an opportunity once again to review your network security, devices, and solutions to make sure they can keep up with the new "pace" of 5G and the cybersecurity battles of tomorrow.

Sources:

1 &2) https://www.sdxcentral.com/articles/news/the-5g-economic-impact/2020/03/.
3) Please see "Why 5G Requires New Approaches to Cybersecurity," available at https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/.
4) https://allongeorgia.com/georgia-state-news/georgia-location-among-5-of-dept-of-defenses-600-million-5g-testing-installations/
5) https://www.dhs.gov/science-and-technology/news/2020/10/15/feature-article-5g-introduces-new-benefits-cybersecurity-risks
6) "SOC 2 Compliance," https://www.imperva.com/learn/data-security/soc-2-compliance/
7) See "Moving the Encryption Conversation Forward," available at https://carnegieendowment.org/2019/09/10/moving-encryption-policy-conversation-forward-pub-79573/. Creating true end to end encryption certain can help mitigate, in whole or in part, any potential risks associated with 5G.

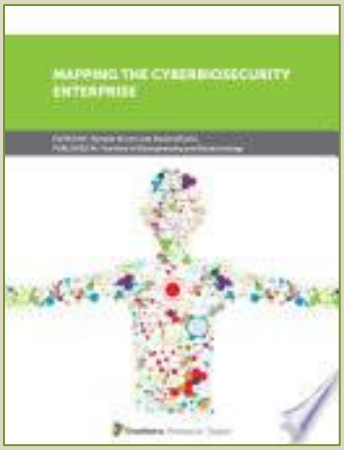
Paul Ferrillo *is a partner at the law firm of McDermott Will & Emer. He focuses his practice on corporate governance issues, complex securities class action, major data breaches and other cybersecurity matters, and corporate investigations. He is also an Adjunct Professor at Florida State University College of Law, and the current Director of the New York Chapter of Infraguard. Paul is author of the books Take Back Control of Your Cybersecurity Now: Game Changing Concepts on AI and Cyber Governance Solutions for Executives and Navigating the Cybersecurity Storm: A Guide for Directors and Officers*
Chuck Brooks*, President of Brooks Consulting International, is a globally recognized thought leader and subject matter expert Cybersecurity and Emerging Technologies. He is Adjunct Faculty at Georgetown University in the Cyber Risk Management and Applied Intelligence programs. During his career, Chuck received two Presidential Appointments, and served an executive for several leading public companies. LinkedIn named Chuck as one of "The Top 5 Tech People to Follow on LinkedIn." He was named by Thompson Reuters as a "Top 50 Global Influencer in Risk, Compliance," and by IFSEC as the "#2 Global Cybersecurity Influencer." He is also a Visiting Editor of Homeland Security Today.*

Mapping the Cyberbiosecurity Enterprise

By Randall Murch and Diane DiEuliis

Source: https://www.frontiersin.org/articles/10.3389/fbioe.2019.00235/full

Oct 03 – We are pleased to introduce this Research Topic in Frontiers in Bioengineering and Biotechnology on a new area of biosecurity, termed "Cyberbiosecurity." This term, originally introduced in the recently published strategic article by Murch et al. entitled "Cyberbiosecurity: An Emerging New Discipline to Help Safeguard the Bioeconomy (*Front. Bioeng. Biotechnol*. doi: 10.3389/fbioe.2018.00039), describes the security vulnerabilities that exist at the intersection of cybersecurity, cyber-physical security, and biosecurity.



Entitled "*Mapping the Cyberbiosecurity Enterprise*," this collective of papers was amassed to firmly establish this topic as a new discipline within biosecurity. Each article contributes to developing and presenting deeper understanding of this emerging topic, and helps to delineate the range of current and potential applications of cyberbiosecurity. We also anticipate that this collective will foster greater engagement between the biosecurity and cybersecurity communities.

"Cyberbiosecurity" has been defined as "understanding the vulnerabilities to unwanted surveillance, intrusions, and malicious and harmful activities which can occur within or at the interfaces of comingled life and medical sciences, cyber, cyber-physical, supply chain and infrastructure systems, and developing and instituting measures to prevent, protect against, mitigate, investigate and attribute such threats as it pertains to security, competitiveness, and resilience." While cybersecurity is a broad and well-researched existing field, its application to specific aspects of the life sciences necessitates a conjoining of experts from each discipline which have predominantly existed in silos to date. Defining cyberbiosecurity as a discipline is a necessary first step in bringing these disparate groups together to expand understanding of the risks from their relative perspectives.

Mapping the topology of cyberbiosecurity has just begun, but proponents have realized that it has expansive applications across the life sciences, most obviously in the biomedical and pharmaceutical domains. But as the digitization of biology grows, biotechnology is expanding far beyond these traditional silos. The purposeful engineering of biology, including application of the classical "design, build, test" cycle, is opening unprecedented opportunities for biomaterials and biofuels and their use, for agriculture and food systems (from large scale crop engineering to "farm to table"), and for bioinformatics and "AI" (from small field tools to large-scale complex systems and cloud computing). As biotechnologies continue to advance and evolve, cyberbiosecurity will be a key consideration in existing critical infrastructure related to all these arenas. Further, new components of critical infrastructure may emerge and be defined through advances in the synthetic biology industry, and cybersecurity will need to be assessed for those new components.

In our view, awareness and identification of vulnerabilities is an important first step in launching the field, followed by the development and implementation of mitigations and solutions. Eventually, practitioners in this growing field will be responsible for the development of guidelines and standards of governance, which will require adherence and compatibility with existing national defense strategies.

This Special Collection, represented by both U.S. and international contributors, includes writings on a number of the topical areas described above. Vulnerabilities associated with synthetic biological manufacturing are described, including specific discussions of biopharmaceutical production. The evolving platforms for biotechnology, including distributed manufacturing models and laboratory automation, are included for consideration. Importantly, a discussion of the public health and stability ramifications of cyberbiosecurity in settings outside the US are also considered. General themes in other fields, such as agriculture, biopharma, and labs of the future are represented in stand-alone contributions. Some technical aspects of tool development, such as DNA synthesis security screens, and access to pathogen genome databases provide insights on current thinking and perceptions of risk. Finally, broad consideration is given to cyberbiosecurity in the national security context, given any new aspect of biosecurity must mesh with existing national security approaches and frameworks in the biodefense realm. Authors have also provided discussions of options for training and strategies for workforce development, all of which can help to build not only a general awareness of cybersecurity among biologists and synthetic biology engineers, but potentially develop a core of cyberbiosecurity specialists or practitioners that will be needed for risk assessments and solutions.

It is our hope that this eclectic set of insights and perspectives will broadly stimulate academia, government, non-profits, and the private sector to identify, prioritize, resource and pursue research, and implement solutions in the realm of cyberbiosecurity. Such research, outcomes and change management should focus on risk analysis, methods and technologies, education and training, guidelines and standards, policy, regulations and legal frameworks.

2021 Predictions: Hackers will Continue to Exploit COVID-19 Vulnerabilities

Source: https://i-hls.com/archives/105317

Nov 21 – In 2021, remote working due to COVID-19 will require that organizations better secure their new distributed networks and cloud deployments to keep their applications and data protected, claims Check Point Software Technologies in its 2021 cyber security predictions.

This means enforcing and automating threat prevention at all points of the network – from employees' mobiles and endpoints, to IoT devices, to clouds – to stop advanced attacks from spreading rapidly across organizations, and exploiting weaknesses to breach sensitive data. Automating prevention will be critical, especially due to the ongoing cyber-skills shortage.

Among other pandemic-related predictions, the company warns that news of vaccine developments or new national restrictions will continue to be used in phishing campaigns, as they have been through 2020. The pharma companies developing vaccines will also continue to be targeted by malicious attacks from criminals or nation-states looking to exploit the situation.

Attacks will continue to disrupt remote learning activities over the coming year. The education sector experienced a 30 percent increase in weekly cyber attacks during the month of August, in the run up to the start of new semesters.

Q3 of this year saw a sharp rise in double-extortion ransomware attacks – hackers first extract large amounts of sensitive data, prior to encrypting a victim's databases. Then attackers threaten to publish that data unless ransom demands are paid, putting extra pressure on organizations to meet hackers' demands.

The botnet army will continue to grow: hackers have developed many malware families into botnets, to build armies of infected computers with which to launch attacks.

Cyber attacks by nation states will continue to grow, for espionage or to influence events in other countries. Microsoft reported that threat actors from just three countries launched 89 percent of nation-state hacking incidents over the past year. Over recent years, the focus has been on securing national critical infrastructure, and while this remains essential, it's also important to recognize the impact of attacks against other state sectors, including national healthcare organizations and Government departments.

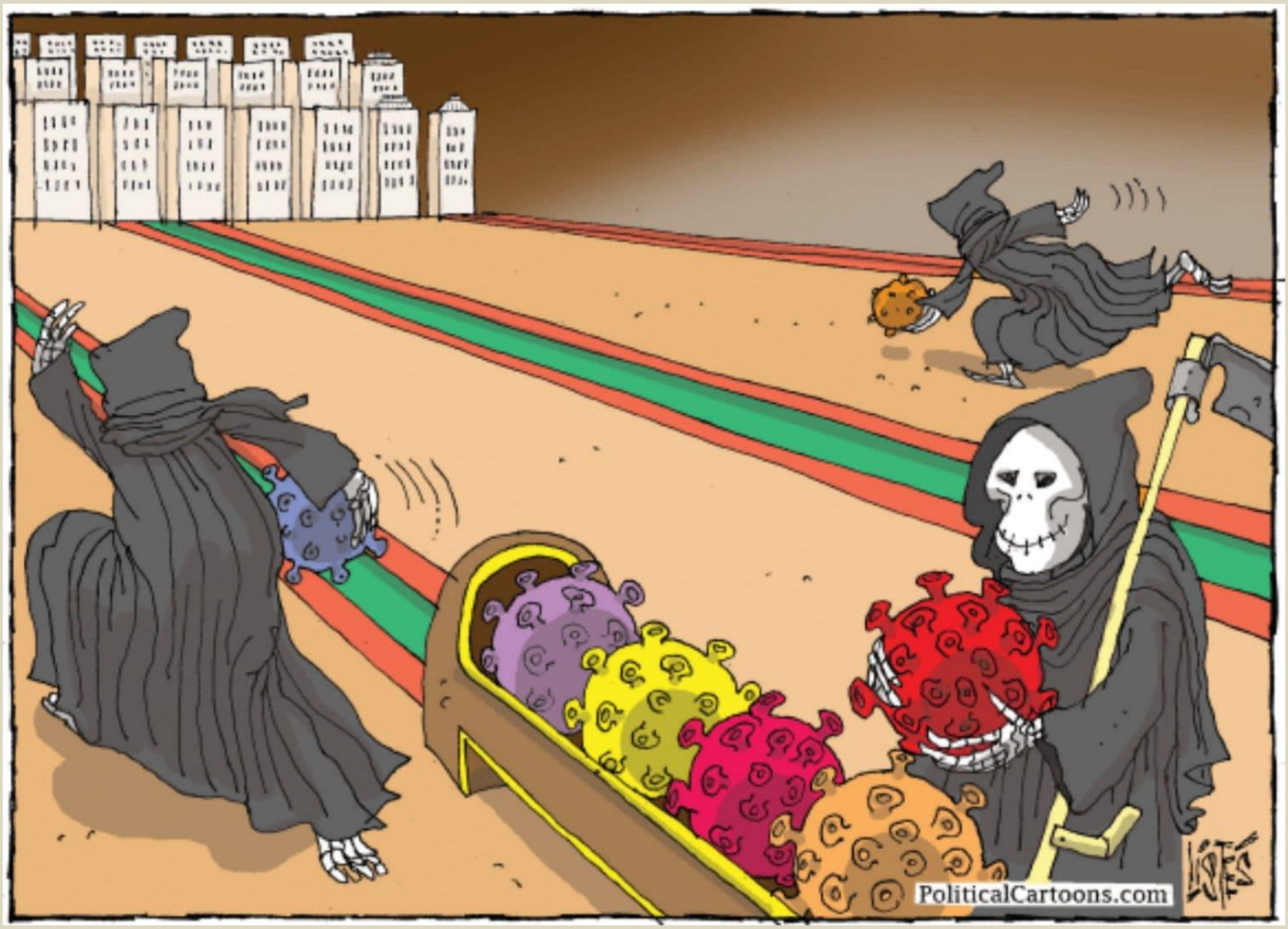
Techniques for fake video or audio are now advanced enough to be weaponized and used to create targeted content to manipulate opinions, stock prices or worse. Earlier this year, a political group in Belgium released a deepfake video of the Belgian prime minister giving a speech linking COVID-19 to environmental damage and calling for action on climate change. Many viewers believed the speech was real. At a simpler level, audio could be faked for voice phishing – so that a CEO's voice could be forged to bypass voice authentication.

The erosion in privacy has been magnified with buggy COVID-19 contact-tracing apps, which have privacy problems, leaking data about individuals. And that's just legitimate apps: mobile malware targeting users' banking credentials and committing click-fraud on adverts is a major growing threat.

5G benefits and challenges: the totally connected, high-speed world promised by 5G also gives criminals and hackers opportunities to launch attacks and cause disruption by targeting that connectivity. E-health devices will collect data about users' wellbeing, connected car services will monitor users' movements, and smart city applications will collect information

about how users live their lives. This massive volume of data from always-on, 5G devices will need to be protected against breaches, theft and tampering to ensure privacy and security against attacks, especially as a lot of this data will bypass corporate networks and their security controls.

As 5G networks roll out, the numbers of connected IoT devices will massively expand – drastically increasing networks' vulnerability to large scale, multi-vector cyber attacks. IoT devices and their connections to networks and clouds, are still a weak link in security: it's hard to get complete visibility of devices, and they have complex security requirements, according to continuitycentral.com.



ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

C2BRNE DIARY

DRONE NEWS

Drone Program for COVID-19 Era

Source: https://i-hls.com/archives/104631

Oct 21 – The UK Space Agency has backed a healthcare drone start-up that aims to help in the response to COVID-19. The medical drone delivery service will transport coronavirus samples, test kits and protective equipment between hospitals.
Apian, a start-up project founded by trainee doctors, can help free up healthcare staff, avoid courier waiting times and minimize the risk of virus transmission.
Forming part of the NHS Clinical Entrepreneur Program, Apian aims to establish a network of secure air corridors for electric drones which can carry COVID-19 samples, test-kits and PPE.
The **hybrid drones** — which have the rotors of a typical drone and the wings of a plane — can carry a maximum of 2 kilograms (4.4 pounds) and fly about 60 miles (96 kilometers.)
Their developers are trialing "dronepad" infrastructure so the miniature aircraft can take off from and land on hospitals, laboratories and warehouses. They are planning to scale up the trials and set up a nationwide network of secure air corridors to enable the drone delivery service to work safely across National Health Service sites – the UK's NHS Air Grid (NAG).
Apian is creating these corridors by working closely with the Civil Aviation Authority, UK Space Agency and the emergency services, according to businesscloud.co.uk.
The drone project is among others set to share 1.3 million pounds ($1.7 million) of funding from the U.K. Space Agency and the European Space Agency to businesses developing space-based solutions for challenges created by Covid-19, according to abcnews.go.com.

PERSPECTIVES ON TERRORISM Volume 14, Issue 5

Taking Fourth-Generation Warfare to the Skies? An Empirical Exploration of Non-State Actors' Use of Weaponized Unmanned Aerial Vehicles (UAVs—'Drones')

by Håvard Haugstvedt and Jan Otto Jacobsen

Source: https://www.universiteitleiden.nl/binaries/content/assets/customsites/perspectives-on-terrorism/2020/issue-5/haugstvedt-and-jacobsen.pdf

Recent events in and outside of conflict zones have raised apprehensions about the threat that Unmanned Aerial Vehicles (UAVs) might pose to modern societies. There have been reports of organizations like the Islamic State of Iraq and Syria (ISIS) weaponizing their UAVs. However, scholarly literature exploring this topic is scarce. This article brings forth findings from empirical evidence systematically collected and complied from open sources and databases (n = 440). Our findings demonstrate that non-state actors, especially in the Middle East, have acquired weaponized UAV capabilities. We have also found that non-state actors choose targets discriminately, preferring hard targets over soft targets, and that their UAV attacks have so far not led to mass casualties. However, the latter may change if target preferences change. These findings should further raise awareness of the threat posed by weaponized UAVs in non-state hands while acknowledging a disturbing implication for counterterrorism efforts—their bombs might become harder to stop.

▶▶ Read the full paper at source's URL.

Håvard Haugstvedtis *is a PhD Research Fellow at the Department of Social Studies, University of Stavanger.*
Jan Otto Jacobsen *is Associate Professor at the Department of Social Studies, University of Stavanger.*

EDITOR'S COMMENT: A very interesting paper with statistics that highlight the importance of the weaponization of UAVs in modern times. The message is that drones are force multipliers and should be taken seriously in order to avoid bloody surprises.

Risk in the Sky?

Tests performed at the University of Dayton Research Institute's Impact Physics Lab show that even small drones pose a risk to manned aircraft (Oct 2020)

Play (k)

Unmanned Aerial Vehicles Market: the roadmap after Covid-19, an accurate perspective on the market with insights upto 2025

Source: https://aerospace-journal.com/uncategorized/349623/unmanned-aerial-vehicles-market-the-roadmap-after-covid-19-an-accurate-perspective-on-the-market-with-insights-upto-2025/

Oct 29 – The Unmanned Aerial Vehicles market analysis is provided for the international markets including development trends, competitive landscape analysis, and key regions development status. The report provides key statistics on the market status of the Unmanned Aerial Vehicles manufacturers and is a valuable source of guidance and direction for companies and individuals interested in the industry.

Our industry professionals are working reluctantly to understand, assemble and timely deliver assessment on impact of COVID-19 disaster on many corporations and their clients to help them in taking excellent business decisions. We acknowledge everyone who is doing their part in this financial and healthcare crisis.

Major players covered in this report

Northrop Grumman (US), Aeryon Labs (Canada), Parrot (France), DJI (China), Textron (US), Boeing (US), General Atomics (US), and 3D Robotics (US).

The global Unmanned Aerial Vehicles market 2020 research is a professional and in-depth study on the current state of the industry and provides a basic overview of the industry including definitions, classifications, applications and industry chain structure. The Unmanned Aerial Vehicles market analysis is provided for the international markets including development trends, competitive landscape analysis, and key regions development status. Development policies and plans are discussed as well as manufacturing processes and cost structures are also analyzed. This report also states import/export consumption, supply and demand Figures, cost, price, revenue and gross margins.

This report presents the worldwide Unmanned Aerial Vehicles market size (value, production and consumption), splits the breakdown (data status 2016-2019 and forecast to 2026), by manufacturers, region, type and application. This study also analyzes the market status, market share, growth rate, future trends, market drivers, opportunities and challenges, risks and entry barriers, sales channels, distributors and Porter's Five Forces Analysis.

The report focuses on global major leading industry players of Unmanned Aerial Vehicles market providing information such as company profiles, product picture and specification, capacity, production, price, cost, revenue and contact information. Upstream raw materials and equipment and downstream demand analysis is also carried out. The Unmanned Aerial Vehicles market development trends and marketing channels are analyzed. Finally the feasibility of new investment projects are assessed and overall research conclusions offered.

With tables and figures helping analyze worldwide Unmanned Aerial Vehicles market, this research provides key statistics on the state of the industry and is a valuable source of guidance and direction for companies and individuals interested in the market.

The report gives a detailed description of drivers and opportunities in Unmanned Aerial Vehicles market that helps the consumers and potential customers to get a clear vision and take effective decisions. Different analysis models, such as, Unmanned Aerial Vehicles are used to discover the desired data of the target market. In addition to this, it comprises various strategic planning techniques, which promotes the way to define and develop the framework of the industries.

Global Unmanned Aerial Vehicles Market Segmentation

By Type:

By UAV Type, (Fixed-Wing UAVs,Multirotor UAVs,Single Rotor UAVs,Hybrid VTOL UAVs), By Class, (Small UAVs,Tactical UAVs,Strategic UAVs,Special Purpose UAVs), By System, (UAV Airframe, By Material Type,UAV Avionics,UAV Propulsion Systems, By Component,UAV Software,UAV Cameras, By Type,UAV CBRN Sensors,UAV Intelligence Payloads, By Type,UAV Radar, By Type,UAV LiDAR,UAV Gimbals,Others), By Mode of Operation, (Remotely Operated UAVs,Semi-Autonomous UAVs,Fully-Autonomous UAVs), By Range, (Visual Line of Sight (VLOS),Extended Visual Line of Sight (EVLOS),Beyond Line of Sight (BLOS)), By Point of Sale, (OEM, Aftermarket), By MTOW, (<25 Kilograms,25-150 Kilograms,>150 Kilograms)

By Application:
UAV Market, By Application, (Military, Civil & Commercial, Homeland Security, Consumer)

The content of the study subjects, includes a total of 15 chapters:
Chapter 1 Introduction and Overview
Chapter 2 Industry Cost Structure and Economic Impact
Chapter 3 Rising Trends and New Technologies with Major key players
Chapter 4 Global Unmanned Aerial Vehicles Market Analysis, Trends, Growth Factor
Chapter 5 Unmanned Aerial Vehicles Market Application and Business with Potential Analysis
Chapter 6 Global Unmanned Aerial Vehicles Market Segment, Type, Application
Chapter 7 Global Unmanned Aerial Vehicles Market Analysis (by Application, Type, End User)
Chapter 8 Major Key Vendors Analysis of Unmanned Aerial Vehicles Market
Chapter 9 Development Trend of Analysis
Chapter 10 Conclusion

Reasons to Buy This Report:
1. A complete Unmanned Aerial Vehicles view is offered by elaborating market size, growth, eminent industry players
2. The competitive landscape view, Unmanned Aerial Vehicles industry dominance across different regions and countries is offered
3. Unmanned Aerial Vehicles development opportunities, challenges, investment feasibility, estimated growth, and demand-supply statistics are covered
4. Unmanned Aerial Vehicles industry bifurcation based on product type, applications, regions will offer complete insights
5. Extensive primary along with paid interviews and secondary research techniques are applied to derive the market numbers
6. The report can be customized for various regions, key players, type, applications based on users' requirement

Get Off on purchasing this report, Ask Here for Discount @ https://www.adroitmarketresearch.com/contacts/enquiry-before-buying/450?utm_source=AD

Watch China's New Drone Swarm Capabilities

Source [**video**]: https://i-hls.com/archives/104901

Oct 28 – China has been working for several years on using small UAVs in a swarm. Now it seems that the Chinese military (PLA) will deploy swarms of unmanned aerial vehicles (UAVs) in the near future.

A video footage released by the China Electronics Technology Group Corporation (CETC) shows a modified Dongfeng Mengshi 6×6 CTL181A armored vehicle fitted with a 48-tube multiple UAV launcher being used in trials at an undisclosed location.
The video also shows several UAVs being deployed from civil helicopters, indicating that development work on multiple launch platforms is in progress, according to janes.com. Subsequent footage showed the UAVs

forming a small swarm along with a simulated attack on a mock target. It also showed how imagery from the UAVs was being relayed to the operator.
The launcher seen on the vehicle could be adapted for installation in warships and, if installed on amphibious landing vessels, it could be used to support amphibious operations, according to janes.com.

Major Step on Way to Drone Flights Over Europe's Cities

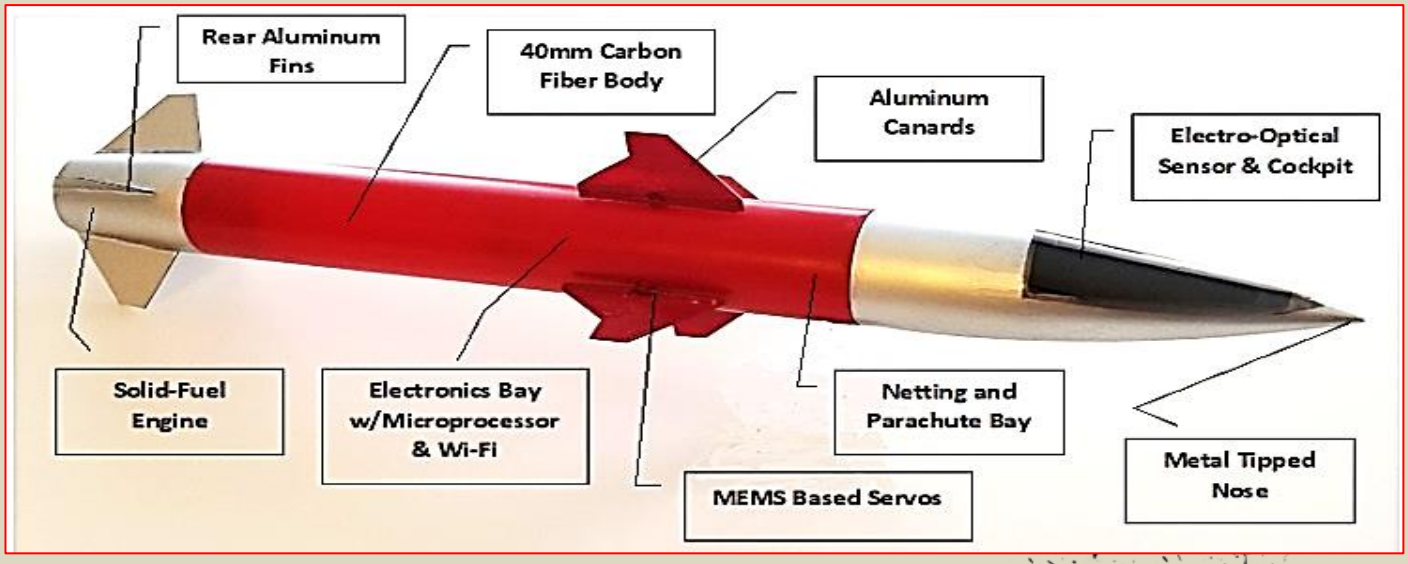
Source: https://i-hls.com/archives/104930

Oct 28 – Drones are quite a new entrant to busy urban environments, therefore it is important that the aviation authorities know who is using them and for what purpose, to ensure public safety.
Registered users will now be able to fly their drones anywhere in the European Union with a single registration. The European Union Aviation Safety Agency (EASA) has delivered a digitalized and secure system for the exchange of drones' registration data among the national authorities of the Member States.
Drone users will be legally obliged to register as from December 31, 2020 with their national aviation authorities.
EASA Executive Director Patrick Ky said: "We want to make this process as straightforward as possible for the users. The repository allows information registered with one authority to be shared with others, creating the basis for seamless drone usage across the European Union without the need to register in separate Member States. "
The solution launched by EASA on October 15, 2020 is a broker system based on open web technologies and secured standards which facilitates the transfer of drones' information between the Member States through the Agency, acting as a hub.
In parallel, it will act as a test case for a larger project to create a fully centralised database of information at EASA, providing the basis for more effective cooperation between EASA and its Member States on certification, oversight and enforcement.
This database will act as a repository for certificates, approvals, licences, declarations and transfers of responsibilities, in addition to the drones' registration data, according to easa.europe.eu.

New Counter Drone Swarm System Unveiled

Source: https://i-hls.com/archives/104946

Oct 30 – Small armed unmanned aerial vehicles are becoming increasingly threatening to countries around the world, especially when they are loaded with explosives. New smart anti-drone munitions offer a safe and cost-effective means to neutralize these threats and even cope with drone swarms.
The non-lethal munitions are surface-to-air and air-to-air self-guided missiles are a new class of smart "fire and forget" projectiles that will give the Military, Homeland Security, and Law Enforcement the ability to deal with threatening unmanned aerial vehicles.
SmartRounds has been issued a US patent "Non-Lethal Smart Weapons with Computer Vision" for these munitions.
SAVAGE "Smart Anti-Vehicle Aerial Guided Engagement" missiles are 40mm counter-UAV munitions that can be fired from the



company's custom multi-tube ground launcher or another UAV at high velocity and equipped with computer vision object detection and target tracking.

The long-range guided missile impacts the enemy drone with enough kinetic energy to disable or destroy it.
The missile is equipped with a parachute to safely return to the ground for reuse. SRI's proprietary computer vision algorithms along with an electro-optical sensor allows the missile to follow the target after it leaves the launcher by adjusting the missile's aerodynamics and changing its direction. This ensures that the projectile will reach its target even if the UAV is moving at high speed.
AI algorithms give multiple SAVAGE missiles the ability to communicate with each other in flight to maximize their effectiveness in dealing with a drone swarm, according to newswire.com.

Armenian National Committee of America
NATIONAL HEADQUARTERS

Evidence of U.S. Parts in Turkish Drones Deployed by Azerbaijan

Battlefield evidence confirms that Turkey's Bayraktar Drones - deployed by Azerbaijan against Armenian civilians in Artsakh - contain parts and technology from U.S. firms, U.S.-based affiliates of foreign firms, and firms located in NATO ally countries (Canada, UK, France, Germany, Austrian, and Netherlands).

How will the UAE Use the New MQ-9B UAVs?

Source: https://i-hls.com/archives/105212

Nov 14 – The controversial sale of US weapons to the UAE within the framework of the peace agreement with Israel included some unmanned air verhicles. Up to 18 General Atomics Aeronautical Systems MQ-9B UAVs) were included in the $23.4 billion sale of

aircraft and weapons to the United Arab Emirates (UAE) approved by the US Department of State. The sale includes also 50 Lockheed Martin F-35A Lightning II stealth fighters, and air-to-air and air-to-surface munitions, as US secretary of state Mike Pompeo declared.
Typically, these armed intelligence, surveillance and reconnaissance UAVs are restricted to the USA's closest allies due to a Missile Technology Control Regime policy of a "strong presumption of denial". The arms-control agreement classifies the UAV in the same category as cruise missiles capable of delivering a weapon of mass destruction.

However, the Trump administration updated the US policy in July, allowing for case-by-case approvals to sell UAVs with maximum flight speeds less than 432kt (800km/h). Using that new policy, the USA approved Taiwan's pending acquisition of four MQ-9Bs on 3 November, according to flightglobal.com.
Included with the MQ-9B proposal are related weapons such as 515 Lockheed AGM-114 Hellfire missiles, Leonardo Seaspray 7500 maritime radars and Sage 750 electronic support measures systems.
Presumably intended to spot and track small Iranian diesel-electric submarines, the MQ-9Bs would come with anti-submarine warfare mission kits, receivers and acoustic processors, as well as SSQ-36B thermometric sonobuoys, SSQ-53G passive sonobuoys and SSQ-62F active sonobuoys.

Autonomous Robotics and Quantum Technology Initiative in Abu Dhabi

Source: https://i-hls.com/archives/105342

Nov 21 – Autonomous robotics is only one of the areas of interest at the center of an innovation initiative in the UAE. Within efforts to establish its status as a global hub for innovation and advanced technologies, Abu Dhabi has unveiled its new technology Innovation Institute (TII), a dedicated applied research pillar of the Advanced Technology Research Council (ATRC).
The seven areas of focus include quantum research; autonomous robotics; cryptography; advanced materials; digital security; directed energy; and secure systems. The institute aims to deliver discovery science and breakthrough technologies that have a global impact through the seven dedicated research centers.
The move is intended to position Abu Dhabi and the UAE as a global hub for advanced technology research.
Teams of international scientists and researchers joined the institute from around the world within two months of the first board meeting in August 2020. TII will also drive applied research, intellectual property development, and academic and industry partnerships.
Importantly, the institute will have the flexibility to rapidly progress research, with a defined research roadmap, committed long-term funding and the ability to make effective decisions in a fast-paced environment, according to itp.net.

First Time – Millions of Lab Tests Will be Transported by Drones

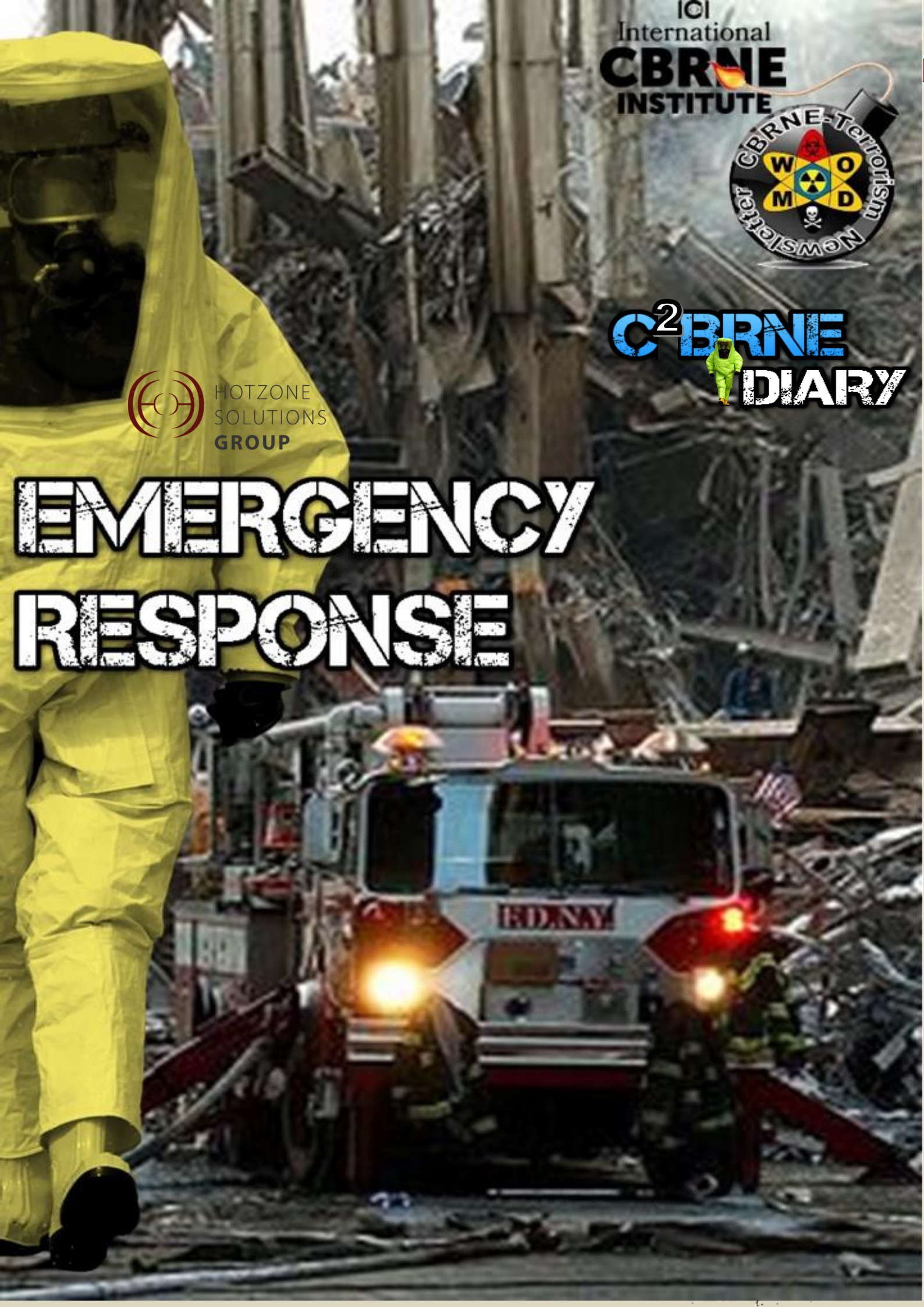
Source [+video]: https://i-hls.com/archives/105347

Nov 21 – The first urban beyond-visual-line-of-sight (BVLOS) medical drone delivery network has been launched in the largest city of the European Union with the potential to serve millions of patients each year.
Matternet, the developer of an urban drone logistics platform, has launched operations at Labor Berlin hospital laboratory in Germany.

Permanent operations expected to take flight next year. The drone network expects to significantly improve the timeliness and efficiency of Labor Berlin's diagnostics services by providing an option to avoid roadway delays, which will improve patient experience with potentially life-saving benefits and lower costs.

Labor Berlin is Europe's largest hospital laboratory, responsible for diagnostics for 80 percent of patient beds in Berlin. Currently, over 15,000 samples are transported daily across Labor Berlin's extensive network.

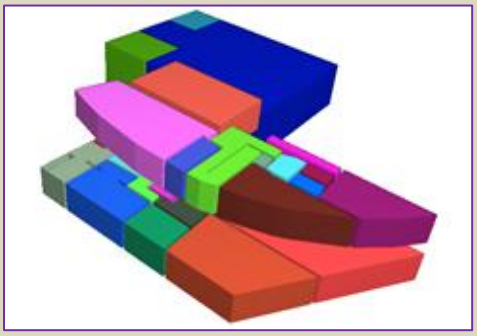
During the initial phase of the program, Matternet will work with Labor Berlin to determine optimal ways to integrate drone delivery into the laboratory group's existing workflow. The partners intend to invite government and public sector representatives to observe drone flights, and engage other airspace users such as Helicopter Emergency Rescue Services, Berlin police and Berlin's airports. Matternet will also work closely with the Air Navigation Service Provider in Germany and UTM providers to integrate the drones safely into Berlin's airspace.
The drone system has been operating around the world since 2017 through partnerships with Swiss Post, UPS and most recently Japan Airlines, according to uasweekly.com.


ICI
International
CBRNE
INSTITUTE
CBRNE-Terrorism Newsletter
W
O
M
D
C2BRNE
DIARY
HOTZONE
SOLUTIONS
GROUP
EMERGENCY
RESPONSE
FDNY

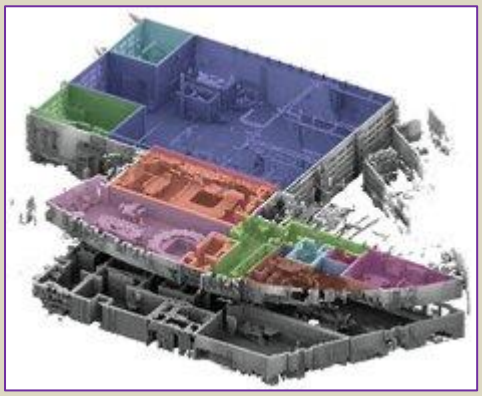
Creating 3-D Maps of Complex Buildings for Disaster Management

Source: http://www.homelandsecuritynewswire.com/dr20201023-creating-3d-maps-of-complex-buildings-for-disaster-management

Oct 23 – In case of an emergency, first responders like the fire brigade need up-to-date information. 2D maps are a common source of information but they can be difficult to read in an emergency situation. University of Twente'sPhD-student Shayan Nikoohemat created an algorithm that can accurately generate 3D models of the insides of large buildings from point clouds.



Indoor 3D models are the digital twins of building interiors. The 3D models could be used by first responders to get a good impression of large buildings, like shopping malls, a hospital or a sports complex, on their way to the emergency. 2D maps represent important information – like the location of emergency exits – on tangled floor plans, making them difficult too read quickly and after each reconstruction, these maps are outdated. "Sometimes, these maps are so outdated that the real building looks completely different than the floor plans. We need a fast and reliable approach to create the digital 3D model of interiors.", says Shayan.



From Point Cloud to 3D Map

Luckily, laser scanners can quickly scan a whole building after every reconstruction. However, these scanners create point clouds, unstructured data which still has to be converted into a 3D model. The data doesn't know if a scanned point is a wall, an exit or, for example, a table. According to Shayan, his program solved this: "For my PhD thesis, I created algorithms that automatically understand the data and can create 2D and 3D maps. We can detect and model doors, stairs, obstacles and navigable areas which are crucial data for the emergency planning."

Recognizing Elements

The algorithm can recognize different structural elements such as walls, slabs, ceilings, and openings. Individual items like furniture, however, still pose a problem. "It is not yet able to correctly label everything, but the structural elements are enough to create an accurate map, which we tested on several real datasets," he says. During his postdoc, he will further develop the system to also work for individual items. Huib Fransen of the Safety Region Rotterdam-Rijnmond was delighted with the results: "Shayan's project is exciting for us and we were happy to provide him with the scanning sites for test cases."

Mobile Flood Tool

Source: http://www.homelandsecuritynewswire.com/dr20201103-mobile-flood-tool

Nov 03 – The U.S. Geological Survey announced Friday the completion of a new mobile tool that provides real-time information on water levels, weather and flood forecasts all in one place on a computer, smartphone or other mobile device.

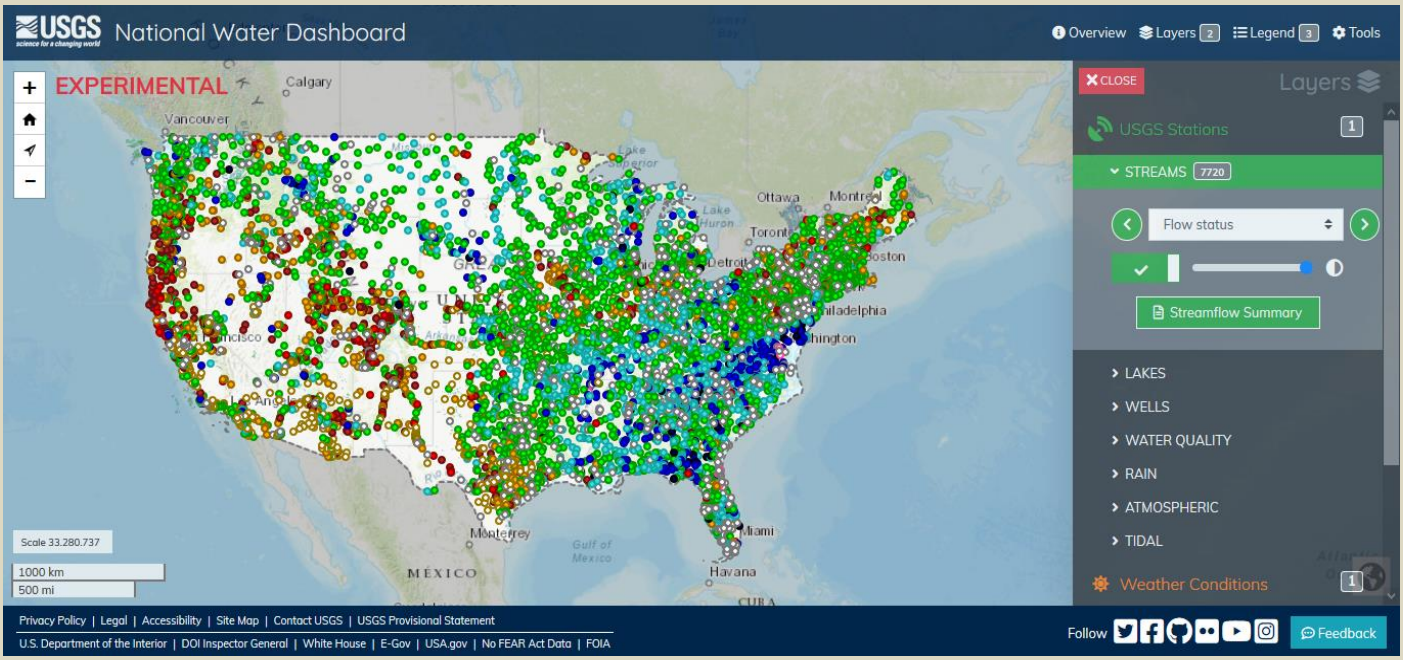
The new USGS National Water Dashboard, or NWD, provides critical information to decision-makers, emergency managers and the public during flood events, informing decisions that can help protect lives and property.

"The National Water Dashboard is a much-needed advancement that will help keep communities across the country safe during extreme weather conditions," said Tim Petty, Ph.D., Department of the Interior Assistant Secretary for Water and Science, from an agricultural round table with the Water Subcabinet in Janesville, Wisconsin. "The development of a comprehensive tool that can provide real-time, critical information on mobile devices is great news for areas in our country that are prone to flooding or drought. In addition to giving the public key information on what's happening in their communities, it will also help improve the response of federal, state and local agencies during storms, floods and drought conditions."

"Our vision is the National Water Dashboard will be a one-stop resource for all available USGS water data used by the public to make decisions that can preserve life and property," said Jim Reilly, Ph.D., director of the USGS. "The USGS will continue to build out this tool incorporating future advances in water information so the public will have the latest and best information on hazards and resources."

Information from the NWD will help inform forecasting, response and recovery efforts for agencies such as the National Weather Service, the Federal Emergency Management Agency, the U.S. Army Corps of Engineers, and other federal, state and local agencies. The

tool can be used by forecasters and local emergency managers as they issue flood- and evacuation warnings, verify safe evacuation routes and coordinate emergency response efforts. The NWD can assist the USACE as they manage water supplies in river basins and operate flood-control reservoirs. During a drought, the tool can help state resource managers identify areas where water supplies are at risk.



"The National Water Dashboard is an exceptional tool for staying up to date on real-time USGS water information coupled with forecasts and warnings from NOAA's National Weather Service," said retired Navy Rear Adm. Tim Gallaudet, Ph.D., assistant secretary of commerce for oceans and atmosphere and deputy NOAA administrator. "Giving individuals access to water information whether it be a flood or drought, on their mobile device, will help protect lives and property."

The NWD presents real-time stream, lake and reservoir, precipitation and groundwater data from more than 13,500 USGS observation stations across the country. This information is shown along with NOAA weather data such as radar, watches and warnings, past precipitation totals, precipitation forecasts and drought conditions from other open water-data sources. The NWD also links to the USGS WaterAlert system, which sends out instant, customized updates about water conditions.

"The National Water Dashboard builds on the USGS Texas Water Dashboard that was created in 2016," said Don Cline, Ph.D, USGS Associate Director for Water Resources. "Expanding this tool nationwide will increase the ease and ability for the public to have access to USGS real-time water data at all times to help make informed decisions regarding the safety of their families and homes."

"The U.S. Army Corps of Engineers values the continued partnership and active engagement within our Federal family," said Chandra S Pathak, Policy Advisor and Senior Engineer for the U.S. Army Corps of Engineers Engineering and Construction Division. "The new USGS National Water Dashboard is well suited to support the ever-evolving needs for increased hazard risk awareness and mitigation actions toward preparedness and response."

In addition to its value in protecting life and property and in managing water use, the NWD can provide adjunct benefits to the American public, such as recreational planning. The Colorado River is a popular recreation destination for white-water rafting. The NWD is a useful application to explore local streamflow conditions before heading out on your next float trip. Just click directly on a specific site to get the latest information. In this example, the streamflow at 09402500 Colorado River near Grand Canyon, Arizona, is shown to be 11,900 cubic feet per second. You can see its flow rate is considered above normal for this day of the year by the light-blue color of the station. From this view, users can also see streamflow values of other local waterways at a glance.

Sources

The NWD uses real-time data from the USGS National Water Information System. NWIS is the world's largest authoritative enterprise water information system, which is foundational to advancing USGS science priorities and meeting the needs of stakeholders. Data in NWIS have been collected from more than 1.9 million sites through time, with some real-time stations in operation for more than 100 years.

▶▶ **Visit the** USGS NWIS website to learn more.

Impact of the COVID-19 pandemic and crisis on the operations of critical infrastructure and essential services operators in South East Europe

Source: https://www.torchmarketing.co.uk/wp-content/uploads/2020/09/WSRAutumn2020.pdf

By mid-2020, COVID-19 pandemic (referring the period of writing this analysis) has caused a large number of deaths, significant economic damage and the collapse of many companies around the world, and surprisingly highlighted the considerable unreadiness of international organizations and the vast majority of countries to achieve timely and coordinated responses to the challenges they faced. That has additionally complicated the situation, intensified the effects of the crisis and created numerous cascading effects in all sectors.

The Strategic Stockpile failed; experts propose new approach to emergency preparedness

North Carolina State University
Source: https://www.sciencedaily.com/releases/2020/11/201112120500.htm

Nov 12 – A new analysis of the United States government's response to COVID-19 highlights myriad problems with an approach that relied, in large part, on international supply chains and the Strategic National Stockpile (SNS). A panel of academic and military experts is instead calling for a more dynamic, flexible approach to emergency preparedness at the national level.

"When COVID-19 hit, the U.S. was unable to provide adequate testing supplies and equipment, unable to provide adequate personal protective equipment (PPE), and didn't have a functioning plan," says Rob Handfield, first author of the study and Bank of America University Distinguished Professor of Operations and Supply Chain Management at North Carolina State University.

"The SNS hadn't replenished some of its supplies since the H1N1 pandemic in 2009-10. Many of its supplies were expired. And there was no clear leadership. Federal authorities punted problems to the states, leaving states to fight each other for limited resources. And the result was chaos. We need to be talking about this now, because the nation needs to be better prepared next time. And there is always a next time."

To that end, Handfield and collaborators from NC State, Arizona State University, the Naval Postgraduate School and the Air Force's Contracting Career Field Management Team came together to outline the components that are necessary to ensure that there is an adequate federal response to future health crises. They determined that an effective federal program needs to address five criteria:

1). More Flexibility: In order to respond to unanticipated threats, any government system needs to have sufficient market intelligence to insure that it has lots of options, relationships and suppliers across the private sector for securing basic needs.

"You can't stockpile supplies for every possible contingency," Handfield says.

2). Inventory Visibility: The government would need to know what supplies it has, where those supplies are, and when those supplies expire. Ideally, it would also know which supplies are available in what amounts in the private sector, as well as how quickly it could purchase those supplies.

"The same is true on the demand side," Handfield says. "What do people need? Where? When?"

3). Responsiveness: The governmental institution overseeing emergency preparation needs to have leadership that can review information as it becomes available and work with experts to secure and distribute supplies efficiently. This would be an ongoing process, rather than a system that is put in place only in the event of crises.

4). Global Independence: The COVID-19 pandemic has highlighted the fact that the U.S. has outsourced manufacturing of critical biomedical materiel, because it was cheaper. Authorities need to consider investing in domestic manufacturing of PPE, testing supplies and equipment, pharmaceutical chemicals, syringes, and other biomedical supplies.

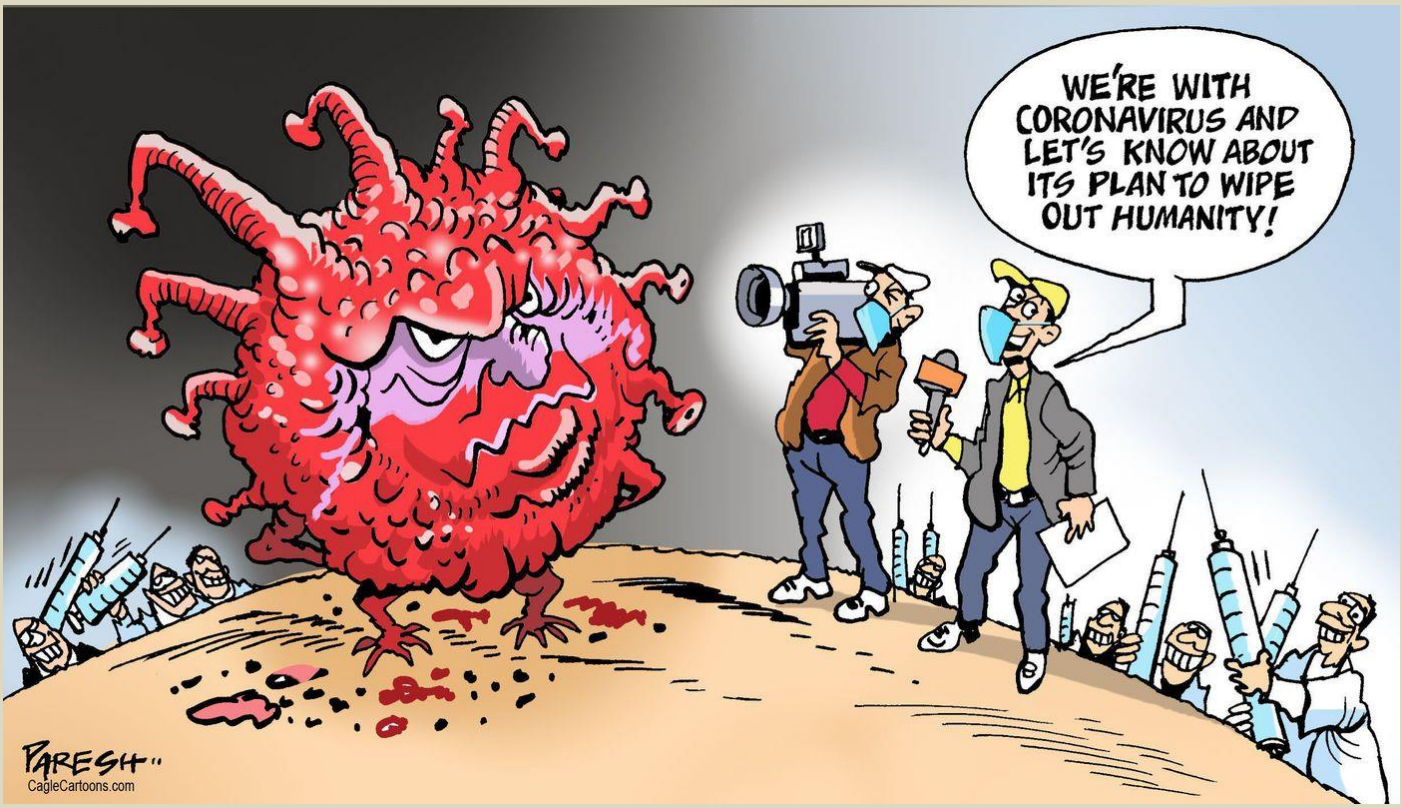
"The past year has really driven home the consequences of being dependent on other nations to meet basic needs during a pandemic," Handfield says. "Relying largely on the least expensive suppliers for a given product has consequences."

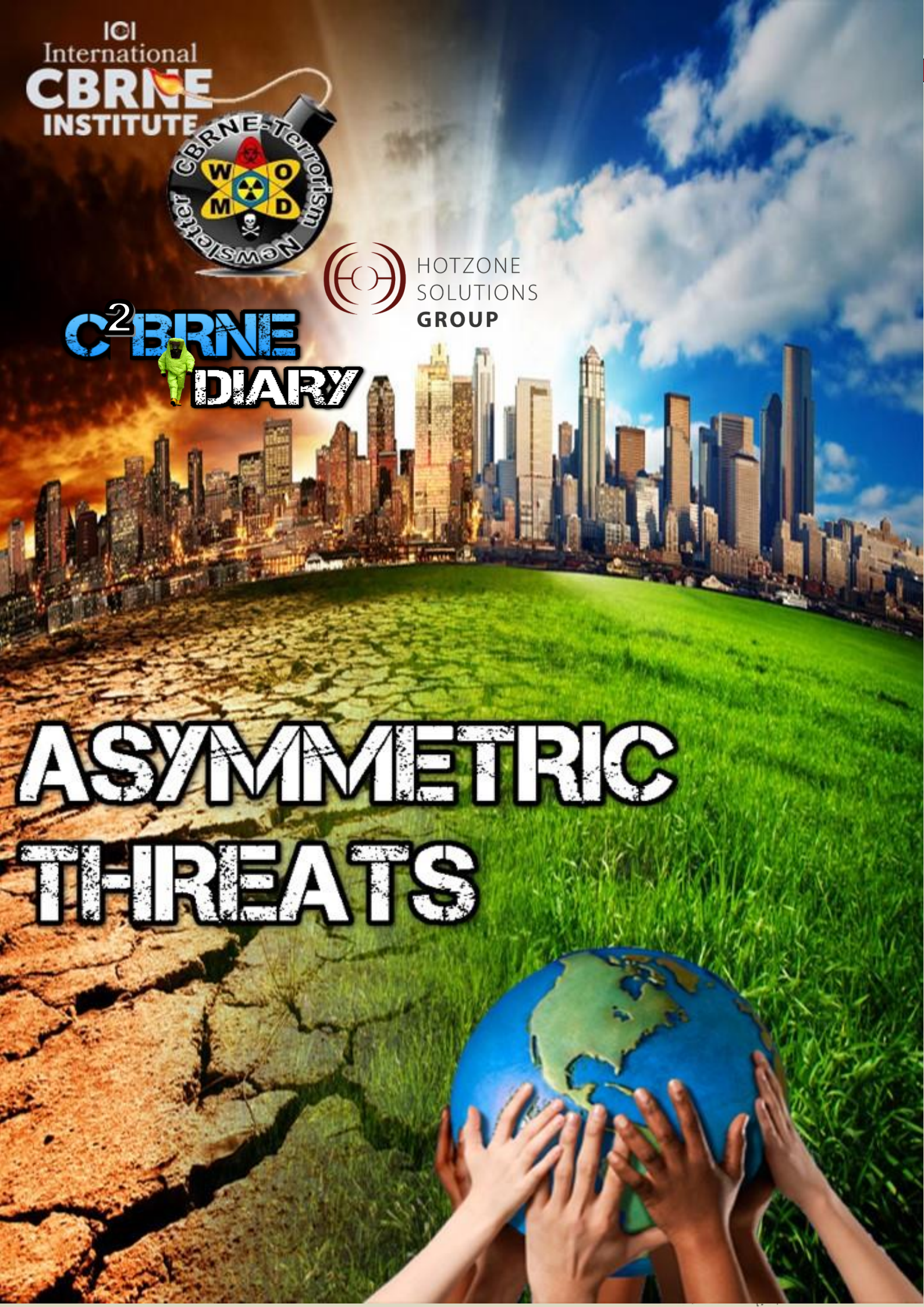
5). Equitable: The government needs to ensure that supplies get to where they are most needed in order to reduce the infighting and hoarding that we've seen in the COVID-19 pandemic.

"A first step here is to settle on a way of determining how to prioritize needs and how we would define an equitable allocation and distribution of supplies," Handfield says.

The last ingredient is bureaucratic: Coordinating all five of these components should be done by a permanent team that is focused solely on national preparation and ensuring that the relevant federal agencies are all on the same page.
"This is a fundamental shift away from the static approach of the SNS," Handfield says. "We need to begin exploring each of these components in more detail -- and defining what a governing structure would look like. We don't know how long we'll have until we face another crisis."

The paper, "A Commons for a Supply Chain in the Post-COVID-19 Era: The Case for a Reformed Strategic National Stockpile," is published open access in *The Milbank Quarterly*. The paper was co-authored by Blanton Godfrey, the Joseph D. Moore Distinguished Professor in NC State's Wilson College of Textiles; Major Daniel Finkenstadt of the Naval Postgraduate School; Eugene Schneller of Arizona State; and Peter Guinto of the Air Force's Contracting Career Field Management Team.




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

Most Surprising Thing about a New Report Showing Climate Change Imperils the U.S. Financial System Is That the Report Even Exists

By Jeffrey Dukes

Source: http://www.homelandsecuritynewswire.com/dr20201102-most-surprising-thing-about-a-new-report-showing-climate-change-imperils-the-u-s-financial-system-is-that-the-report-

Nov 02 – Burnt orange daytime skies signal that the consequences of climate change are already here. But while we tend to focus on the death and destruction resulting from the growing frequency and severity of wildfires and other disasters, we often pay less heed to the ways their costs ricochet through the financial system, with the potential for widespread collateral damage.

The wildfires raging in the West illustrate the problem. Their unprecedented damage has spooked insurance companies, which have raised rates, dropped coverage for high-risk properties and even walked away from markets entirely, depressing property values. This has forced states like California to step in and offer more coverage for affected residents. Beyond putting taxpayers on the hook, it could also lead to municipal bankruptcies, large bondholder losses and financial crises.

People in the West aren't the only ones facing these problems. Droughts and floods are becoming more common in many regions, including my own state of Indiana, threatening crops, property and infrastructure while driving up insurance premiums.

As an expert on the impacts of climate change, I contributed to a recent report that examined what climate change means for the U.S. financial system. Our report includes many important findings and recommendations, perhaps most notably that the U.S. financial system is imperiled by climate change.

The report's greatest significance, though, may be that it exists at all.

Unanimous Agreement from a Diverse Group

The subcommittee I served on was formed last November by the Commodity Futures Trading Commission, the government agency that regulates complex financial instruments known as derivatives. This alone was a bit surprising given that the Trump administration, which appointed the commissioners, has been consistently hostile to efforts to fight or even assess the risks of climate change.

Our group included representatives from oil companies, agribusiness, banks, investment firms and environmental organizations, as well as a handful of academics like me. We were told to broadly assess the implications of climate change for the financial system and provide recommendations to the government. And we did, writing a 166-page report with dozens of recommendations, some of them potentially controversial, such as adding the costs of climate damage to the price of fossil fuels.

Remarkably, this diverse group unanimously voted to adopt the report and forward it to the Commodity Futures Trading Commission, which released it on Sept. 9.

Our key finding – and the one that underlies every recommendation – is this: Climate change, partly by increasing the risks and severity of wildfires, hurricanes and other disasters, poses a threat that permeates the U.S. financial system. And so, the government needs to make climate-related risk more visible and prepare the financial system for disruptions.

Managing Climate Risks

Two types of risks are associated with climate change: physical and transition.

Physical risk has dominated the news lately in coverage of wildfires and storms. It's simply the threat climate change poses to life, property and public health.

Just as smoke from the fires in the West has blown across much of the United States, the impacts of those fires, and other disasters, can drift through the U.S. financial system with cascading consequences.

Transition risk, on the other hand, is more about the costs associated with our responses to climate change, such as sudden shifts in policy or in people's preferences and behaviors.

If governments took sudden, dramatic action to reduce the use of fossil fuels, through a high price on carbon or a stronger mandate, the values of the companies that find, extract, process and deliver those fuels could plummet. The companies susceptible to rapid devaluations as a consequence of government actions – or shifts in societal preferences – thus have high transition risk, which should accordingly reduce their value today.

Helping the System See the Risks

However, for investors to take physical and transition risks into account, these risks have to be quantified and disclosed.

A first step, and the report's most important recommendation, is that legislators should put a price on carbon emissions. The government currently subsidizes the cost of fossil fuels

through tax breaks and other mechanisms. Incorporating the full cost of climate disruption into the price of these fuels would help redirect huge sums of money into climate-friendly technologies and industries.
But alone it's not enough, since the climate is already being disrupted, and more needs to be done to help the financial system see and react to a variety of changing risks.
The government can help banks and other financial companies do this by specifying how they should measure and report their financial risks from climate change. The government can also require publicly traded companies across all sectors to identify and report climate risk using transparent measurement techniques, so that investors trust the numbers, which need to be comparable across institutions and, ideally, sectors, so people can use them in decision-making.
The economic risks of climate change in the U.S. financial system are currently too hard for investors and regulators to see.
Illuminating them will help markets work to everyone's benefit. First, this will lower the risk of a sudden market crash. Second, clear, comparable risk information will discourage investment in climate-disrupting activities and motivate economic actors to incentivize further solutions.

Jeffrey Dukes *is Director of the Purdue Climate Change Research Center, Purdue University.*

Shuttering Asymmetric Warfare Group and Red Team is the 'wrong direction,' retired Army three-star says

By Kyle Rempfer
Source: https://www.armytimes.com/news/your-army/2020/11/04/shuttering-asymmetric-warfare-group-and-red-team-is-the-wrong-direction-retired-army-three-star-says/

Army Maj. Tommy Broome, with the Asymmetric Warfare Group, provides security from an observation post overlooking the Kholbesat bazaar, in Khowst province, Afghanistan, in March 2011. (Lt. Col. Sonise Lumbaca/Army)

The Army's decision to close some key innovation programs closely associated with the Afghanistan and Iraq wars is ill-advised, according to retired Lt. Gen. David W. Barno, who led coalition forces in Afghanistan from 2003 to 2005.
Units like the Fort Meade-based Asymmetric Warfare Group, composed of seasoned soldiers and tasked with expediting new tactics and equipment to battlefields, "need to be empowered" and "given more authority, because they have been proven to be successful," Barno said Monday at the Association of the U.S. Army.
Larger bureaucratic structures in the Army will find it difficult, if not impossible, to deliver those creative solutions, according to Barno, who visited the Asymmetric Warfare Group while researching his book, "Adaptation under Fire: How Militaries Change in Wartime."
"[The Army's] deactivating the Asymmetric Warfare Group … The Rapid Equipping Force is now going away," Barno said. "The Red Team at Fort Leavenworth has now been notified they're going to be shut down. These are moves in the wrong direction. You've got to have those pioneers out there breaking the ice. … Stripping them out of the system is not going to make the system more nimble. It's going to have, I'm afraid, the opposite effect."
The Rapid Equipping Force, headquartered at Fort Belvoir, found ways to use commercial products to address urgent requirements around the globe. And the Red Team, also known as the University of Foreign Military and Cultural Studies, was tasked with teaching ways for Army leaders to avoid "group-think" and to view dilemmas through multiple perspectives, sometimes finding problems they didn't know existed.
The closures are casualties of the Army's shift away from counter-insurgency and towards large-scale warfare against near-peer enemies.
"Those organizations exist[ed] because the regular structures didn't do what they needed to do under extraordinarily difficult circumstances," said Nora Bensahel, a defense policy scholar who co-authored "Adaptation under Fire."
"We're both very disappointed, although perhaps not surprised, that when those circumstances change and budgets get tighter, that they're going to be on the chopping block, because they exist to circumvent the regular system," she added.
Right now, the Defense Department is prioritizing buying weapons systems and developing doctrine designed around a potential conflict with an adversary like Russia or China.
Even though the Pentagon has a poor record of predicting what future wars will look like, Barno and Bensahel argued Monday that what's more important is changing once that future war starts and quickly shedding strategies and technologies that are failing.
"We believe that there's now, what we characterized in our book, an adaptability gap, and that gap is growing," Barno said.
Several key factors make that gap much larger today: strategic uncertainty around the globe, with the United States now facing a multi-polar world order; new domains of warfare, to include cyberspace and outer space; and a period of rapid change across society.

"It took 38 years, for example, for radio to reach 50 million people around the world. Facebook did that in one year," Barno said. "That also is affecting military technological change. We're seeing huge leaps ahead in weaponry and capabilities and the role of the internet … in ways that we've not experienced in warfare before."

Sgt. Maj. Raymond Hendrick, left, an Asymmetric Warfare Group adviser, explains blast-radius details of the man-portable line charge system during a training exercise just outside of Forward Operating Base Zangabad, Afghanistan, in October 2013. (Cpl. Alex Flynn/Army)

Adaptability problems could compound during this period of exponential change. And there are numerous causes of concern when it comes to the U.S. military's ability to adapt, according to Bensahel.
Leadership can be risk-averse, and there is often excessive amounts of doctrine that is difficult to revise, she said. There's also "structural tension" between the combatant commands, which prioritize the needs of today's troops, and the armed services, which are training and equipping for a future war, Bensahel added.
The book does present solutions to those problems, including the risk aversion among senior leaders, which Bensahel said should be countered by adding more intensive writing assignments and role playing at the war colleges "to give people practice in adapting quickly to unforeseen situations."

Battalion task forces and brigade combat teams tend to be well-honed through combat training center rotations, but major unit exercises don't test leaders in the same way, according to Barno.
Running an exercise to the "point of failure, so it shuts down the system and gives [senior leaders], for instance, challenges in an adversary that they did not expect … we don't do that nearly as well as we do down at the tactical level," said Barno.
Though the officers at the tactical level are, realistically, the same ones who end up in senior roles later in their careers, their priorities change once they enter staff positions in a bureaucracy, according to Bensahel.
"Folks at the most senior levels of the service were highly invested in their programs of record, did not want to admit that there were problems with them and did everything they could to prevent alternatives from being explored," Bensahel said.
"Very often, what adaptability at the highest levels requires is taking your playbook and everything that you've learned in your experience and either throwing it out or at least questioning the basic assumptions that may have been there throughout your entire career, unchallenged," Bensahel added.

Kyle Rempfer *is a staff reporter for Military Times, focusing on the U.S. Army. He served an enlistment as an Air Force Special Tactics CCT and JTAC.*