10\20

HZS

C²BRNE DIARY

Dedicated to Global First Responders

October 2020

hope

A HOTZONE SOLUTIONS GROUP PUBLICATION


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

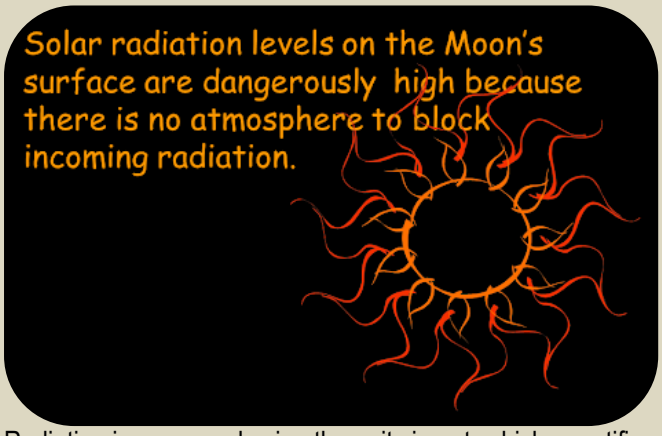
We Finally Know How Much Radiation There Is on The Moon, And It's Not Great News

Source: https://www.sciencealert.com/scientists-predict-how-long-humans-can-survive-radiation-on-the-moon

Sep 26 – As the US prepares to return humans to the Moon this decade, one of the biggest dangers future astronauts will face is space radiation that can cause lasting health effects, from cataracts to cancer and neurodegenerative diseases.

Though the Apollo missions of the 1960s and 1970s proved it was safe for people to spend a few days on the lunar surface, NASA did not take daily radiation measurements that would help scientists quantify just how long crews could stay.

This question was resolved Friday after a Chinese-German team published in the journal *Science Advances* the results of an experiment carried out by China's Chang'E 4 lander in 2019.



"The radiation of the Moon is between two and three times higher than what you have on the ISS (International Space Station)," co-author Robert Wimmer-Schweingruber, an astrophysicist at the University of Kiel told AFP.

"So that limits your stay to approximately two months on the surface of the Moon," he added, once the radiation exposure from the roughly week-long journey there, and week back, is taken into account.

There are several sources of radiation exposure: galactic cosmic rays, sporadic solar particle events (for example from solar flares), and neutrons and gamma rays from interactions between space radiation and the lunar soil.

Radiation is measured using the unit sievert, which quantifies the amount absorbed by human tissues.

The team found that the radiation exposure on the Moon is 1,369 microsieverts per day - about 2.6 times higher than the International Space Station crew's daily dose.

The reason for this is that the ISS is still partly shielded by the Earth's protective magnetic bubble, called the magnetosphere, which deflects most radiation from space.

Earth's atmosphere provides additional protection for humans on the surface, but we are more exposed the higher up we go.

"The radiation levels we measured on the Moon are about 200 times higher than on the surface of the Earth and five to 10 times higher than on a flight from New York to Frankfurt," added Wimmer-Schweingruber.

NASA is planning to bring humans to the Moon by 2024 under the Artemis mission and has said it has plans for a long term presence that would include astronauts working and living on the surface.

For Wimmer-Schweingruber there is one work-around if we want humans to spend more than two or three months: build habitats that are shielded from radiation by coating them with 80 centimeters (30 inches) of lunar soil.

North Korean envoy: COVID-19 under control, weapons are 'self-defense'

Source: https://gephardtdaily.com/national-international/north-korean-envoy-covid-19-under-control-weapons-are-self-defense/

North Korean Ambassador to the United Nations Kim Song speaks before the 75th U.N. General Assembly on Tuesday. Photo screenshot of United Nations Web TV

Sep 30 — North Korea's top envoy to the United Nations said Tuesday that leader Kim Jong Un fended off the COVID-19 pandemic in his country, as controversy grows in the South over a North Korean decision to shoot and kill a South Korean citizen in North Korean territory.

Ambassador Kim Song said before the 75th U.N. General Assembly the "far-sighted leadership" of the North Korean leader enabled the regime to bring the virus under "safe and stable control."

The North Korean diplomat did not disclose any health data. He also declined to say there have been "zero" cases of the coronavirus, a frequently issued claim in the first half of the year.

Kim Song instead said Kim Jong Un's "extraordinary wisdom and strong determination" enabled the country of 25 million to take "pre-emptive measures" to "prevent the inflow and spread of the pandemic."

North Korea took a "series of state measures to block the virus inflow into the country," the ambassador said.

Editor's comment: click on photo

The North Korean people "adhered strictly" to anti-epidemic measures. The state also does not tolerate the slightest oversight, Kim Song said.

The North Korean envoy's claims about the pandemic in his country comes at a time when some politicians in South Korea are demanding more answers on the recent death of a South Korean officer in the North. The man may have been shot and possibly burned because of draconian measures against COVID-19 in the country, South Korean news services reported last week.

Political friction is growing within the South. The administration in Seoul has called for a cooperative joint investigation with the North. Seoul has also said there is evidence the 47-year-old South Korean victim had voluntarily defected by sea, the same day his brother, Lee Rae-jin, said his brother was a patriotic public servant and that the government was framing him.

On Tuesday, Kim Song told a sparsely attended General Assembly in New York his country is under a growing nuclear threat, reversing the claims of the international community that Pyongyang continues to build weapons of mass destruction.

"The nuclear threat [against North Korea] continues unabated along with hostile acts before our very eyes," Kim Song said.

"It is an undeniable reality of today that cutting-edge military hardware, including stealth fighters, continue to be introduced into the Korean Peninsula."

Kim Song also said the conclusion North Korea has drawn is that "peace never comes by itself, by the mere wish of one's side."

The ambassador also referred to Pyongyang's nuclear arsenal as an "effective deterrent for self-defense" realized through sacrifices, or the "tightening of our belts."

"Peace is now firmly defended," Kim Song said.

The North Korean ambassador also mentioned his country's preparations for a major anniversary of the ruling Workers' Party, and that Pyongyang's "socialist construction" moves ahead despite the challenges.

"Great projects are being completed one after another … with brilliant labor achievement," Kim Song said, adding the Pyongyang General Hospital, a "modern medical facility," is in its final stages before completion.

"Although we have suffered considerable losses we are vigorously striving to stabilize in a short period of time," the ambassador said, referring to recent floods that destroyed farms and upended entire villages.

Analysts have said North Korea is expected to showcase its latest intercontinental ballistic missile and submarine-launched ballistic missile at the military parade on Oct. 10.

Nuclear weapon transporter truck undergoes rocket crash test

Source: https://newatlas.com/military/nuclear-weapon-transport-truck-crash-test-snl/

Oct 11 – Sandia National Laboratories (SNL) has successfully conducted a full-scale crash test of the semi-tractor-trailer truck that will be used to transport nuclear weapons inside the United States. The Mobile Guardian Transporter was tested at SNL's rocket sled test track in New Mexico in June, where a second fully loaded semi-tractor trailer was propelled by rockets at highway speeds into the transporter for a broadside collision.

Because of the nature of the United States defense industry, the development, building, testing, storage, and deployment of nuclear weapons is spread widely throughout the lower 48 states. This is done for a variety of political, economic, practical, and security reasons, but it means that the US Department of energy and the Department of Defense need to rely on specially made transporters that protect weapons and weapon materials from hijacking and accidents.

Apparently the first of the transporters was the back seat of an ordinary Army sedan, which was used to carry the nuclear materials for the first atomic bomb in 1945. Since then, a family of increasingly sophisticated vehicles has been developed, including aircraft, armored trains, and since the 1990s, the Safeguards Transporter tractor-trailer system.

The rocket propelled truck was accelerated to highway speeds (Sandia National Laboratories)

To replace Safeguard, SNL is working for the National Nuclear Security Administration on the Mobile Guardian Transporter, which is expected to remain in service into the 2050s. For this project, engineers rejected developing an existing design in favor of a blank-sheet approach, which has culminated in the first crash test by the laboratory in two decades.

In previous tests 20 years ago, the transporter crashed into an immobile barrier. This time, the sensor-equipped prototype remained stationary while another truck was fired at it to produce a more realistic accident simulation and determine if the new transporter can keep the weapons cargo safe. The first prototype took 13 months to build with an additional six months to install the electronics before it was put to standard environmental tests that subjected it to extreme temperatures of hot and cold, as well as road driving and vibration tests.

For the crash test, the transporter's sensors handled over 400 channels of data and video, including high-speed video. Such extensive sensor coverage was necessary because only three prototypes will be built before production begins.

"The transportation mission is a critical component of an effective nuclear deterrent," says Jim Redmond, Sandia senior manager over the program. "It provides needed assurance to the American public and our allies of the safety and security of our stockpile. You've got to be able to ship nuclear assets safely and securely or you don't have a deterrence program."

Saudi Arabia's nuclear program: Separating real concerns from threat inflation

By Ali Ahmad

Source: https://thebulletin.org/2020/10/saudi-arabias-nuclear-program-separating-real-concerns-from-threat-inflation/

Oct 08 – In the highly charged political atmosphere surrounding nuclear initiatives in the Middle East, legitimate concerns are sometimes blown out of proportion, with potentially problematic results. This has been the case with recent coverage and commentary on Saudi Arabia's nuclear activities, which have been characterized by a degree of what can be described as "threat inflation."

While there are legitimate questions about what Saudi Arabia eventually intends to do with nuclear technology, the fact is that today the kingdom is not moving to establish either uranium enrichment or plutonium separation capability, without which there is no path to the Bomb. The kingdom's reported uranium mining activities are far from what is needed for a nuclear weapon.

The nonproliferation community should certainly be vigilant regarding what the kingdom is doing or planning to do on the nuclear front; given the geopolitical context in the Middle East, however, promoting exaggerated and alarmist claims is counterproductive and could actually be harmful to nonproliferation efforts.

In August, the *Wall Street Journal* reported that the kingdom had built, with help from China, a secret facility to extract yellowcake from uranium ore. Yellowcake is concentrated, natural uranium in powdered form. The report stated that, "The [yellowcake extracting] facility, which hasn't been publicly disclosed, is in a sparsely populated area in Saudi Arabia's northwest and has raised concern among US and allied officials that the kingdom's nascent nuclear program is moving ahead and that Riyadh is keeping open the option of developing nuclear weapons."

Several weeks later, the *Guardian* published a report outlining the kingdom's uranium ore reserves—rock that is still in the ground—noting that it likely has enough of these reserves to enable domestic production of nuclear fuel. The report stated, "If Saudi Arabia is able to mine sufficient uranium domestically, rather than relying on foreign providers, it could give the kingdom a boost toward creating its own weapons programme, experts say."

Reports like these give the impression that the kingdom is well down the path toward developing its own nuclear weapons. But this is misleading. Dozens of countries have identified recoverable uranium reserves on their own territories. And uranium mining, or even yellowcake extraction, is far from a usable weapon.

There are two paths to making a Bomb. The **first** would involve taking yellowcake, converting it from a solid to a gas form, and then enriching it to increase the concentration of uranium 235, the fissile isotope that can sustain a nuclear chain reaction. While natural uranium ore in the ground has a concentration of about 0.7 percent uranium 235, power reactor grade uranium requires enrichment levels between 3 and 5 percent, and weapons grade uranium needs to be enriched to about 90 percent. Today, Saudi Arabia has no enrichment capability.

The **second** path involves taking the spent fuel out of a reactor once it has burned up and putting it through chemical reprocessing to separate out fissile plutonium. This plutonium could then be weaponized. But here again Saudi Arabia does not have any operational, or even under construction, power reactors, nor does it have a reprocessing capability.

It is the kingdom's rivalry with Iran that seems to frame the wider perception of Saudi Arabia's nuclear news or announcements, particularly ever since Crown Prince Mohammed Bin Salman's alarming statement in March 2018 that the **kingdom will pursue nuclear weapons if Iran does.** However, there is a big difference between issuing such a serious political statement—about a future hypothetical scenario—and taking tangible steps toward weaponization.

Moreover, while it is rational to view Saudi Arabia's nuclear activities through the lens of its rivalry with Iran, the same dynamics can also explain why the kingdom has so far been unwilling to commit to forgo uranium enrichment and reprocessing activities, or to agree to the International Atomic Energy Agency's (IAEA) Additional Protocol, which would give the IAEA additional access to ensure the kingdom's program stays peaceful.

But unlike Iran's nuclear program, the Saudi nuclear program is so far more of a collection of incoherent intentions than tangible actions. Even producing nuclear fuel for power reactors domestically, which is within states' rights under the Nuclear Non-Proliferation Treaty, requires sustained financial and scientific investments in more complex parts of the nuclear fuel cycle. Apart from a low-power research reactor currently under construction, all available evidence suggests there has been very little progress on these investments.

Because its program is so embryonic, Saudi Arabia has an unmodified "small quantities protocol" agreement with the IAEA, which means it is exempt from routine inspections. Although the current policy leaves future options open and fuels concerns, it appears more of a political stance not to sign away national rights in the face of an uncertain Iranian nuclear program.

In this context, despite some reserved denials by the Saudis, they may actually desire that the threat of their nuclear activities be exaggerated. This could serve two purposes: first, to promote the image that the Saudi leadership is willing to "take risks" and be confrontational on a very sensitive issue, contrary to what many analysts have predicted; and second, to indirectly increase international pressure on Iran's nuclear program, since the Saudi reaction is perceived to be directly linked to it.

In approaching the delicate subject of nuclear proliferation in the region, it is necessary to be both realistic and measured. While it is important to acknowledge that several Middle Eastern nuclear programs have been underestimated in the past, overblowing the threat level could be an unnecessary escalatory factor. After all, the Bush administration's threat inflation on Iraq was disastrous.

***Ali Ahmad** is a Research Fellow studying energy policy at Harvard Kennedy School's Project on Managing the Atom and International Security Program. His research interests include energy security and resilience and the political economy of nuclear energy in newcomer markets, with focus on the Middle East.*

The terror threat of Iran in the Arab Peninsula

By Shaul Shay

Source: https://www.rieas.gr/researchareas/global-issues/middle-east-studies/4532-the-terror-threat-of-iran-in-the-arab-peninsula

Oct 10 – The security services of Saudi Arabia and Bahrain announced in September 2020, that they have thwarted terrorist plots and arrested terrorists in both countries that received support and funding from Iran. The Iranian backed Houthi rebels also conducted in September 2020, a spate of cross-border missile and drone attacks targeting Saudi military and civilian targets... **Read more**

***Shaul Shay** is senior research fellow at the International Institute for Counterterrorism (ICT) at the Interdisciplinary Center Herzliya and former deputy head of Israel's National Security Council.*

Japan to release Fukushima's contaminated water into sea: reports

Source: https://www.reuters.com/article/us-japan-disaster-water/japan-to-release-fukushimas-contaminated-water-into-sea-reports-idUSKBN27037O

Oct 16 – Nearly a decade after the Fukushima nuclear disaster, Japan's government has decided to release over one million tonnes of contaminated water into the sea, media reports said on Friday, with a formal announcement expected to be made later this month. The decision is expected to rankle neighbouring countries like South Korea, which has already stepped up radiation tests of food from Japan, and further devastate the fishing industry in Fukushima that has battled against such a move for years.

The disposal of contaminated water at the Fukushima Daiichi plant has been a longstanding problem for Japan as it proceeds with an decades-long decommissioning project. Nearly 1.2 million tonnes of contaminated water are currently stored in huge tanks at the facility.

The plant, run by Tokyo Electric Power Company Holdings Inc 9501.T, suffered multiple nuclear meltdowns after a 2011 earthquake and tsunami.

On Friday, Japan's industry minister Hiroshi Kajiyama said no decision had been made on the disposal of the water yet, but the government aims to make one quickly.

"To prevent any delays in the decommissioning process, we need to make a decision quickly," he told a news conference.

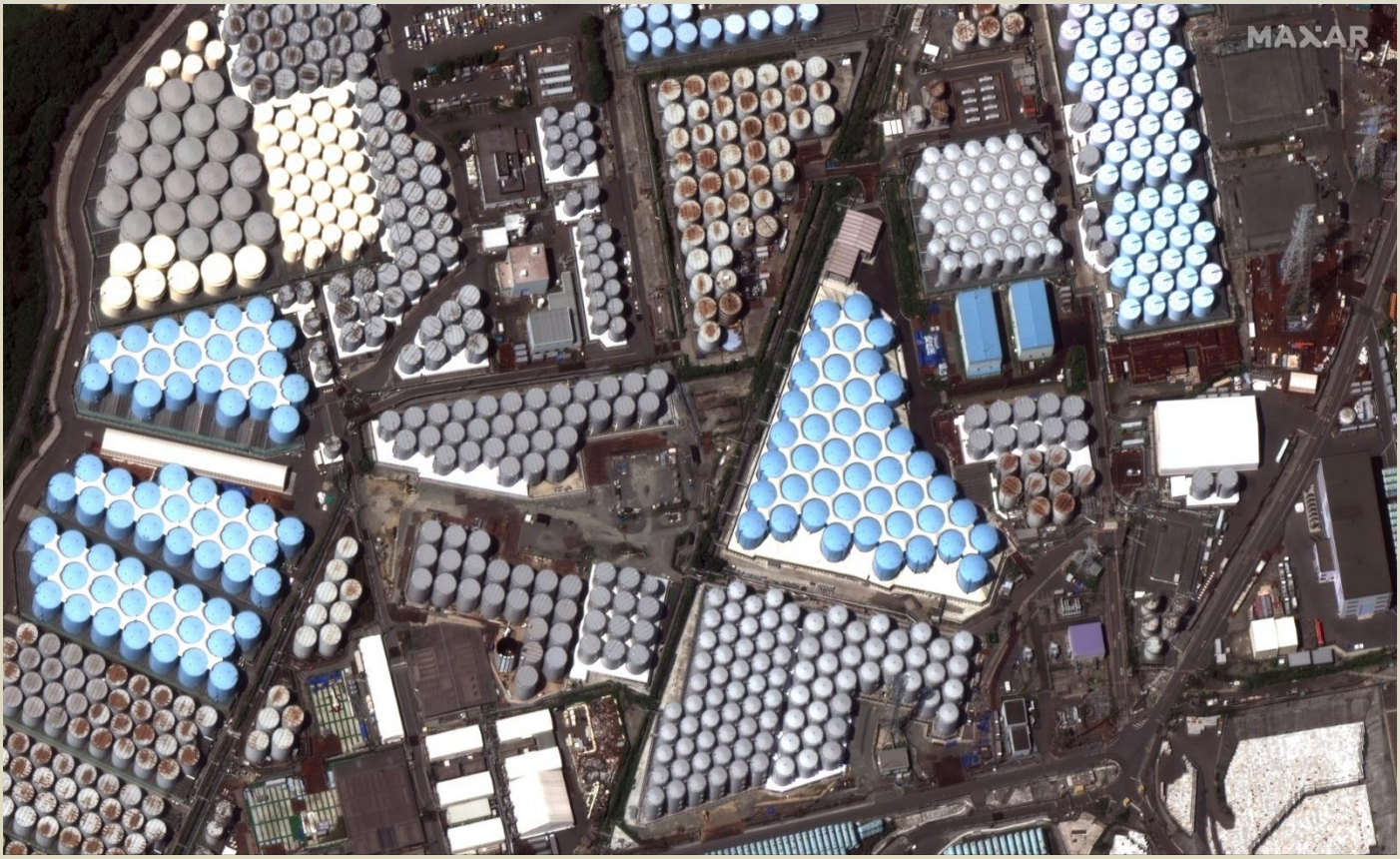
He did not give any further details, including a time-frame.

The Asahi newspaper reported that any such release is expected to take at around two years to prepare, as the site's irradiated water first needs to pass through a filtration process before it can be further diluted with seawater and finally released into the ocean.

In 2018, Tokyo Electric apologised after admitting its filtration systems had not removed all dangerous material from the water, collected from the cooling pipes used to keep fuel cores from melting when the plant was crippled.

It has said it plans to remove all radioactive particles from the water except tritium, an isotope of hydrogen that is hard to separate and is considered to be relatively harmless.

It is common practice for nuclear plants around the world to release water that contain traces of tritium into the ocean.



In April, a team sent by the International Atomic Energy Agency to review contaminated water issues at the Fukushima site said the options for water disposal outlined by an advisory committee in Japan - vapour release and discharges to the sea – were both technically feasible. The IAEA said both options were used by operating nuclear plants.

Last week, Japanese fish industry representatives urged the government to not allow the release of contaminated water from the Fukushima plant into the sea, saying it would undo years of work to restore their reputation.

9 mil radiocontaminated soil bags storage facility

South Korea has retained a ban on imports of seafood from the Fukushima region that was imposed after the nuclear disaster and summoned a senior Japanese embassy official last year to explain how Tokyo planned to deal with the Fukushima water problem.

During Tokyo's bid to host the Olympic Games in 2013, then-prime minister Shinzo Abe told members of the International Olympic Committee that the Fukushima facility was "under control".

The Games have been delayed to 2021 because of the pandemic and some events are due to be held as close as 60 km (35 miles) from the wrecked plant.

The NTI Nuclear Security Index

July 2020

Source: https://www.ntiindex.org/wp-content/uploads/2020/09/2020_NTI-Index_Report_Final.pdf

The NTI Nuclear Security Index assesses countries' progress on nuclear security, highlights security gaps, and recommends actions for governments to better protect nuclear materials and facilities and build an effective global nuclear security architecture. Developed with the Economist Intelligence Unit, the NTI Index is recognized globally as the premier resource and tool for tracking the security of some of the deadliest materials in the world.

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

C²BRNE DIARY

EXPLOSIVE NEWS

Magawa the minehunting rat sniffs out gold medal

Source: https://www.army-technology.com/news/magawa-the-minehunting-rat-sniffs-out-gold-medal/

Sep 25 – An African giant pouched rat named Magawa has been awarded a PDSA Gold Medal for detecting 39 landmines and 28 items of unexploded ordnance to date in Cambodia.

Magawa is the first rat to win the award and is one of several 'HeroRATs' bred and trained by Belgian NGO APOPO to detect landmines after bred for that purpose.
Since the 1970s it is estimated that between four million and six million landmines were laid in Cambodia, three million of which have yet to have been found. Landmines have killed around 64,000 people there.
Cambodia has the highest rate of mine amputees in the world, at over 40,000 people.
HeroRATs have so far found around 500 mines and 350 unexploded bombs in the country.
The landmines are largely a holdover from decades of war in the country and were planted by some factions including the Khmer Rouge.
The rats are light enough to walk over landmines without causing them to detonate.
A rat can search a tennis court-sized area in thirty minutes, ignoring scrap metal by detecting the chemical components of the ordnance. The PDSA said a human with a metal detector searching the same area would take up to four days.

Benjamin Netanyahu: Hezbollah has "weapons" depot near fuel depots in Beirut

Source: https://www.athina984.gr/en/2020/09/30/mpeniamin-netaniachoy-i-chezmpolach-echei-apothiki-quot-oplon-quot-konta-se-apothikes-kaysimon-sti-viryto/

Sep 30 – Israeli Prime Minister Benjamin Netanyahu today accused Lebanese Hezbollah of having a "secret" weapons depot near "fuel depots" in Beirut, which could cause a "new tragedy" in the event of an explosion.
For the past two years, Israel has accused Hezbollah, Iran's ally, of turning rockets into precision-guided missiles at various facilities in Lebanon, most notably a facility near Beirut International Airport.
In a speech from Jerusalem to the UN General Assembly today, Netanyahu presented a map showing what he said was a "secret weapons depot" on the

southern outskirts of Beirut, a Shiite stronghold near the airport. These are, according to the Israeli army, precision-guided missiles.

He clarified that "this" warehouse was located "one meter" from a "gas company" and fifty meters from a "gas station".

Referring to the deadly blast that rocked Beirut in early August, the Israeli prime minister, who is at war with Iran and Hezbollah, warned of "another tragedy" in the event of an explosion at the alleged weapons depot.

"I tell the people of the Jnah district (south of Beirut – No15 in the map – right) to act now, to oppose it, because if it explodes it will be another tragedy," Netanyahu said in English.

"I say to the Lebanese people: Israel does not want your evil, but Iran wants it. "Iran and Hezbollah have deliberately put you and your families in serious danger."

Israel and Lebanon are technically at war, and their common border, patrolled on the Lebanese side by UN forces, remains the scene of sporadic incidents.

Last year, fierce exchanges of fire on the border between the two countries brought to mind the story of one day, the ghost of the 2006 war between Israel and Hezbollah.

Since the start of the war in Syria, Israel has carried out several airstrikes in that country, specifically targeting Lebanese Hezbollah fighters and Iranian forces backing Syrian President Bashar al-Assad.

Bomb-laden donkey used in Boko Haram assassination attempt in Nigeria

Source: https://www.nzherald.co.nz/world/news/article.cfm?c_id=2&objectid=12368788

Sep 29 – Nigerian militants linked to Islamic State have used a bomb-laden donkey to attack a high-ranking government official, the latest in a series of violent attacks in the west African country.

The latest attack happened on Sunday when Babagana Zulum, Governor of Borno state, was returning to the state capital, Maiduguri, from the town of Baga, the BBC reported.

Zulum's convoy spotted a donkey on the road ahead and soldiers fired on it, setting off the explosives.

Boko Haram militants then emerged and fired on the convoy in a coordinated ambush, an official who was in one of the vehicles told the BBC.

A number of insurgents were killed in the ensuing shoot-out but the governor and his team survived unscathed.

The attack comes two days after Zulum survived another attack which killed 18.

AFP reported that Zulum has been pushing for displaced residents of Borno state to return to their homes, saying that feeding people displaced by violence in the state was not financially sustainable.
Boko Haram, which was thrust into the public consciousness in 2014 when they kidnapped 276 girls from a secondary school in the town of Chibok, has been engaged since 2009 in a violent insurgency across Nigeria, Chad, Cameroon and Niger.
The ongoing conflict has killed tens of thousands and led to millions being displaced from their homes.
They have been linked with the so-called Islamic State since 2015, when Boko Haram's leader Abubakar Shekau pledged allegiance to the terror group.
Despite Nigeria's president claiming in 2019 that the group was "technically defeated", attacks have escalated in Nigeria in recent months.

Somali Intelligence Agency Seize 79 Tons of Bomb-Making Sulphuric Acid

Source: https://allafrica.com/stories/202010141081.html

Oct 14 – Somalia's National Intelligence and security agency (NISA) said its troops have seized 79 tonnes of sulphuric acid smuggled into the country for use by al-Shabab militants to make explosives.
"We have seized 79 tonnes of sulphuric acid and arrested a number of people who smuggled it into the country and were transporting it to the al-Shabab militants," NISA said in a tweet.
The agency added that investigations were ongoing and the suspects will be arraigned later in court.

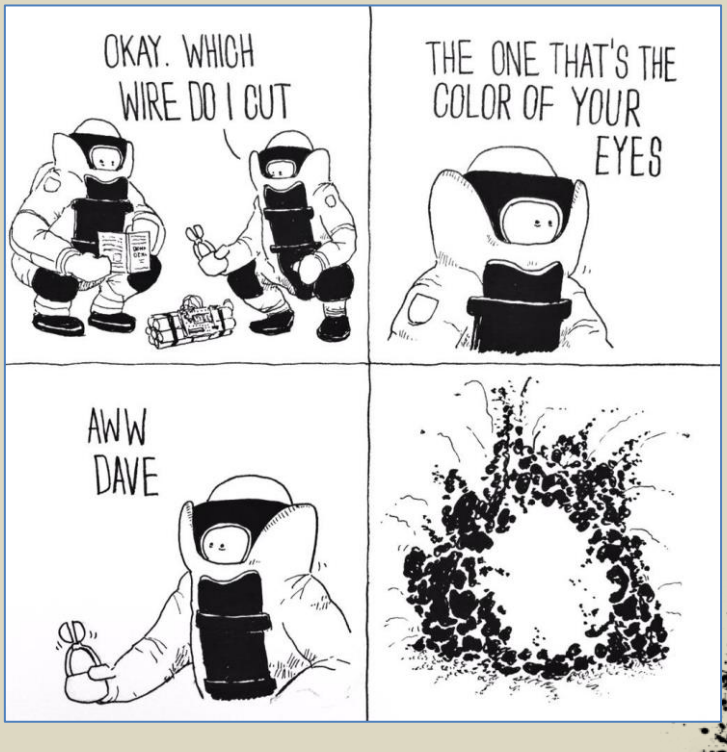
EDITOR'S COMMENT: It would be interesting to know the origin of the sulphuric acid. Given a related history during the IS times, it would be easy to direct suspicions to certain countries interested to cell to areas in conflict or trouble.

Navy EOD Releases Strategic Guidance for next 10 years, developing Force to compete and Win in GPC Environment

Source: https://www.dvidshub.net/news/381171/navy-eod-releases-strategic-guidance-next-10-years-developing-force-compete-and-win-gpc-environment

Oct 19 – Navy EOD released its force-shaping blue print for the next 10 years, Oct. 19, as its leadership looks to mold the military's maritime EOD force into one that best supports the U.S., its allies and partner nations to compete and win in an era of Great Power Competition (GPC).
The force's first major strategic mission update since 1997, the plan was developed to meet the challenges of a changing national security environment and position Navy EOD to best serve its clear, secure, build and protect role within the Navy Expeditionary Combat Force (NECF), said Rear Adm. Joseph DiGuardo, commander of Navy Expeditionary Combat Command (NECC).
"The NECF clears the explosive, security, and physical hazards emplaced by our adversaries; secures battlespace for the naval force; builds the critical infrastructure, domain awareness, and logistic capacity to rearm, resupply, and refuel the fleet; protects the critical assets the Navy and the nation need to achieve victory and reinforce blue-water lethality," said DiGuardo, who oversees the NECF, which is comprised of Navy EOD, the Maritime Expeditionary Security Force, the Naval Construction Force, and diving and salvage units.
"As part of the NECF, our EOD forces play a pivotal role clearing the explosive hazards in any environment to protect the fleet and Joint Force—from the simplest impediment to the most complex weapon of mass destruction—and build an understanding of our adversary capabilities by exploiting those hazards. Navy EOD is the key to our nation being undeterred by explosive threats," said DiGuardo.
"The strategic plan ensures Navy EOD supports the NECF by eliminating explosive threats so the fleet, Navy and nation can fight and win whenever, wherever and however it chooses," said Capt. Oscar Rojas, commodore of the Coronado, Calif., -based EOD Group (EODGRU) 1.
Rojas said this will be accomplished through the strategic plans' five core objectives: develop the Navy EOD force to win against near-peer competitors and empowered non-state actors; expand Navy EOD's advantage against competitors' undersea threats; capitalize on Navy EOD's ability to counter WMDs; grow Navy EOD's expertise in its ability to counter, neutralize and understand next-generation weapons systems; and enhance the EOD capabilities of allies and partner nations.
"Our strategic plan was designed to guide us in creating a force that can deter adversaries and win in a complex security environment," said Capt. Rick Hayes, commodore of

EODGRU-2, which operates out of Virginia Beach, Va. “That is why we dedicated an objective to specifically focus on developing and caring for our Sailors. Our people are our most important asset—they are our weapons system.”
The plan lays out how Navy EOD will grow its ability to recruit and retain the best talent, develop strong leaders of character, and use its force resiliency program, STRIKE, to improve the physical and mental care Navy EOD personnel receive throughout their careers.
“Navy EOD’s unique mission requires us to be fit in mind, body and spirit. We want our current and future operators to have access to the best facilities with the most qualified staff, so they are ready to deploy when called upon,” said Hayes, adding STRIKE’s holistic approach includes giving EOD operators access to athletic trainers, physical therapists and mental health professionals.
The force’s 1,800 operators can also expect an increased emphasis on building their knowledge and capabilities in areas critical to succeeding in a GPC environment, according to the plan.
This includes Navy EOD enhancing its expeditionary undersea capabilities by working in cyberspace. The force will pursue using unmanned systems (UMS) to access adversary communication networks to disrupt, delay or destroy weapons systems.
EOD operators will see initiatives expanding exploitation training—the understanding of a weapons systems’ assembly, capabilities and weaknesses—throughout their careers along with educational opportunities to develop their expertise to counter WMDs (CWMD). They will also work with leaders in industry, research and development, and academia to stay at forefront of unmanned systems, explosives detection, and forensic science.
Additionally, the plan calls for Expeditionary Mine Countermeasures (ExMCM) companies to be a testbed for these new systems and software.
“The operators using emerging UMS technology are the closest to the challenges. Our strategic plan will empower them to provide us feedback from the tactical level during the capability development process to help accelerate solutions to the ever-evolving threats,” said Rojas.
ExMCM companies provide military commanders a flexible, scalable and rapidly-deployable capability that ships and aircraft do not offer. They are capable of operating in theater from a variety of craft within days of tasking.
“ExMCM will be instrumental in bolstering the capabilities of our allies and partner nations as we look to better interoperate with them and define shared responsibilities during GPC in the maritime environment,” said Rojas.
The 10-year plan has ExMCM companies working with allies and partner nations to expand initiatives, such as subject matter expert exchanges and multinational exercises designed to deter peer and near-peer adversaries.
All the objectives put forward in the 2030 plan are essential to delivering a lethal, resilient and sustainable Navy EOD force that can be called upon during contingency and crisis operations, said Hayes.
“Realizing this vision will be impossible without the support of everyone in the Navy EOD community. By leveraging their creativity, discipline and leadership, we will develop a force for 2030 that continues to protect the security and future of the American people,” said Hayes.



ICI International CBRNE INSTITUTE

HOTZONE SOLUTIONS GROUP

CBRNE-Terrorism Newsletter

C²BRNE DIARY

CYBER NEWS

Nine Growth Opportunities for Post-Corona Age

Source: https://i-hls.com/archives/104272

Oct 02 – The COVID-19 pandemic has created new opportunities for innovation. The **smart city** global market is expected to reach $2.46 trillion by 2025. In fact, smart cities are highlighted as only one of nine key trends capable of generating growth opportunities from Covid-19, according to a study by Frost & Sullivan. Smart cities will prioritize more digitalized services and a strong data analytics infrastructure, leading to increased spending on technology.

Murali Krishnan, visionary innovation group senior industry analyst at Frost & Sullivan said: "In the near term, companies should focus on diversifying supply chains and leveraging new opportunities arising from changing customer demands. In the long term, it is important to internally adapt to new technologies that support workplace and operational continuity to have a smoother transformation during recovery."

The other key trends highlighted in *The Reshaping of Industries Caused by Covid-19* analysis include:

Connected living and voice activation: the increased adoption of contactless surfaces post-pandemic will power the home automation and security markets. Systems encompassing voice activation technology will become increasingly popular among consumers

Connected work: reformed connected work scenarios will accentuate the need for "cloud everything". New subscription-based models will witness a growing demand for unified-communications-as-a-service (UCaaS)

Digital health: digital health driven by telemedicine and robotic care will become the new standard of care delivery. Standardisation of service across the care continuum will require more service and technology providers

Geopolitical balance: countries should work together to keep trade flowing and ensure the supply of essential products, sending a signal of confidence to the global economy

Human augmentation: the behavioral analytics market is expected to reach $3bn in revenue in 2030, up from $230m in 2019. Post-Covid-19, behavioural data will be used to enhance healthcare systems, financial services, and cybersecurity

Lights-out operations (the management of a remote and largely unmanned recovery data center through the use of remote management software): autonomous "lights-out" operations will propel the demand for remote asset management solutions, and service providers will focus on data management strategies and data-driven business models

Supply chain optimization: the supply chain industry is creating radical innovations with augmented reality, virtual reality, advanced robotics, real-time inventory tracking, and exploring how 3D printing could completely disrupt the supply chain in the next 10 years

Technology advancements: pandemic preparedness will speed up the deployment of artificial intelligence (AI) solutions and accelerate AI innovation. Beyond specific disease management, post-pandemic economies also will rely on AI and machine learning (ML) tools to expedite digital transformation across key business initiatives, according to smartcitiesworld.net.

A Ransomware Attack Has Struck a Major US Hospital Chain

Source: https://www.wired.com/story/universal-health-services-ransomware-attack/

Sep 28 – Universal Health Services, a hospital and health care network with **more than 400 facilities across the United States, Puerto Rico, and United Kingdom**, suffered a ransomware attack early Sunday morning that has taken down its digital networks at locations around the US. As the situation has spiraled, some patients have reportedly been rerouted to other emergency rooms and facilities and had appointments and test results delayed as a result of the attack.

An emergency room technician at one UHS-owned facility tells WIRED that their hospital has moved to all-paper systems as a result of the attack. *Bleeping Computer*, which first reported the news, spoke to UHS employees who said the ransomware has the hallmarks of Ryuk, which first appeared in 2018 and is widely linked to Russian cybercriminals. Ryuk is typically used in so-called

"big-game hunting" attacks in which hackers attempt to extort large ransoms from corporate victims. **UHS says it has 90,000 employees and treats about 3.5 million patients each year,** making it one of the US' largest hospital and health care networks.

"We are using paper for everything. All computers are completely shut down," the UHS employee told WIRED. "Paper is workable, there is just a lot more documentation to be done so things don't get lost—orders, meds, etc. Patient care is about the same still in the ER, since we are where the patient enters the hospital and the visit gets started. There is concern for patients who were already on the floors when this happened, but everyone is stepping up their game big time."

"Our facilities are using their established back-up processes, including offline documentation methods," UHS said in a statement. The company did not return a request for further comment from WIRED and would not confirm that it is a ransomware attack. The company's statement did confirm that the "IT network across Universal Health Services facilities is currently offline, due to an IT security issue," and that patient and employee data appear not to have been compromised in the attack.

Ransomware attacks on large organizations have been prevalent since the mid-2010s, but the pace of assaults seems to have increased in recent months. Hospitals, in particular, have long been a favorite target, because patient safety hangs in the balance when a hospital's network goes down. In addition to UHS, the Ashtabula County Medical Center in Ohio and Nebraska Medicine have both suffered ransomware attacks in recent days that caused system outages and threatened patient services.

And earlier this month, a patient with a life-threatening condition died in Düsseldorf, Germany, after a ransomware attack at a nearby hospital forced her to be taken to a more distant facility. The episode may have been the first example of a patient who died because of the fallout from a ransomware attack.
"These incidents are hugely concerning; they could have fatal consequences," says Brett Callow, a threat analyst at the antivirus company Emsisoft. "I would say things are as bad as they've ever been—worse, in fact."
Ryuk ransomware was attributed to North Korean actors when it first emerged, but many researchers now link it instead to Russian cybercriminals. It's often preceded by a phishing attack that infects a target with a trojan, then exfiltrates the victim's data and triggers a Ryuk infection. The ransomware seems to be used by a few splinter groups in addition to its originators, though, making it difficult to trace and correlate activity from the presence of the malware alone. The actor that first used it throughout 2018 and 2019 seemed to go dark in April, but has recently reappeared.
"There are indications that the original actors are back and carrying out attacks after their absence," Emsisoft's Callow says. "The number of attacks is spiking, and as always they have a liking for health care along with other organizations."
Ryuk is one of several large ransomware families which have hit not just health care, but other large companies like Garmin and Lenovo, the shipping and logistics firm Pitney Bowes, Tribune Publishing, and numerous municipal governments around the country.
Some ransomware gangs vowed not to hit hospitals during the pandemic, but actors tied to Ryuk made no such promise.
Some researchers are calling for a ban on paying ransoms, arguing that drastically reducing that incentive is the only measure that will stop ransomware's rise now. The recommendation has been controversial, though, given how high the stakes can be for returning to normal operations during an attack—especially when the target is critical infrastructure or a health-care-related organization.
"This is extremely important. It's truly vile that people are willing to go after hospitals," the UHS ER technician told WIRED. "It is a life-or-death situation."

International Maritime Organization Hit by Cyber Attack

Source: https://imo-newsroom.prgloo.com/news/imo-website-currently-unavailable-working-to-restore-systems

Oct 05 – A number of IMO's web-based services are currently unavailable.
The issue (since 30 September 2020) is affecting IMO's public website (www.imo.org), and internal intranet services.
Internal and external emails are working as normal. Service has been restored to the GISIS database (https://gisis.imo.org/Public/Default.aspx); IMODOCS (https://docs.imo.org/Default.aspx); and Virtual Publications (https://vp.imo.org/Login.aspx?ReturnUrl=%2f).
The interruption of service was caused by a sophisticated cyber-attack against the Organization's IT systems that overcame robust security measures in place. IMO IT technicians shut down key systems to prevent further damage from the attack. The IMO is working with international IT security experts to restore systems as soon as possible, to identify the source of the attack, and further enhance security systems to prevent recurrence.

In a Battle of AI versus AI, Researchers Are Preparing for the Coming Wave of Deepfake Propaganda

By John Sohrawardi and Matthew Wright
Source: http://www.homelandsecuritynewswire.com/dr20201009-in-a-battle-of-ai-versus-ai-researchers-are-preparing-for-the-coming-wave-of-deepfake-propaganda

Oct 09 – An investigative journalist receives a video from an anonymous whistleblower. It shows a candidate for president admitting to illegal activity. But is this video real? If so, it would be huge news – the scoop of a lifetime – and could completely turn around the upcoming elections. But the journalist runs the video through a specialized tool, which tells her that the video isn't what it seems. In fact, it's a "deepfake," a video made using artificial intelligence with deep learning.
Journalists all over the world could soon be using a tool like this. In a few years, a tool like this could even be used by everyone to root out fake content in their social media feeds.
As researchers who have been studying deepfake detection and developing a tool for journalists, we see a future for these tools. They won't solve all our problems, though, and they will be just one part of the arsenal in the broader fight against disinformation.

The Problem with Deepfakes

Most people know that you can't believe everything you see. Over the last couple of decades, savvy news consumers have gotten used to seeing images manipulated with photo-editing software. Videos, though, are another story. Hollywood directors can spend millions of dollars on special effects to make up a realistic scene. But using deepfakes, amateurs with a few thousand dollars of computer equipment and a few weeks to spend could make something almost as true to life.

Deepfakes make it possible to put people into movie scenes they were never in – think Tom Cruise playing Iron Man – which makes for entertaining videos. Unfortunately, it also makes it possible to create pornography without the consent of the people depicted. So far, those people, nearly all women, are the biggest victims when deepfake technology is misused.

Deepfakes can also be used to create videos of political leaders saying things they never said. The Belgian Socialist Party released a low-quality nondeepfake but still phony video of President Trump insulting Belgium, which got enough of a reaction to show the potential risks of higher-quality deepfakes.

Perhaps scariest of all, they can be used to create doubt about the content of real videos, by suggesting that they could be deepfakes. Given these risks, it would be extremely valuable to be able to detect deepfakes and label them clearly. This would ensure that fake videos do not fool the public, and that real videos can be received as authentic.

Spotting Fakes

Deepfake detection as a field of research was begun a little over three years ago. Early work focused on detecting visible problems in the videos, such as deepfakes that didn't blink. With time, however, the fakes have gotten better at mimicking real videos and become harder to spot for both people and detection tools.

There are two major categories of deepfake detection research. The first involves looking at the behavior of people in the videos. Suppose you have a lot of video of someone famous, such as President Obama. Artificial intelligence can use this video to learn his patterns, from his hand gestures to his pauses in speech. It can then watch a deepfake of him and notice where it does not match those patterns. This approach has the advantage of possibly working even if the video quality itself is essentially perfect.

Other researchers, including our team, have been focused on differences that all deepfakes have compared to real videos. Deepfake videos are often created by merging individually generated frames to form videos. Taking that into account, our team's methods extract the essential data from the faces in individual frames of a video and then track them through sets of concurrent frames. This allows us to detect inconsistencies in the flow of the information from one frame to another. We use a similar approach for our fake audio detection system as well.

These subtle details are hard for people to see, but show how deepfakes are not quite perfect yet. Detectors like these can work for any person, not just a few world leaders. In the end, it may be that both types of deepfake detectors will be needed.

Recent detection systems perform very well on videos specifically gathered for evaluating the tools. Unfortunately, even the best models do poorly on videos found online. Improving these tools to be more robust and useful is the key next step.

Who Should Use Deepfake Detectors?

Ideally, a deepfake verification tool should be available to everyone. However, this technology is in the early stages of development. Researchers need to improve the tools and protect them against hackers before releasing them broadly.

At the same time, though, the tools to make deepfakes are available to anybody who wants to fool the public. Sitting on the sidelines is not an option. For our team, the right balance was to work with journalists, because they are the first line of defense against the spread of misinformation.

Before publishing stories, journalists need to verify the information. They already have tried-and-true methods, like checking with sources and getting more than one person to verify key facts. So by putting the tool into their hands, we give them more information, and we know that they will not rely on the technology alone, given that it can make mistakes.

Can the Detectors Win the Arms Race?

It is encouraging to see teams from Facebook and Microsoft investing in technology to understand and detect deepfakes. This field needs more research to keep up with the speed of advances in deepfake technology.

Journalists and the social media platforms also need to figure out how best to warn people about deepfakes when they are detected. Research has shown that people remember the

lie, but not the fact that it was a lie. Will the same be true for fake videos? Simply putting "Deepfake" in the title might not be enough to counter some kinds of disinformation.
Deepfakes are here to stay. Managing disinformation and protecting the public will be more challenging than ever as artificial intelligence gets more powerful. We are part of a growing research community that is taking on this threat, in which detection is just the first step.

John Sohrawardi *is Doctoral Student in Computing and Informational Sciences, Rochester Institute of Technology.*
Matthew Wright *is Professor of Computing Security, Rochester Institute of Technology.*

Fooling Deepfake Detectors

Source: http://www.homelandsecuritynewswire.com/dr20201012-fooling-deepfake-detectors

Oct 12 – Last month Sophie Wilmès, the prime minister of Belgium, appeared in an online video to tell her audience that the COVID-19 pandemic was linked to the "exploitation and destruction by humans of our natural environment." Whether or not these two existential crises are connected, the fact is that Wilmès said no such thing. Produced by an organization of climate change activists, the video was actually a deepfake, or a form of fake media created using deep learning. Deepfakes are yet another way to spread misinformation – as if there wasn't enough fake news about the pandemic already.
Because new security measures consistently catch many deepfake images and videos, people may be lulled into a false sense of security and believe we have the situation under control. Unfortunately, that might be further from the truth than we realize. "Deepfakes will get only easier to generate and harder to detect as computers become more powerful and as learning algorithms get more sophisticated. Deepfakes are the coronavirus of machine learning," said Professor Bart Kosko in the Ming Hsieh Department of Electrical and Computer Engineering.
In a recent paper originating from Professor Kosko's neural learning and computational intelligence course, Electrical and Computer Engineering masters students Apurva Gandhi and Shomik Jain showed how deepfake images could fool even the most sophisticated detectors with slight modifications. Concurrent research from Google Brain cited their paper and extended methods for creating these modifications. A team at the University of California San Diego also arrived at similar conclusions about deepfake videos.
Today's state-of-the-art deepfake detectors are based on convolutional neural networks. While initially, these models seem very accurate, they admit a major flaw. Gandhi and Jain showed that these deepfake detectors are vulnerable to adversarial perturbations – small, strategically-chosen changes to just a few pixel values in an image
"If a deepfake is a virus and a deepfake detector is a vaccine, then you can think of adversarial perturbations as a mutation," said Gandhi. "Just like one tiny mutation of a virus might render a vaccine useless, tiny perturbations of an image can do the same to state-of-the-art deepfake detectors."
The results of their paper expose just how flawed our current security systems are. The neural networks the two trained initially identified over 95% of the normal, everyday deepfakes. But when they perturbed the images, the detectors were able to catch (checks notes) zero percent. Yes, you read that correctly. Under the right circumstances, this technique essentially renders our entire deepfake security apparatus obsolete. With an election around the corner and a pandemic threatening global stability, the ramifications cannot be understated.
Of course, the goal of any good engineer is to provide solutions, not just point out flaws. And the next step for Gandhi and Jain is to do just that. Their first idea is to make neural networks more stable to adversarial perturbations. This is done by something called regularization, a strategy that improves the neural network stability while it is still being trained. This technique improved the detection of perturbed deepfakes by 10% – encouraging but not game-changing.
Their more promising strategy, however, is something called the **deep image prior defense**. Essentially this process tries to remove these sneaky perturbations from the images before feeding them to a detector. To develop this technique, the two creatively re-purposed algorithms originally written to improve image quality. While the deep image prior defense identified perturbed deepfakes with 95% accuracy, the algorithm is very slow. **Processing just one image can take 20-30 minutes.** "A pressing challenge is to find more efficient methods, potentially without neural networks, to improve deepfake detectors so that they are immune to adversarial perturbations," said Jain. Then these techniques could improve vulnerable detectors on platforms like social media."

Europol Targets Jihadist Propaganda

Source: https://www.europol.europa.eu/newsroom/news/targeted-propaganda-material-disseminated-in-languages-of-western-balkan-countries
Oct 08 – A total of 346 links of terrorist content on 27 platforms were assessed and referred during a law enforcement action day involving Western Balkan countries.

The referral action day targeting online jihadist propaganda took place on October 6 2020. The European Union Internet Referral Unit (EU IRU) at Europol organized the operational activities in cooperation with Croatia. Specialized units from Albania, Bosnia and Herzegovina, Croatia, North Macedonia, Montenegro, Serbia and Slovenia also participated in the action day.
The referral action targeted online content disseminated by members and supporters of al-Qaeda, the so-called Islamic State and affiliated groups. The counterterrorism units from the participating countries, together with the EU IRU, looked into jihadist propaganda material, such as video tutorials, nashids, social media accounts inciting to violence. The content was spread in the languages of the Western Balkan countries mainly by local supporters of the targeted jihadist organizations.
Europol's EU Internet Referral Unit collected the contributions sent by the Western Balkan countries and stored the content in its database. After cross-checking against Europol databases and performing de-confliction with participant countries, the material was referred to the online service providers.

Trust in COVID Info Sources Varies by Demographics, Beliefs

By Mary Van Beusekom
Source: http://www.homelandsecuritynewswire.com/dr20201015-trust-in-covid-info-sources-varies-by-demographics-beliefs

Oct 15 – People seek COVID-19 information from different sources based on sex, age, education level, political bent, and beliefs about the pandemic, according to a study published last week in *JMIR Public Health and Surveillance*.
Led by researchers at New York University (NYU), the study involved recruiting US adults on Facebook to complete an online survey in two rounds in March and April on their use of 11 different coronavirus information sources and their most trusted source of information.
The vast majority of the 11,242 participants who completed the survey (91.2%) said they turned to traditional news sources such as television, radio, podcasts, and newspapers. But the largest single source of COVID-19 information was government websites (87.6%), which were also the most trusted source (43.3%). Another large source was social media (73.6%), although participants said they trusted government information far more.
Men and those aged 40 and older reported lower levels of trust in government websites than younger participants. Those surveyed in April, as opposed to March, were significantly less likely to use and trust government websites, while trust in other websites, radio news or podcasts, and spouses or other partners more than doubled during that time. April participants also used, on average, 0.58 fewer sources than March respondents.
Non-white participants were more likely than whites to consult doctors and religious leaders for sources of information.

Type and Number of Sources, Knowledge Levels
The 7,811 of 11,242 respondents (69.5%) who reported consulting mainstream media sources said they most often used television network news outlets such as CNN (24.0%), Fox News (19.3%), and other local or national stations (35.2%).
Republicans were significantly more likely to rely on Fox News and less likely to consult all other mainstream media outlets. In contrast, participants with a bachelor's degree or higher said they relied more on CNN and other international news networks. Respondents 60 years and older said they relied more on Fox News and MSNBC than on international news sources.
On average, respondents used 6.1 sources of coronavirus information. Men and participants who were aged 40 and older, unemployed or retired, and Republican used fewer sources than those with children at home and a higher education level. Respondents with a bachelor's degree or higher were more likely than others to use all sources of information except for traditional media.
While many coronavirus-related beliefs were significantly predictive of information sources and degree of reliance on mainstream media, the link between source and COVID-19 knowledge was mixed.
Use of more information sources was linked to improved awareness that wearing face coverings helps impede spread of the virus, and participants who used government websites had significantly more COVID-19 awareness than others.
Most survey respondents were women (59.0%), white (92.7%), employed (59.5%), and living in suburbs (51.0%).

Influence of Beliefs, Political Affiliation
Those who relied on CNN or MSNBC tended to agree that COVID-19 is deadlier than seasonal flu, the media has devoted the right amount of coverage to the pandemic, and the virus is a bigger issue than the government suggests, while they disagreed that warm weather reduces virus spread and that coronavirus is a smaller issue than media coverage suggests.
Those who consulted government websites were more likely than those who didn't to disagree that the coronavirus was released as a terroristic act, the media exaggerated the

threat of COVID-19, and warm weather slows the spread of the virus, while people who watched Fox News tended to agree with those statements. The also tended to disagree that COVID-19 is deadlier than seasonal flu, the media coverage of the pandemic has been proportional to the problem, and the coronavirus is a bigger issue than the government has suggested.

The authors said that understanding the development of coronavirus information, the channels used for dissemination, and the populations targeted is important to be able to convince the public that lockdowns and other public health measures—which can cause substantial social disruptions—are needed to contain the virus. Targeted messages through trusted sources can also help counter misinformation spread over the Internet.

"COVID-19 information source was significantly determined by participant sociodemographic characteristics and was also associated with both knowledge and beliefs about the pandemic," the authors wrote. "Study findings can help inform COVID-19 health communication campaigns and highlight the impact of using a variety of different and trusted information sources."

Lead author Shahmir Ali, a doctoral student at NYU, said in a university press release that public health officials need to work to ensure that COVID-19 information reaches diverse populations.

"We have already started to see this, for instance, through initiatives by social media platforms to connect users with COVID-19 information while they are using these apps," Ali said. "Our research provides crucial evidence to push for these types of initiatives to get COVID-19 information out to the public in a manner that matches what sources they already use and trust."

Mary Van Beusekom *is a news writer at the University of Minnesota's Center for Infectious Diseases Research and Policy (CIDRAP).*

Details of Russia's Cyberattacks against Olympic, Paralympic Games Revealed

Source: http://www.homelandsecuritynewswire.com/dr20201021-details-of-russia-s-cyberattacks-against-olympic-paralympic-games-revealed

Oct 21 – **The U.K. On Monday (19 October) exposed malicious cyberactivity from Russia's GRU military intelligence service against organizations involved in the 2020 Olympic and Paralympic Games before they were postponed.**

The activity involved cyber reconnaissance by the GRU targeting officials and organizations involved in the Games, which had been due to take place in Tokyo during the summer.

The U.K. National Cyber Security Center (NCSC) said the the incidents were the latest in a campaign of Russian malicious activity against the Olympic and Paralympic Games, with the U.K. on Monday also revealing details of GRU targeting of the 2018 Winter Olympic and Paralympic Games in Pyeongchang, Republic of Korea.

The NCSC, a part of GCHQ, says it assesses with high confidence that these attacks were carried out by the GRU's Main Centre for Specialist Technologies (GTsST), also known as Sandworm and VoodooBear.

Details were released after the U.S. Department of Justice announced criminal charges against Russian military intelligence officers working for the GRU's cyber unit for conducting cyberattacks against the 2018 Winter Games and other cyberattacks.

The Foreign Secretary Dominic Raab has issued a statement making clear that the Russian government cannot act with impunity.

Paul Chichester, the NCSC's Director of Operations, said:

"We condemn these attacks carried out by the GRU and fully support the criminal charges announced today by the U.S. Department of Justice.

"These attacks have had very real consequences around the world – both to national economies and the everyday lives of people.

"We will continue to work with our allies to ensure that we are the hardest possible target for those that seek to cause disruption and harm in cyberspace."

In the attacks on the 2018 Games, the GRU's cyber unit attempted to disguise itself as North Korean and Chinese hackers when it targeted the opening ceremony. It went on to target broadcasters, a ski resort, Olympic officials and sponsors of the games.

The GRU deployed data-deletion malware against the Winter Games IT systems and targeted devices across the Republic of Korea using VPNFilter.

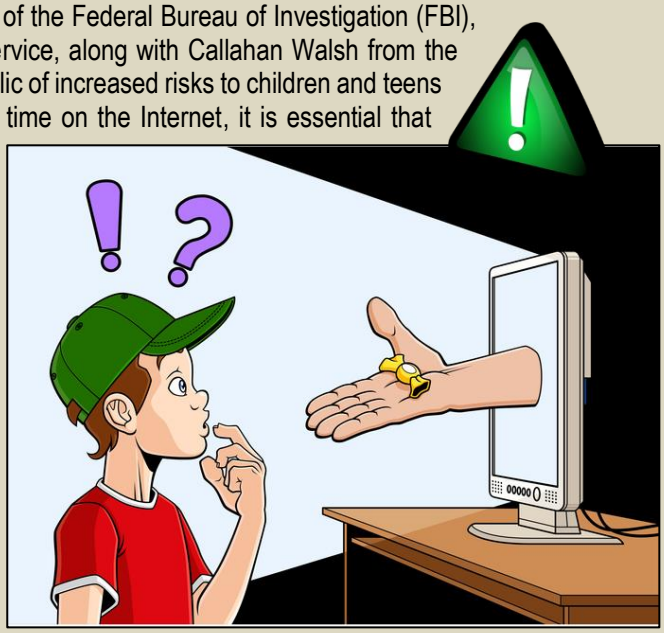
The NCSC assesses that the incident was intended to sabotage the running of the Winter Olympic and Paralympic Games, as the malware was designed to wipe data

from and disable computers and networks. Administrators worked to isolate the malware and replace the affected computers, preventing potential disruption.

Internet Predators: Warnings and Prevention for Families During the Pandemic and Beyond

Source: https://www.hstoday.us/subject-matter-areas/cybersecurity/internet-predators-warnings-and-prevention-for-families-during-the-pandemic-and-beyond/

Oct 14 – Antoinette T. Bacon, Acting United States Attorney for the Northern District of New York, and James P. Kennedy, United States Attorney for the Western District of New York, met today with leaders of the Federal Bureau of Investigation (FBI), Homeland Security Investigations (HSI), and the United States Marshals Service, along with Callahan Walsh from the National Center for Missing and Exploited Children (NCMEC), to warn the public of increased risks to children and teens from online sexual predators. In an era where children are spending more time on the Internet, it is essential that parents, guardians, educators and trusted adults know the risks and how to prevent exploitation.



"Children are spending more time online, for school, for clubs, and for playdates. Parents don't know all the apps or how to use them, but sexual predators do. They know where the kids are and how to reach them. Just as parents taught kids to be safe at home by locking the doors at night, parents must learn how to keep kids safe online. Computers can be scary. The internet can be intimidating. But in this case, ignorance is not bliss," said Antoinette T. Bacon, Acting United States Attorney for the Northern District of New York. "The Department of Justice is committed to keeping kids safe. We will continue to pursue online sexual predators, and with increased awareness on the part of parents and communities, we will stop even more."

"The borderless nature of the Internet has made these crimes which transcend jurisdictional boundaries," stated United States Attorney Kennedy. "Cases in our district frequently involve victims in the Northern District and vice versa. Working together we will use our prosecutorial resources to do all that we can to protect our kids, but we cannot do it alone. All New Yorkers and all Americans have a duty to protect our children—both in the physical and online world."

"Homeland Security Investigations is committed to the Safety Pledge initiative, which demonstrates a whole of government commitment to protecting and safeguarding children online," said Kevin Kelly, HSI Special Agent in Charge. "It is a reminder that we must all dedicate ourselves to implement the critical measures at home and in our communities that are necessary to keep children safe from online predators."

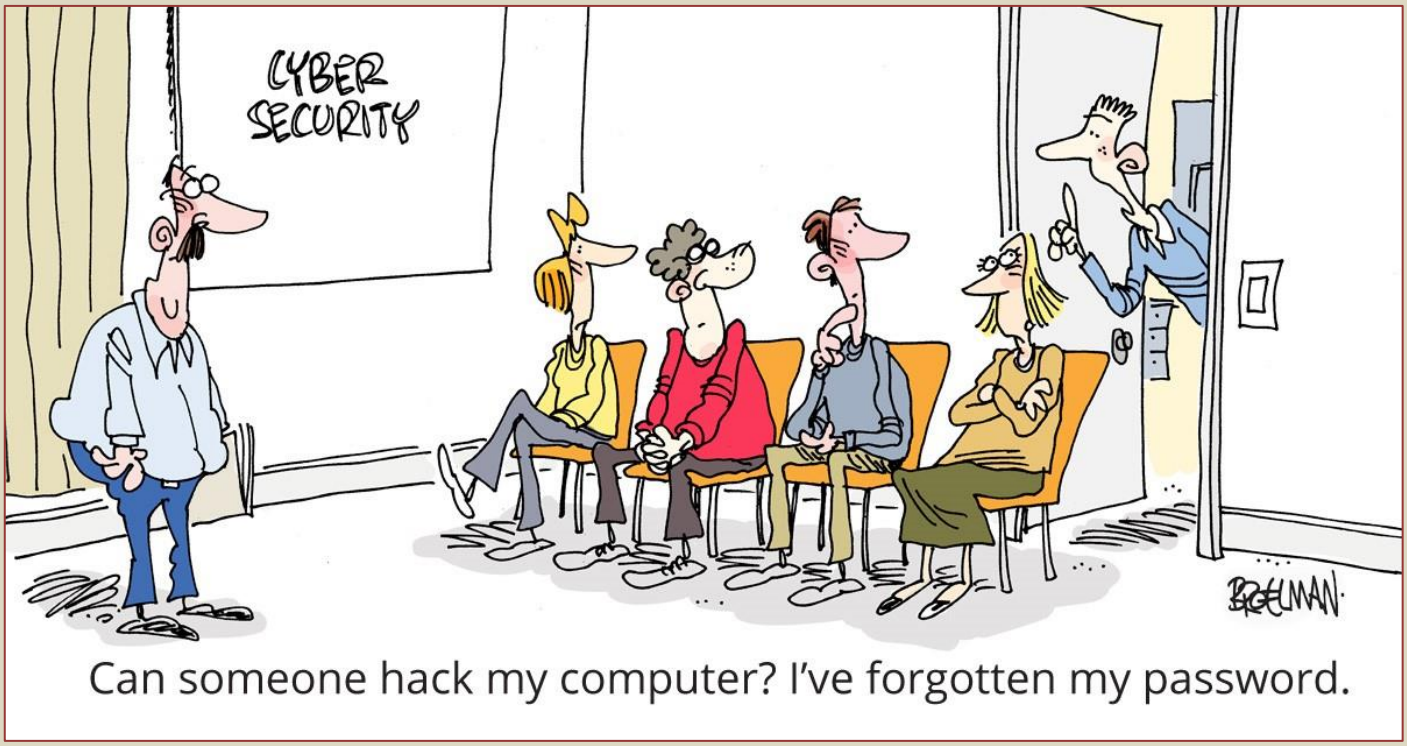
"Make no mistake about it, investigating and arresting online predators is a top priority for the FBI and our office is leading the charge locally in keeping our most vulnerable safe from the monsters who lurk behind their keyboards. These disturbing individuals are preying on innocent children online and our office is working with our partners to aggressively pursue justice for their victims," said Thomas F. Relford, Special Agent in Charge, Federal Bureau of Investigation, Albany Field Office.

"At NCMEC, we are dedicated to fighting child sexual abuse online wherever we find it and working to prevent the future victimization of children," said Callahan Walsh, NCMEC Child Advocate. "With increased screen time experienced by both adults and children during the pandemic, the opportunities for exploiters to pray on our kids has only increased and we encourage parents to talk to their kids about being safe online."

Lisa Fletcher, the Assistant United States Attorney who oversees the prosecutions of these cases in the Northern District of New York, and has seen hundreds in our district says, "Ensuring the safety of our children is the most important job any of us will ever have. We must all educate ourselves and talk to our children about the risks inherent in the open access the Internet provides. Talk to your kids about what sites they are visiting, what apps they use, whom they are texting and messaging, what kinds of pictures they take of themselves, and what kinds of pictures other people send to them. Encourage them to share with you anything makes them uncomfortable, whether an image, a message, or a solicitation. Showing that you care will go a long way with a child, and that in turn will go a long way in keeping them safe."

Prevention is key. There are resources available for parents, teachers, and our kids from kindergarten through high school.

- NetSmartz has a number of websites with tool kits, games, videos for all ages, PowerPoints for educators, Tip Sheets and more. Go to NetSmartz.org
- Homeland Security Investigations and NCMEC just launched their SafetyPledge campaign, encouraging parents to pledge to talk with their children about this threat. Their website includes a tool kit packed with information. Go to SafetyPledge.org
- The Federal Bureau of Investigation's website, entitled Safe Online Surfing, has resources categorized from 3rd grade through 8th grade, for teachers and students. Go to SOS.FBI.gov



ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

C2BRNE DIARY

DRONE NEWS

When stupidity & PSYOPs meet technology

Source: https://www.pronews.gr/amyna-asfaleia/ellinotoyrkika/918726_toyrkiko-drone-epaixe-ton-toyrkiko-ethniko-ymno-pano-apo

Sep 26 – The Turks continue the challenges, this time a Turkish drone flew to Kastelorizo and started playing the Turkish national anthem.

Specifically, the incident took place on the morning of Saturday, September 26, with the residents wondering where the raids and the Turkish national anthem are coming from.

Residents began to wonder where the sound of the raid came from, when they suddenly saw a drone flying the Turkish national anthem and raids flying over their heads.

"It's unthinkable! Did the gossipy Turks come to play raids in our houses? Its a shame! Let them know that we are not afraid of them, let them put an end to the speakers, we do not understand from such. We have our Army here that protects us. "But the police must act," said a resident of Kastelorizo, expressing his indignation at the incident.

At the same time, he revealed that strangers (?) had painted, again by drone (?), with red paint the Greek flag located in the northern part of the island and formed by stones painted in blue and white.

"If they think that in such ways, they will frighten us, the Turks are laughing," the resident notes. "As soon as the Army was informed, it immediately repaired the damage and the Greek flag is again there for the Turks to see from the other side."

Meanwhile, continuing its provocative policy in the Aegean, Turkey today issued NAVTEX, for September 29, blocking an area between Rhodes and Kastelorizo.

Qatar Airways becomes the first global carrier to operate Honeywell's ultraviolet cabin cleaning technology

Source: https://www.iloveqatar.net/news/general/qatar-airways-first-global-carrier-operate-honeywell-uv-cabin-system

Sep 28 – Qatar Airways becomes the first global carrier to operate Honeywell's Ultraviolet (UV) Cabin System, further advancing its hygiene measures onboard. In clinical tests, UV light has been shown to be capable of inactivating various viruses and bacteria when properly applied.

Approximately the size of a beverage cart, the system has extendable UV arms that treat aircraft seats, surfaces and cabins without using cleaning chemicals.

Having already received six of the Honeywell UV Cabin System, the devices have undergone comprehensive testing onboard Qatar Airways aircraft, before entering service. The airline aims to acquire additional units in the near future, in order to operate them onboard all aircraft turnarounds at Hamad International Airport (HIA).

Qatar Airways Group Chief Executive, His Excellency Mr. Akbar Al Baker, said: "We are pleased to be the first global airline to operate the Honeywell UV Cabin System onboard our aircraft. In clinical tests, UV light has been shown to be capable of inactivating various viruses and bacteria when properly applied at specified doses.

"During these unprecedented times, the health and safety of our crew and passengers continue to be of the utmost importance. Since the start of the pandemic, we have been regularly introducing new and effective safety and hygiene measures onboard our aircraft, based on our unparalleled expertise of flying consistently throughout."

Honeywell Aerospace President EMEAI, Mr. James Currier, said: "Honeywell has technology today that can make air travel safer – from the traveller to the airport worker, throughout the airport and onboard the aircraft. We're working across business lines to develop new products such as Honeywell ThermoRebellion, a new temperature-monitoring solution - Environmental Control System Check, which allows airlines to monitor airflow in the cabin, and an array of Personal Protective Equipment. All this allows for cleaner and safer airports."

Qatar Airways' aircraft will continue to be regularly disinfected using cleaning products recommended by the International Air Transport Association (IATA) and the World Health Organization (WHO). The Honeywell UV Cabin System will be utilised as an additional step

after manual disinfection, to ensure the very highest standards of cleanliness. The airline's onboard linen and blankets will continue to be washed, dried and pressed at microbial lethal temperatures, while its headsets are rigorously sanitised after each flight. These items are then sealed into individual packaging by staff wearing hygienic disposable gloves.

Qatar Airways' aircraft also features the most advanced air filtration systems, equipped with industrial-size HEPA filters that remove 99.97% of viral and bacterial contaminants from re-circulated air, providing the most effective protection against infection.

In July, Qatar Airways further increased its health and safety measures onboard by introducing new personal protective equipment (PPE) for customers and cabin crew. The airline's robust measures included offering face shields to all passengers, in addition to a disposable protective gown for cabin crew, which is fitted over their uniforms, in addition to safety glasses, gloves and a mask.

Onboard, all Qatar Airways passengers are provided with a complimentary protective kit. Inside a ziplock pouch, a single-use face mask, large disposable powder-free gloves and an alcohol-based hand sanitiser gel are offered. Business Class customers also receive an additional 75ml sanitiser gel tube. In addition, for aircraft equipped with Qsuite, Qatar Airways' award-winning business seat, Business Class customers are offered even greater privacy with sliding partitions and fully closing doors, and an option to display a 'Do Not Disturb (DND)' indicator if they wish to limit their interactions with cabin crew.

Since the start of the COVID-19 crisis, the airline has also applied other additional health and safety measures on-board its flights. Business Class meals are served covered on a tray instead of a table set up, and a cutlery wrap is offered to passengers as an alternative to individual cutlery service, in an effort to minimise contact between crew and passengers. Qatar Airways has also introduced single-use menu cards and sealed refreshing wipes. Economy Class meals and cutlery are served sealed as usual, and menu cards have been temporarily discontinued. All social areas onboard the aircraft have been closed adhering to social distancing measures.

HIA, the airline's hub in Doha, has also introduced UV-C disinfectant robots which are fully autonomous mobile devices emitting concentrated UV-C light, and are deployed in high passenger flow areas to reduce the spread of pathogens. The Oryx Airport Hotel at HIA has also implemented UV-C light to monitor and ensure a thorough cleaning process across all rooms, using a pen only visible under UV light to mark frequent touchpoints. The marked areas undergo the highest levels of sanitisation before being checked and analysed, allowing the hotel management to further enhance its cleaning techniques and standards.

In addition, HIA has implemented stringent cleaning procedures and applied social distancing measures throughout its terminals. All passenger touchpoints are sanitized every 10-15 minutes and every boarding gate and bus gate counter is cleaned after each flight. Hand sanitizers are provided at immigration and security screening points.

The national carrier of the State of Qatar now operates over 650 weekly flights to more than 90 destinations, providing more flexible travel options to more global destinations than any other airline. A multiple award-winning airline, Qatar Airways was named 'World's Best Airline' by the 2019 World Airline Awards, managed by the international air transport rating organisation Skytrax. It was also named 'Best Airline in the Middle East', 'World's Best Business Class', and 'Best Business Class Seat', in recognition of its ground-breaking Business Class experience, Qsuite. It is the only airline to have been awarded the coveted "Skytrax Airline of the Year" title, which is recognised as the pinnacle of excellence in the airline industry, five times. Its home and hub, HIA, was recently ranked 'Best Airport in the Middle East' and 'Third Best Airport in the World' by the Skytrax World Airport Awards 2020.

An Insider Perspective: What the Internet Means to UK Jihadists

By Dr. Elizabeth Pearson

Source: https://gnet-research.org/2020/09/14/an-insider-perspective-what-the-internet-means-to-uk-jihadists/

Sep 14 – September 2016, just hours before I was due to interview the radical Islamist leader Anjem Choudary, I received a text. He asked, for reasons of propriety, could I bring someone along (a *mahram*)? It was a last-minute request. The one friend who was willing and free had never heard of Anjem Choudary. 'Who is he again?' she asked. 'I'm sure he'll tell you,' I said. And so he did, introducing himself with a speech about how many thousands of Twitter followers he had.

Choudary was a known social media influencer, sharing views aligned closely with those of Islamic State. Many of his supporters travelled to Syria and Iraq. Many did not come back. In the end his accounts were removed.

Scholars of radicalisation know that the net matters, even if the extent is unclear. We know that the Internet can act as a facilitator to radicalisation, aiding groups to recruit and propagandise. What's more, as terrorists populated social media platforms, data was easy to find. This data allowed us to better understand, from an organisational perspective, how extreme movements engaged the Internet. But so far this has mainly been an 'outside-in' analysis. What's less clear from large-n studies are the meanings extreme actors themselves attach to the online space. Additionally, offline and online behaviours are frequently each

explored as separate spaces, despite calls for the relationship between them to be better understood.
This GNET Insight is about going 'inside-out'. Talking to extremists is hard, but doing so – as I did in the course of my PhD – helps us understand what the net means to extreme actors, as people, not just members of an organisation. This blog is based on semi-structured interviews carried out between May 2016 and February 2018 with some 14 participants networked to the banned Islamist group al-Muhajiroun, led by Choudary. It's also about better understanding, through those encounters, the complex and blurred relationship between what we think of as 'online' and 'offline' in radicalisation.

So, what did the online space mean to participants?

First, although policymakers can talk about online and offline as distinct, to the research participants, this was a false dichotomy. Connections initiated online did not stay online, and links made there were not trivial. For instance, white convert Adam told me his marriage to a young Muslim woman developed from online messaging, which complemented and intensified an existing local link. For Umm M, a convert in her 30s, an online connection also led to marriage. Her husband, a high-status Islamist, approached her online to translate a text but then quickly crossed continents to meet and marry her. Both Saleha, a 19-year-old British Bangladeshi student and Abu M, in his early 20s, also told me they had had romantic relationships that began online, both describing the community as a dating pool. Social media as a jihadist dating site is not a new idea. But these participants said finding a devout – read salafi-jihadi – partner through the Internet was about an expression of the *deen* of Islam. Saleha considered her online affair a 'proper relationship', hoping it would lead to marriage, as a fulfilment of Islam.

Heart-washing

Second, what is less well captured in the online radicalisation literature is the emotion participants invest in the online community. Participants were involved in all the activities noted in literature on the online strategies of extremist groups – *dawah* in the form of street propagandising, recruitment, network-consolidation, evidencing views, sharing news links, and organising of events. However, these terms fail to capture the fundamental affective and emotional experience participants described in involvement in these actions. As Adam told me, "Why do you do it? It's because you're helping other people and it makes you feel good." When later charged with terrorism offences he hoped photographs of his good deeds online would convince authorities of his moral intentions, "feeding the homeless people, giving old people clothes – I can show the police and maybe it will help." Participants also resisted the vocabulary used by scholars, including myself. Rifat, one of Choudary's circle, told me he saw himself described in the media as 'an acolyte' of Anjem Choudary, when this was in fact 'friendship'. Recruitment, online mobilisation, *dawah* – to Rifat, these were simply 'the truth'. These actions mattered because they were authentic, in a world of inauthenticity, amorality and secularism, the antithesis of Islam.
This was particularly important when considering what terrorism scholars would characterise as online mobilisation. It is well known that videos depicting atrocities against Muslims across global contexts produce recruits. Zakir, later jailed for terrorism offences, was on the brink of tears as he described a particularly distressing image widely circulated on social media: a wailing Syrian father holding his headless toddler daughter. Grief demands an appropriate response. These tears would result in Zakir's aiding the struggle.
Indeed, Umm M, who had watched her husband systematically recruit to Islamic State told me, "It was easy for people to get carried away. I don't know if it's 'brainwashing', they are not using their brains on this, they are using their hearts. It is heart-washing… driven by emotions." Umm M, like others, distanced herself from explanations of recruitment or radicalisation that did not emphasise authenticity and emotion.
Third, it was clear that the context and location of accessing online spaces factored in radicalisation. For instance, for some time before I spoke to her, Saleha had propagandised online for Daesh. She explained the attraction, which partly lay in how she accessed the

Internet: this was secret from her strict family, who would not allow her to have a boyfriend. It was also only on her phone, as there was only one computer in the house. This phone was always on her person, and every notification of a new message filled her with excitement. The relationship with her mobile phone itself was emotional, secret, and sensual, involving touch, sight, and sound.

Community vs Paranoia

Fourth, the online space offered a community that could confer authority, and status. I had not intended to ask about participants' relationship with online spaces. But they spontaneously talked about social media, because it mattered. People for instance referred to the 'Facebook Crew', an online community they acknowledged as a barometer for their own views and knowledge. Islamic knowledge was one indicator of status in this network. Popularity was another. As Choudary hinted, leaders were admired for many reasons, not all strictly theological. Umm M, whose husband was respected and popular said, "It's a celebrity thing. You know [my ex-husband] has got a lot of fans. He has charm – all the girls, a lot of girls were after him. I'm not insecure but – [he had] groupies." Women whose Twitter biographies warned brothers not to DM them, at the same time sent flirtatious messages to Umm M's ideologue husband.

Finally, this meant that the online network, this community of like minds, brought with it not just social and emotional benefits, but risks. The 'Facebook Crew' could turn on an individual it suspected of betrayal, or *fitnah* and dissent. Participants repeatedly emphasised that I must not reveal online that they were talking to me, in case they were ostracised. They also feared being tagged in posts that might have criminal repercussions, particularly by members who did not live in the UK. One participant told me he had had mental health issues as a result of his membership of this community. The longer that I spoke to participants, the more they revealed the ways in which the Internet was harming them:

"They have a very insecure mentality. Anyone that doesn't fit their spectrum, would easily get bashed and called a spy."

"Every Muslim should just stay off social media and – don't use the Internet. I don't need the Internet."

"I have many pro Isis friends on fb some think I'm also an Isis supporter... if they find out I'm not they will probably call me a non-Muslim, so I just keep quiet."

The community had benefits, but it also bound participants to the Islamic State network, even when they wanted to leave.

Online/Offline: A False Dichotomy

It will never be easy to stop talking about extremist spaces as either online or offline. The language we routinely use makes this distinction for us. But the insights from this 'insider-out' approach suggest the false dichotomy of online versus offline in understanding radicalisation. This was one blurred space. Equally, we cannot understand radicalisation as about either ideology or emotion. My conversations with members of Anjem Choudary's social media network revealed how online mattered to them: as community, and as a site of knowledge, status, and truth. It was about connections, authenticity, an affective experience. In particular, therefore, this insight calls for greater recognition of the role of emotion in radicalisation. And it problematises the framing of work on online extremism that fails to take account of the ways in which people who support extreme groups understand and apply meaning to their own online space.

Dr. Elizabeth Pearson *is a Lecturer at the Cyber Threats Research Centre (CyTReC) @ University of Swansea, specialising in gender, extremism, and how to counter extremism. Elizabeth has an interest in offline and online and their intersections. She has worked with VOX-Pol, the EU's online extremism research network, conducting research on gender in ISIS-supporting communities on Twitter. She studied for her PhD in War Studies at King's College London, where she explored gender in both 'Islamist' and 'far-right' movements in the UK through field research and interviews with activists. Elizabeth is also an Associate Fellow at RUSI and has carried out research for the London-based think tank examining attitudes to both Violent Extremism and Countering Violent Extremism in the UK, France, Germany, the Netherlands and Canada. Elizabeth also maintains a dataset of female suicide bombing in West Africa and has an interest in issues of gender in relation to 'Boko Haram'. She has worked with the European Union Technical Assistance to Nigeria's Evolving Security Challenges (EUTANS) and with RUSI on CVE delivery in Nigeria. Before academia, Elizabeth spent more than fifteen years with BBC radio where she worked in production, reporting and feature-making, mainly for BBC Radio Four.*

Purdue University and Abu Dhabi Work Together on Cybersecure Drone Swarms

Source: https://www.hstoday.us/subject-matter-areas/airport-aviation-security/purdue-university-and-abu-dhabi-work-together-on-cybersecure-drone-swarms/

James Goppert is part of a multidisciplinary team studying how drone technology can help Abu Dhabi, the capital city of the United Arab Emirates, become a Middle East technology and innovation hub. (Purdue University photo/John Underwood)

Oct 06 – A group of Purdue University researchers have been tasked to make sure drones and their systems could operate securely, safely and efficiently in the United Arab Emirates capital, Abu Dhabi.

Inseok Hwang, a professor in the School of Aeronautics and Astronautics, is principal investigator on a three-year, $2.3-million grant from the Technology Innovation Institute in Abu Dhabi to study the application of secure drone swarms in urban environments.

The project requires expertise in autonomous vehicles, control, sensing, virtual reality and security. James Goppert, a visiting assistant professor in the School of Aeronautics and Astronautics and managing director of the UAS Research and Test Facility, and Dongyan Xu, the Samuel D. Conte Professor of Computer Science and director of CERIAS (Center for Education and Research in Information Assurance and Security), Purdue's cybersecurity research and education center, are co-principal investigators on the project.

"We will address this problem in a highly integrated, interdisciplinary way," Hwang said. "We will consider it from the program level to the high-level network of systems, so we accomplish the hierarchic way from the very detailed lower level, the software and hardware level, to the large network of vehicles and from the single vehicle to multivehicle. So it's multidimensional. That's one of the unique pieces of this project."

The project will utilize one of Purdue's unrivaled assets, the UAS Research and Test Facility. The 20,000-square-foot, 35-feet high facility, located at Hangar 4 of the Purdue University Airport, features the largest indoor motion capture system in the world and offers unique capabilities for novel research.

Goppert will build a mixed reality environment, combining a virtual reality urban environment with a scaled physical model of the city. The drones will fly and navigate the city, and the environment can be programmed to simulate a wide range of settings, including weather,

traffic and urban development, to test the drones' applicability and agility. The testing will be done with single vehicles as well as swarms, which could include 10 drones.
Hwang said he hasn't seen any research done using mixed reality to this scale. Neither has Goppert.
"Our unique capability is that we have such a large environment to do it," Goppert said. "Just running so many vehicles at once is going to be a challenge. In the past, several vehicles have been used. But if we're going to be running swarms where each vehicle needs a rendered virtual mixed reality image, that's going to be really computationally challenging. That's what we're pushing forward. "We thought we could try to bring it as close to real-life as possible to get as many of the bugs worked out before they actually deploy such a system. We can do it all in software, but there's an added advantage in bringing it closer to reality by making some of it actual robots."
Hwang and Xu will have a multitiered approach from the cybersecurity and robustness standpoint. Xu will investigate from the cyber perspective of security, encryption, authentication and peer-to-peer communications. Hwang will develop a mathematical model and use the control theoretical solution approach, assessing potential cyberattacks on the systems and working to design a controller in such a way that the system becomes more resilient to attacks.
"This project reflects exciting synergies between two areas of technical excellence at Purdue: aeronautics and astronautics, and cybersecurity," Xu said.
Ultimately, all of the research will be integrated and pieced together around the state-of-the-art test bed, which could happen toward the end of the second year of the three-year grant.

The Chemical and Biological Attack Threat of Commercial Unmanned Aircraft Systems

By LTC Claude A. Lambert, U.S. Army
Source: https://www.ausa.org/publications/chemical-and-biological-attack-threat-commercial-unmanned-aircraft-systems#.X4Chg3bPnMA.twitter

Sep 29 – In September 2013, at a political campaign rally in Dresden, Germany, a small unmanned aircraft system (UAS),[2] or "drone," flew within feet of German Chancellor Angela Merkel and Defense Minister Thomas de Maiziere, hovering briefly before crashing into the stage near Merkel's feet.[3] This harmless stunt by a political activist demonstrated that drones, especially those using autonomous navigation systems, could be stealthy, accurate and potentially deadly. Had this drone been armed with a chemical or biological warfare (CBW) agent, it may have incapacitated or killed this high-level delegation, garnering international attention and triggering profound concern regarding the government's inability to secure and defend vulnerable populations from any UAS capable of delivering CBW agents.
Recent Events
There have been other incidents involving commercial UAS and national security. In April 2015, a small UAS, possibly tainted with radioactive cesium, was discovered on the roof of the Japanese Prime Minister's office. The UAS was "carrying a camera and a bottle of unidentified liquid that bore a sticker with the universal symbol of radioactivity."[4] In January 2017, the Islamic State of Iraq and Syria (ISIS) started using commercial UAS to provide reconnaissance and targeting information against coalition forces[5] and began showing interest in conducting UAS-based CBW attacks.[6]
Some violent extremist organizations (VEO) are arming commercial UAS with small munitions to attack adversaries.[7] Likewise, UAS confrontations with military, law enforcement, pilots and citizens are increasing, as the Federal Aviation Administration (FAA) now receives over 100 adverse UAS reports each month.[8] These examples illustrate the intrusive, undetectable and potentially lethal nature of this emerging technology.[9]

This report briefly outlines the rapid development and proliferation of commercial UAS, their potential dual-use capability to deliver CBW agents and proposes recommendations on countering this likely persistent threat.

A commercial drone sprays pesticide on crops. Such drones are readily available and could be used as a delivery system for chemical or biological attacks.

Advancements in UAS: Agricultural Spraying Drones and CBW Delivery

UAS have been around for years, evolving primarily for military use: The Flying Bomb (1918); Target Practice (1935); Surveillance (1964–1969); and Hunter-Predator (2001–Present).[10] Countries around the world are adopting UAS technology for domestic uses. Currently, there are 86 nations

with UAS capabilities—both armed and unarmed.[11] The development and proliferation of UAS technology is driven by the commercial sector as drones become cheaper, lighter, easier to use and more sophisticated—penetrating nearly every sector of the economy.[12] Some fields benefiting from modern drone technology include: agriculture, construction, real estate, applied sciences, law enforcement, media, mining, private security, search and rescue and wildlife conservation.

The use of drones for agricultural crop spraying continues to increase, as do the available options for UAS platforms. In the 1990s, the Japanese developed one of the first UAS agricultural sprayers, the Yamaha R-50, and its successor, the Yamaha R-MAX, in response to demand for efficient, cost-effective aerial agricultural spraying.[13] Manned fixed-wing crop dusters had been in use in Japan for many years, but the small size of most Japanese farms meant that this method was inefficient and costly. The R-MAX allowed more precise small-scale spraying, at a lower cost and risk than manned aircraft.

People around the world are becoming more aware of how their food is grown; they want it to be cultivated with as few pesticides as possible, while at the same time, farms seek to maximize yields through efficiency and manageability in plant protection and fertilization. These factors contribute to the development of UAS agriculture technology that can apply precise pesticides, fertilizers and herbicides on agricultural land.

In addition to Japanese agriculture spraying UAS technology, **China is leading the field in commercial UAS**. In particular, China's Dà-Jiáng Innovations (DJI) is the market leader in easy-to-fly UAS.[14] DJI quadcopters have become the standard in commercial UAS technology, and its Agras MG-1S agriculture UAS model is no exception. The Agras MG-1S is an octocopter designed for precision variable rate application of liquid pesticides, fertilizers or herbicides. It carries up to 10kg of fluid and can cover 10 acres in a single flight—doing so approximately 60 times faster than manual spraying. Industry standard ceramic nozzles come pre-installed and can be changed out if necessary to accommodate different spraying requirements.[15] The Agras MG-1S was one of two models that the Spanish Military Emergency Unit (UME) trialed for disinfecting large outdoor areas and the exterior of vehicles in the global fight to contain the Coronavirus Disease (COVID-19) pandemic.[16] Thus, significant advancements in UAS agriculture technology should give the joint counter weapons of mass destruction (CWMD) community pause.

The 11th Armored Cavalry Regiment and the Threat Systems Management Office operate a swarm of 40 drones to test the rotational units' capabilities during the battle of Razish, National Training Center on 8 May 2019. U.S. Army photo by Private Second-Class James Newsome

Capability Gaps and Their Implications

The proliferation in the research and development of commercial UAS for agriculture applications demonstrate that this is now an accessible dual-use technology that can realistically deliver CBW agents. A UAS CBW delivery platform is a definite possibility, especially for developing nations or VEOs that may not have the economic or technical means to acquire or employ more advanced delivery systems.[17] Technology has progressed to the point that commercial UAS are now much more capable in terms of operability, reliability, accuracy and range/payload capability than they were just a few years ago. Drone swarm technology, defined by Zachary Kallenborn and Philipp C. Bleek as "multiple UAS capable of coordinating their actions to accomplish shared objectives," is likely to encourage CBW proliferation and to improve the capabilities of states that already possess these weapons.[18]

Drone swarms may also aid in counter-proliferation, prevention, detection and response to a CBW attack, but those applications appear less significant than offensive uses.[19] Thus, the utility and flexibility of UAS make it a potential force multiplier. **UAS increase survivability, make attribution difficult and can be used as standoff weapon systems by states, small groups or individuals seeking to impose costs on a larger or more technologically advanced adversary**. However, the low payload capabilities of a UAS may reduce the direct losses sustained from an attack, but the propaganda value associated with a UAS CBW attack may increase the indirect costs (e.g. psychological, economic or political effects) associated with their use.[20]

Recommendations

The UAS epitomizes the difficulties with rapidly advancing dual-use commercial technology. The prospect of a UAS being used as a potential CBW delivery platform raises concerns that require constant situational awareness, coordination between the defense and law enforcement communities and employment of mitigation technologies. The recommendations below provide a starting point in developing a multi-purpose, synergistic approach in countering a commercial UAS CBW threat.

Develop a National Counter UAS Strategy

The United States does not have a comprehensive counter UAS strategy that includes all elements of the U.S. Government. In 2016, the U.S. Army drafted a counter UAS strategy "to develop and provide a comprehensive set of capabilities that enable commanders to detect, identify and defeat UAS threats and enable strategic and tactical freedom of maneuver and action through all domains, including the electromagnetic spectrum."[21] In early January 2020, the Army was officially selected to serve as DoD's counter small unmanned aerial systems (C-sUAS) executive agent (EA).[22] The EA is chartered to find joint solutions to counter threats caused by small drones and to ensure that the services are not duplicating efforts.[23] One key deliverable that the joint C-sUAS office plans to complete by calendar year 2020 is a DoD counter-drone strategy. While this is a positive first step, it is likely that this strategy will be military-centric, will not address the spectrum of the CBW threat and will lack perspective on the specific capabilities and capacity that U.S. government agencies need to effectively counter any UAS armed with CBW. Thus, a national counter UAS strategy that understands and incorporates parallel counter UAS efforts across federal, state and local levels is key in developing an approach that can improve interoperability to defend and defeat a UAS CBW challenge, if one should arise.

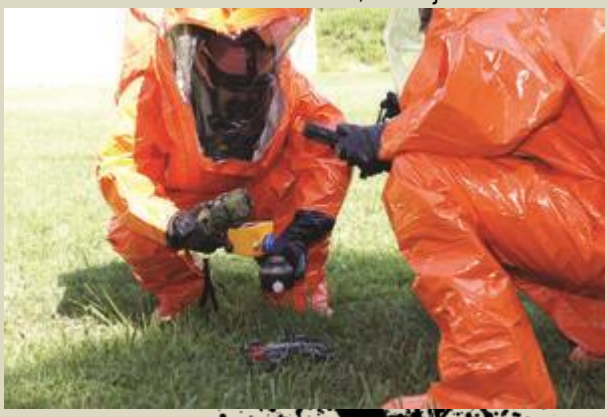
Soldiers from 5th Armored Brigade, First Army Division West, developed a course of instruction to counter the threat of commercial, off-the-shelf unmanned aerial surveillance vehicles at McGregor Range Complex, New Mexico, 28 June 2019. U.S. Army photo by Staff Sergeant Mylinda DuRousseau

Explore Layered Defense Technological Solutions

In recent years, vast resources have been deployed to identify, track and intercept any UAS deemed a threat, but "drones continue to provide a significant challenge to special event security in the U.S."[24] There is no "magic bullet" in countering a UAS CBW threat—no single comprehensive material solution will completely eliminate the UAS problem. **Thus, a "soft kill" to "hard kill" chain is needed to detect, identify and defeat UAS threats.**[25] Kinetic methods, signal hijacking, radio frequency interference and directed energy are areas that can be explored to defeat UAS in a practical, cost-efficient manner. In late July 2019, the U.S. Marine Corps used a new portable jammer system to jam an Iranian UAS in the Strait of Hormuz. The Light Marine Air Defense Integrated System (LMADIS) is a recent example of an effective counter UAS electronic jamming technology.[26] Lastly, the military, law enforcement and commercial security sector should burden share—work closely with commercial industry and partner with the science and technology community to research emerging technologies and capabilities that may address gaps for threat UAS capable of delivering CBW agents.

Update CWMD Exercise and Training Concepts to Incorporate UAS CBW Delivery

The U.S. Army Chemical Corps and the Functional Area 52 Nuclear and Counter-Proliferation Officer Branch, in conjunction with the joint CWMD community, should update their training concepts and scenarios to better prepare the joint force in countering and defending against a UAS CBW threat. The Army and the joint force minimized chemical, biological, radiological and nuclear (CBRN) training during the wars in Iraq and Afghanistan because U.S. adversaries lacked these weapons. Yet, as a result, the joint force now finds itself unprepared to confront a CBW threat.[27] **Commanders need to ensure that their formations understand how UAS-delivered CBW effects can affect personnel, equipment and the dynamics of combat power; they should train for and implement CBW survivability measures and techniques**. Additionally, updating lessons learned in countering ISIS's armed UAS tactics and techniques while incorporating the CBW delivery



dimension in training concepts and exercise scenarios will assist commanders in preparing their forces for this threat.[28]

Ensure a Sufficient Stockpile of Necessary CBRN Protective Equipment
Having enough CBRN protective equipment issued to the joint force and pre-positioned in the right locations is paramount when operating in a contaminated environment. Military units operating in a CBW environment require multiple sets of CBRN protective equipment to stay mission capable. Therefore, it is imperative that the Army's lead materiel integrator for CBRN protective equipment, the U.S. Army Tank-Automotive and Armaments Command (TACOM), ensure that sufficient amounts of CBRN protective equipment swing stock is built to prepare for the potentiality of a UAS CBW attack against the joint force.

Account for CBW-Capable UAS and Swarming Technology in the Missile Technology Control Regime (MTCR)
The U.S. State Department should evaluate whether and to what extent existing international treaties and multi-lateral control regimes are structured sufficiently to discourage proliferation of CBW-relevant UAS and swarming technology.[29] In particular, the State Department should advocate in the MTCR working group that CBW-capable UAS and swarming technology become export-controlled with export licenses on these technologies.

Fully Leverage World Customs Organization (WCO) Operations, Actions and Activities
The international community through the WCO should continue to fund international efforts to counter the diversion and trafficking of precursor chemicals used by VEOs and other criminal organizations for explosives development. The WCO should extend and expand *Programme Global Shield* (a law enforcement operation to combat the increasing illicit use of precursor chemicals to manufacture improvised explosive devices) to add specific Toxic Industrial Chemicals/Materials (TIC/TIM) and critical dual-use CBW components to their monitoring and reporting database.[30] Additionally, as part of the Strategic Trade Controls Enforcement Project (STCEP), it should fund and re-establish *Operation Cosmo* to focus industry and international efforts to disrupt the diversion of licit Chemical Warfare Agent precursors and dual-use components into illicit channels during importation, production, storage, transportation and sale.[31]

Conclusion
Although current commercial UAS technologies are sufficiently threatening, the industry is continuing to advance at a rapid pace that could potentially make these applications exponentially more deadly.[32] It is nearly assured that UAS will become smaller, cheaper and more capable as technology evolves. A UAS capable of delivering CBW agents makes the technology particularly difficult to defend against. One thing is for certain: **anyone willing to develop or acquire a CBW agent and deliver it via a UAS will likely not be able to be deterred**. Therefore, a comprehensive strategy that can be operationalized in conjunction with cost-effective counter UAS technologies and capabilities is critical in defending against and defeating this emerging threat.

★ ★ ★ ★

This paper was the winner of the 2019 Army Strategist Association Writing Contest administered by the Association of the United States Army.

Lieutenant Colonel Claude A. Lambert *is a Strategic Planner at U.S. Army Materiel Command. He holds an MS in technology intelligence with a weapons of mass destruction concentration from National Intelligence University and an MS in peace operations policy from George Mason University. The views expressed in this article are those of the author and do not necessarily reflect the official policy or position of U.S. Army Materiel Command, the U.S. Army or the Department of Defense.*

Drone-jamming gun claimed to be one of the smallest and lightest

Source: https://newatlas.com/drones/e1000mp-drone-jamming-gun/

Oct 09 – For people such as soldiers, security officials and airport workers, drones aren't always a welcome sight. That's why drone-jamming guns were developed, and the new Paladyne E1000MP "pistol" is said to be one of the most compact on the market. Manufactured by **British company** Drone Defence, the E1000MP works in the same fashion as similar products – it emits an electromagnetic signal at the same frequency that a target drone utilizes for control communications, GPS orientation, and video transmission. This causes the drone to lose communication with its operator, resulting in it automatically landing or returning to its point of take-off.

The gun has an operational range of 1 km (0.6 miles), and can be used with either a directional or omnidirectional antenna – the former focuses the jamming signal on one particular drone, while the latter spreads the signal out over a wider area that needs protecting.
It's reportedly even possible for users to gain control of the

frequencies used by the aircraft. This means that they could manually activate its return-to-home function, allowing them to locate its operator by watching where it lands.

The Paladyne E1000MP can be mounted on third-party rifles – Drone Defense

The Paladyne E1000MP is IP56 waterproof (it can withstand high-pressure jets of water), runs for two hours per four-hour charge of its battery, and works at ambient temperatures ranging from -20° C to 60° C (-4° F to 140° F).
It has a claimed weight of 3.5 kg (7.7 lb), which presumably includes both the gun itself and its accompanying control box. While this does indeed put it at the lightweight end of the spectrum, DroneShield's DroneGun MkIII actually comes in significantly lighter, at 1.95 kg (4.3 lb).

A new weapon complicates an old war in Nagorno-Karabakh

By Nabih Bulos
Source: https://www.latimes.com/world-nation/story/2020-10-15/drones-complicates-war-armenia-azerbaijan-nagorno-karabakh

Oct 15 – Huddled together in the basement of the town's music school, the women broke into a chorus of bee-like buzzing sounds to describe what has become their greatest fear.
"We don't see them," said Katarina Abrahamyan, a 38-year-old supermarket cashier. "We hear them."
The "them" she was referring to were drones, a frightening new fixture in the military conflict between Armenia and Azerbaijan that erupted in late September after several years of relative calm. Hundreds have now died in more than two weeks of ferocious clashes over Nagorno-Karabakh, the ethnic Armenian enclave internationally recognized as belonging to Azerbaijan but ruled by an Armenia-backed separatist government.
The drones have turned the hostilities from a bloody, bare-knuckled ground fight waged with infantry and Soviet-era ordnance into a deadly game of hide-and-seek against an all-too-patient — and often unseen — airborne enemy.
"If we can see it with the eye, we shoot at it. If not, we hide," said Ashot Sarkissian, a 51-year-old artillery operator keeping vigil in the town of Askeran, just north of Stepanakert, the capital of Nagorno-Karabakh.
"We need new technology. We need new weapons to fight the drones."
The onslaught from above, which since Sept. 27 has killed five civilians and injured 10 others here in Martuni, a town about 20 miles east of Stepanakert, marks a new and dangerous escalation in the conflict, said Edik Avanesyan, the mayor and a veteran of previous face-offs with Azerbaijani forces.
"The intensity is incomparably higher. Most of these drones are for reconnaissance, and then come the strikes," he said, adding that so far more than 120 residential and administrative buildings in the town have been damaged, along with 40 cars.
"There are days when they don't come, but when they do it's three or four times a day."

Ashot Sarkissian, a 51-year-old artillery operator, examines the remnants of an Azerbaijan drone that crashed into the hillside in Askeran, Nagorno-Karabakh (Marcus Yam / Los Angeles Times).

The drone strikes, along with artillery salvos, forced Avanesyan to order an evacuation of most of Martuni's 6,200 residents, with most women and children seeking refuge outside the town while some of the men stay behind.

The conflict over Nagorno-Karabakh, which ethnic Armenians call Artsakh, dates to World War I, but escalated in the waning days of the Soviet Union. In 1988, ethnic Armenians who formed the majority of the territory's inhabitants sought to secede from Azerbaijan, a Soviet republic; skirmishes between Armenians and Azerbaijanis metastasized into all-out war as the U.S.S.R. collapsed in 1991.

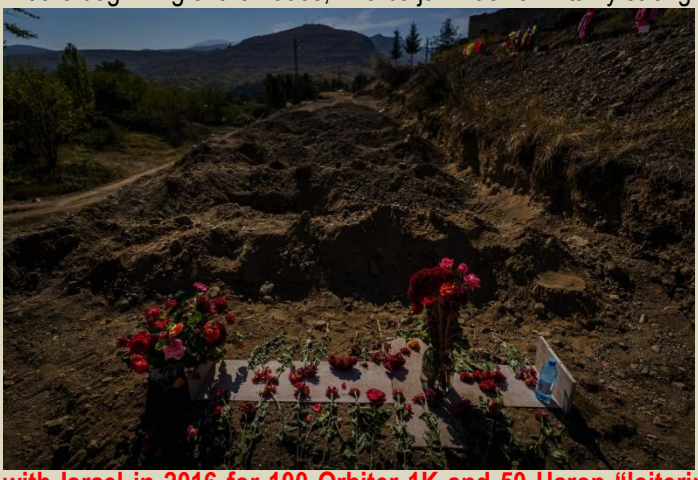
Three years later, after an estimated 30,000 people were killed in fighting and in pogroms targeting Armenians and Azerbaijanis, a cease-fire was called, leaving Armenians in control of Nagorno-Karabakh, along with a number of other provinces amounting to almost 9% of Azerbaijan's territory. More than 1 million people, mostly on the Azerbaijani side, remain displaced from their homes, while Nagorno-Karabakh has taken on a totemic significance for both sides.

A large Azerbaijan missile is embedded in the ground outside Martuni, Nagorno-Karabakh (Marcus Yam / Los Angeles Times).

Drones have upended the calculus undergirding that status quo — especially for Azerbaijan, which has used its oil wealth to dramatically upgrade its arsenal, said Rob Lee, a defense expert in the war studies department at King's College London.

Azerbaijan has vowed to reclaim the mountainous, Delaware-sized territory and launched several offensives over the years. Russia, France and the U.S. — which co-chair the Minsk Group, an 11-country coalition tasked with resolving the so-called frozen conflict — have failed to push the parties toward a final settlement.

"At the beginning of the 2000s, Azerbaijan wasn't militarily strong enough to retake Nagorno-Karabakh," Lee said. "But after a sharp rise in global oil prices and a decade of increased defense spending, including tens of billions of dollars spent on Russian, Israeli and other foreign high-tech arms, the military balance of power shifted by 2016."



Flowers adorn the grave of a fallen service member at a military cemetery in Stepanakert, Nagorno-Karabakh. New graves have been dug next to it in preparation for more burials (Marcus Yam / Los Angeles Times).

Between 2011 and 2019, according to the Stockholm International Peace Research Institute, which maintains a database on global arms expenditure, Azerbaijan spent more than $19 billion on weapons. That included **a $5-billion order with Israel in 2016 for 100 Orbiter 1K and 50 Harop "loitering munitions," or so-called kamikaze drones that can target antiaircraft defense and radar systems. (The Harop appears to have first been deployed by Azerbaijan's military in 2016 in a strike against a bus full of Armenian soldiers.)**

Armenia has spent about $4.8 billion on its arsenal over the same period, and its reliance on Russia as its main weapons supplier means that its unmanned aerial vehicle, or UAV,

capabilities are relatively lacking, because Moscow has not focused its defense development on drones, Lee said. Instead, Armenia has only a small number of domestic UAVs it has employed on the battlefield.

Harop (left) and Orbiter 1K (below) drones

In a nationwide address Friday from the Azerbaijani capital, Baku, President Ilham Aliyev celebrated the shift in his country's war-making abilities.

"Mediators and leaders of some international organizations have stated that there is no military solution to the conflict," Aliyev said. "I have disagreed with the thesis, and I have been right. The conflict is now being settled by military means, and political means will come next."

Bayraktar TB2

A new addition to Baku's arsenal is the Bayraktar TB2, a drone purchased from longtime ally and North Atlantic Treaty Organization member Turkey sometime after June, according to statements given by Azerbaijan's defense minister to local media. The TB2 has become the favored weapon in the skies for Azerbaijan's military, overshadowing even the Turkish F-16 warplanes stationed in the Azerbaijani city of Ganja during joint military exercises between Turkey and Azerbaijan.

Aliyev denied that the F-16s have been used in combat against Armenian forces. He instead credited Turkish drones with reducing Azerbaijan's military casualties in the current flare-up. The TB2 has a flight time of 24 hours and a communication range of almost 100 miles, according to the Turkish government, and comes armed with smart munitions.

"These drones show Turkey's strength," Aliyev said. "It also empowers us."

In recent weeks, the TB2 has made a regular appearance in videos released by Azerbaijan's Defense Ministry, with feeds from the drone's high-definition camera (often set to strains of dramatic classical music) demonstrating the drone's destructive power against older Armenian materiel.

Open-source analysis of such videos indicates that the drones have exacted a devastating toll, disabling some 87 tanks and more than a dozen surface-to-air missile systems. The same analysis shows that Azerbaijan has lost at least 15 UAVs in the fighting.

With the threat of drones omnipresent, officials, army personnel and even civilians have had to alter habits.

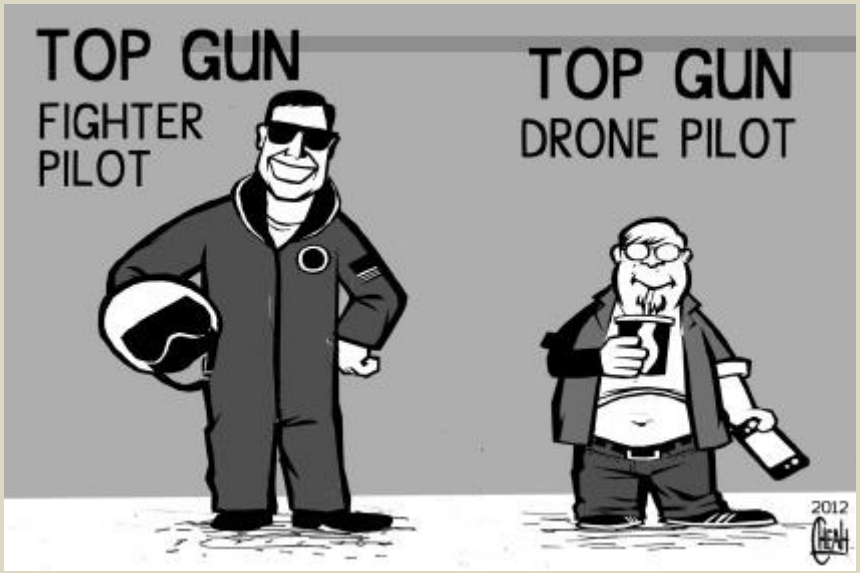
In Martuni (which Azerbaijanis call Khojavend), Avanesyan, the mayor, eschews what he considers a less secure but more modern smartphone in favor of a primitive Nokia, which would reveal less information to an adversary. Similarly, soldiers near the front line are proscribed from using GPS or taking any photos with their phones. Drivers tape up headlights or smear mud on their cars to obscure any markings that could make them a target. Gatherings are discouraged, with people urged not to spend too much time in one place and to designate an emergency shelter.

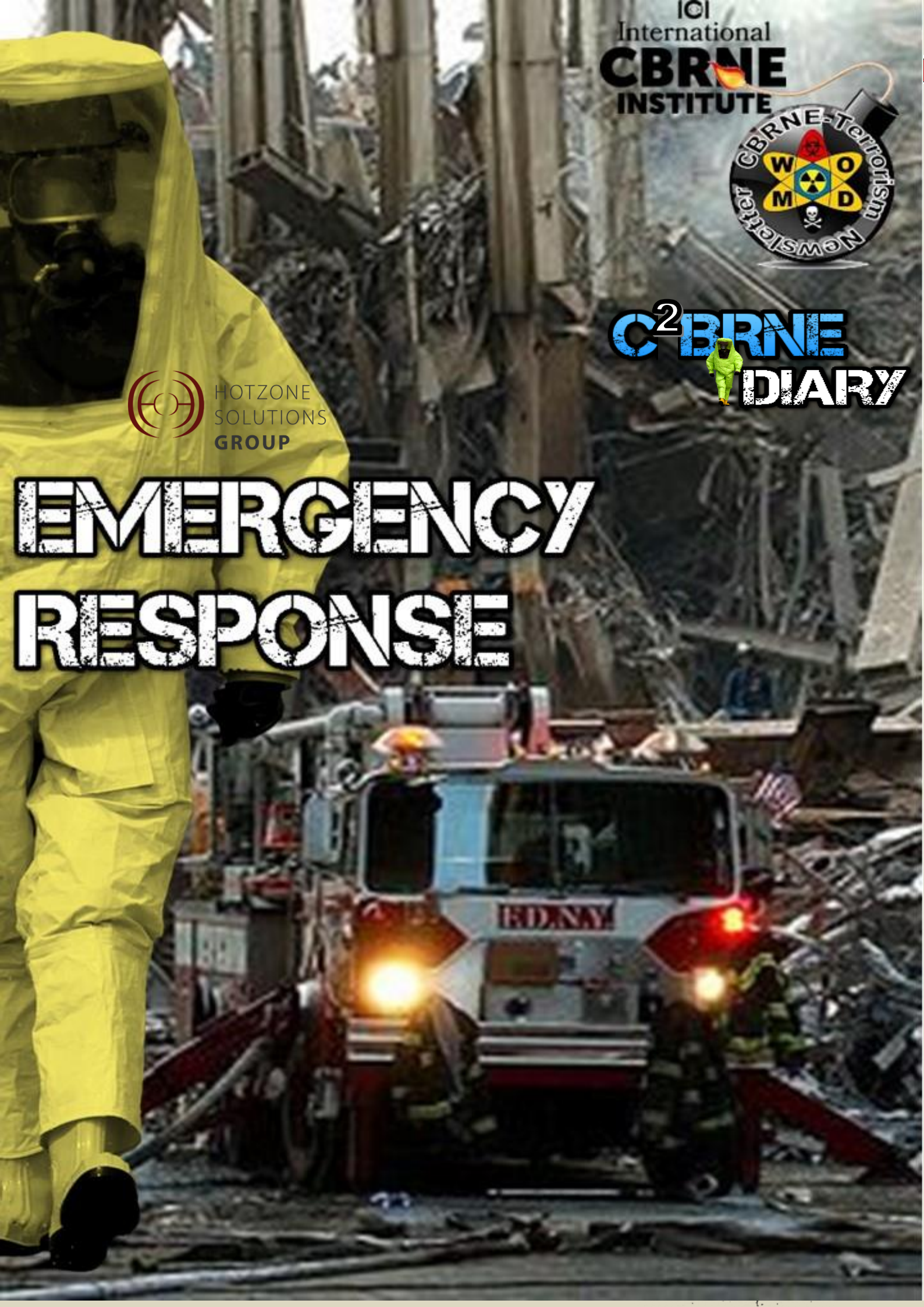
"We can't stay for long," said Seyran Danielyan, 63, Martuni's urban planner, urging a visiting journalist to hurry during a tour of the town. "We don't know when they're going to hit."

Inside the music school, Leonard Hovanissian, a 61-year-old accordion player, sat in the basement near a dusty stack of *qanuns*, traditional stringed instruments, waiting for the bombing that usually followed the sound of drones overhead.
"We hear the buzzing and we quickly go inside," he said.
"We're afraid, and then the sirens begin. It's as if we're in the Second World War."

Nabih Bulos *is the Middle East bureau chief for the Los Angeles Times. Since 2012, he has covered the aftermath of the "Arab Spring" revolution as well as the Islamic State's resurgence and the campaign to defeat it. His work has taken him to Syria, Iraq, Libya, Turkey, Lebanon, Jordan and Yemen as well as on the migrant trail through the Balkans and northern Europe. A Fulbright scholar, Bulos is also a concert violinist who has performed with Daniel Barenboim, Valeri Gergyev and Bono.*

Times staff photographer ***Marcus Yam*** *in Askeran contributed to this report.*




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

Pharmacy disaster preparedness 'poor to moderate'

Source: https://ajp.com.au/news/pharmacy-disaster-preparedness-poor-to-moderate/

Oct 01 – Researchers from the School of Clinical Sciences at the Queensland University of Technology have conducted a systematic literature review to explore pharmacists' and pharmacy students' preparedness for disasters.

Disasters are increasing in intensity and frequency around the world, said researchers Elizabeth McCourt, Judith Singleton, Vivienne Tippett and Lisa Nissen.

"The 2019–2020 bushfire disaster in Australia, and the global COVID-19 pandemic have highlighted the importance of health professionals being prepared for disasters," they said.

"In order to prevent disruptions to the essential services provided by pharmacists during disasters, it is important that pharmacists across all practice settings are prepared."

Following an extensive literature search, only four articles met inclusion criteria and exceeded the quality threshold. Three articles focused on pharmacy students' preparedness for disasters, and one was on registered pharmacists' preparedness.

In the first study, published in 2016, second-year pharmacy students were divided into groups during a workshop and responded to one of three hypothetical infectious disease scenarios—anthrax, pandemic influenza and smallpox. Before the workshop, students had a mean preparedness score of 3.3, on a Likert scale from 0 (*unprepared*) to 10 (*prepared*). After the workshop this score increased to 4.1.

The second study from 2010 examined the preparedness of multiple health professions to respond to a bioterrorism event using a survey. Participants were required to self-assess their competence. The final model found that 82.6% (n = 360 out of 436) of pharmacist participants included in the survey were not prepared for a bioterrorism attack. "Pharmacists seemed to be less prepared than physicians and nurses," the original authors concluded.

Two further studies, both published in March 2020, examined the preparedness of multiple health professional students. Participants were required to self-assess their perceived knowledge, attitude and readiness to practise.

The survey covered three components: knowledge of disasters and disaster medicine (K); attitude towards disasters and disaster medicine (A), and; readiness to practise in a disaster (rP). Pharmacy students in the first study scored a mean KArP score of 90 out of a potential 157 points (57%), while those in the second study scored a mean KArP score of 101 out of a potential 157 points (64%).

"Despite repeated calls for improved preparedness, there is little literature examining the pharmacy professions' preparedness and the literature that does exist is methodologically limited," the QUT research team found.

They said that while the pharmacy professions' preparedness appears to be low, the factors that may influence preparedness may include:

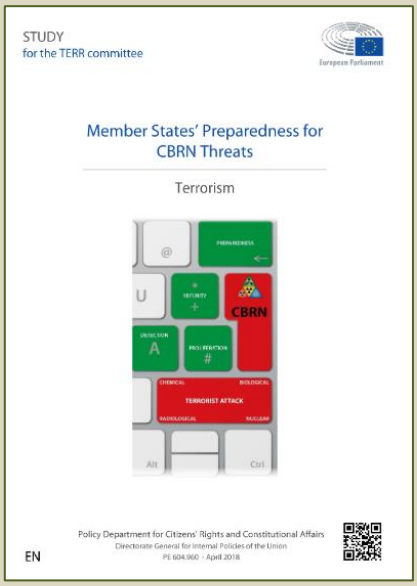
1. **Disaster preparedness interventions** – through education, training and drills. The 2010 study determined that previous involvement in disaster training (P< 0.001) and disaster drills (P < 0.001) were significant predictors of overall preparedness. If a health professional had participated in previous drills or training, they were 2.56 and 2.86 times more likely to be prepared for a bioterrorism attack respectively.
2. **Clinical and administrative competency** – The studies also found that preparedness is directly correlated with perceived competency to fulfil roles in a bioterrorist event. Perceived competency may impact an individual pharmacists' disaster preparedness.
3. **Willingness to respond** – In one of the studies, participants' willingness to respond was reported by the size of the bioterrorist incident (local, regional, state-wide or nation-wide impacts), and the perceived risk of the event (high or low risk). When compared to physicians and nurses, pharmacists were the least likely health professional to respond to a bioterrorist event. The proportion of pharmacists that were willing to respond to bioterrorist events varied between 44.5% for a low risk and nation-wide event, to 80.7% for a low risk and local event.
4. **Demographic factors –** Modelling in the 2010 paper found that gender (p = 0.042), city type (p = 0.020), current position (p = 0.033) and primary workplace type (p = 0.005) were significant predictors of overall preparedness. Pharmacists were significantly less prepared for bioterrorist attacks when compared with nurses and physicians (p < 0.001). Approximately 35% of the physician and nurse workforce surveyed were prepared for a disaster compared with **<18% of pharmacists.**

More robust research is needed, the researchers concluded. "For pharmacists, the lack of research around their preparedness speaks volumes about their current involvement and expectations within disaster management."
Small sample sizes in the review, as well as the diversity in research methodology, made it difficult to draw robust conclusions about the differences in pharmacist and pharmacy student preparedness, they added.
"However, the consistency in poor preparedness across pharmacy students and pharmacists could indicate gaps in preparedness supports for both these groups," they said. "Whilst health professionals such as physicians and nurses may have access to disaster education, training, or drills, there appears to be a lack of these interventions targeted at the pharmacy profession."

▶▶ **The study was published in the** *International Journal of Pharmacy Practice*

Member States' preparedness for CBRN threats

EU publications
Source: https://op.europa.eu/en/publication-detail/-/publication/3357f853-5efd-11e8-ab9c-01aa75ed71a1/language-en



This study, commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the Special Committee on Terrorism outlines the threats posed by Chemical, Biological, Radiological and Nuclear (CBRN) weapons, examines how well Europe is prepared for these threats and assesses where preparedness and response could be improved. It suggests that to date, terrorist attacks in Europe have largely utilised conventional weapons where medical staff are able to respond using conventional medicine and medical practices.

However, threats from the use of CBRN materials for terrorism remain high and evolving. The future threats are likely to come from the use of chemical and biological weapons.

Watch: Original Vehicle for Rapid First Response

Source: https://i-hls.com/archives/104258

Oct 01 – A test flight in the heart of the UK's Lakes District has pushed the boundaries of emergency response, demonstrating the huge potential of utilizing Jet Suits to deliver critical care services. First responders might soon be able to wear jet suits and fly to help and rescue survivors.
The development is the result of a collaboration between Gravity Industries, which has developed and patented a **1,050-brake horsepower Jet Suit**, and the Great North Air Ambulance Service (GNAAS) in the UK.
The Lake District, the UK's most famous national park, includes areas with wild terrain, a fact that resulted in several incidents requiring the medical expertise of the GNAAS critical care team. The undulating peaks and valleys can often mean the helicopter is unable to safely land close to the casualty, forcing travel by vehicle or foot.
During the test flight, Gravity Industries founder and Chief Test Pilot Richard Browning flew from the valley bottom to a simulated casualty site. The simulated casualty site would take around 25 minutes to reach by foot.
The Gravity Jet Suit is able to cover that distance in 90 seconds, opening a range of possibilities in the emergency response arena, according to uasvision.com.
With the test complete, GNAAS and Gravity Industries are now exploring the next steps in this collaboration.

Building Pandemic Preparedness and Resilience to Confront Future Pandemics

By Sally Huang

Source: http://www.homelandsecuritynewswire.com/dr20201001-building-pandemic-preparedness-and-resilience-to-confront-future-pandemics

Oct 01 – With the current COVID-19 pandemic revealing major gaps in national readiness, the Bipartisan Commission on Biodefense brought together members of the legislative and scientific community for a virtual discussion on the need to increase and optimize resource investments to promote changes in US policy and strengthen national pandemic preparedness and response. Even as the nation continues to respond to the COVID-19 crisis, the various panelists unanimously acknowledged that the world will most likely face future pandemics. After having adapted to telework, decisionmakers are determined to enhance and enact new policies and guidelines to better position the nation to effectively respond to future infectious disease threats. Areas requiring the nation's attention were addressed in three separate panel discussions; emerging biological threats and innovative technology for biodefense, emerging biological risks, and the future of biodefense. The recording of the virtual discussion held by the Commission, "The Biological Event Horizon: No Return or Total Resilience," can be found here.

Representatives Susan Brooks (R-IN) and Diana DeGette (D-CO) discussed the responsibility the US has to its people to take advantage of lessons learned so far from the COVID-19 pandemic to integrate into pandemic preparedness and response policies. After all, as much as governments monitor indicators of possible biological attack, there is no set method to predict or foretell events of Mother Nature, "the world's worst bioterrorist" and how it may further increase infectious disease threats. The US, operating from a privileged position as a world power, had a heightened belief of preparedness partly brought on by availability of advanced biotechnologies, but quickly realized the scope of their unpreparedness as private and public sectors were overwhelmed. The shock that resulted from COVID-19 demonstrates that the government not only has to invest meaningfully in CBRN programs, but also speaks to the need to translate scientific research into solutions in order to be well-equipped. For example, expanding and improving management of the Strategic National Stockpile and establishing a national forecasting system of infectious diseases analogous to the National Weather Service. This also includes revamping trainings and imparting institutions with flexible working styles in recognition that teleworking and digital platforms are transforming the working landscape.

This is much needed for government institutions as COVID-19 caused a significant interruption in government operations and its ability to provide services to the people. More importantly, with the November election approaching, the nation requires clear leadership from the White House during this critical time to steer pandemic and biodefense progress in the right direction.

These policy additions and enhancements are also backed by advice given by experts, including Jaime Yassif, PhD, Sohini Ramachandran, PhD, and Nita Madhav, MSPH, about emerging biological risks. There is an evident need to close the gap between science and policy to enrich pandemic preparedness and foster a culture of cooperation, coordination, and resilience. As the panelists mention, numbers of infectious diseases will increase over time, meaning that complex contagion will inevitably become a reality the US and international community have to battle with. Thus, this further highlights the urgent need to fund interdisciplinary research to enhance analytical tools for infectious disease modeling and sheds light on the national forecasting suggestion brought up by the first set of panelists to better coordinate infectious disease analytics and information more efficiently. Proactive preparedness will help ensure proactive and effective reaction.

That being said, all the more reason to pay attention and invest strategically in the future of biodefense. Private and public sectors need to be effectively incorporated into a national strategy in order to improve foundational capabilities and compensate for the noticeable gaps during the COVID-19 pandemic. This includes enhancing and providing support to the supply chain, a critical building block for addressing America's material needs. Additionally, analytic and scientific models should account for modern globalization trends and climate change effects to heighten awareness and response. The recent wildfires spreading across California, Oregon, and Washington serve as an example where unpredictable events have the potential to set up ideal conditions for further disease transmission. Not to mention, natural events cause ecological shifts that also contribute to a changed infectious disease landscape. Decisionmakers have no doubt that this feat will require a strong united front to address these concerns.

The recommendations raised during this virtual discussion led to congressional members underscoring the significance of the **Apollo Project for Biodefense**. Noted as a vital step to building the nation's resilience, this initiative will examine the nation's track record of dealing with infectious diseases, and assess how to better invest and coordinate science and technology efforts and innovation. Extending the ambitions, values, and characteristics of the original Apollo mission,—with the goal of landing the first humans on the moon, to the

current COVID-19 pandemic—the legislative and scientific community are hopeful that the bipartisan Apollo Project for Biodefense will champion public and private sector partnership, and galvanize public support to achieve prevention and mitigation of infectious disease threats. Legislative and scientific communities are optimistic that this initiative will push the country in the right direction to better understand, prepare for, and anticipate future pandemics.

This three-paneled virtual discussion echoes the notion that positive policy change in the realm of infectious diseases is a dynamic and all-inclusive process in which various sectors have to participate and cooperate, and integrate expert advice with legislative detail to properly enact long-term change. Even from a virtual distance, it is clear that members of the legislative and scientific community are ready to take collaborative action to ensure that the world doesn't come to another standstill in the face of future pandemics. As the country continues to struggle and recover from the COVID-19 pandemic, the right policies governed by suitable leadership will determine a nation's future plan, response, and resilience towards infectious diseases. While the Apollo Project for Biodefense emphasizes a united and hopeful front, the panelists are aware that a great deal of coordination is still required before strategies can be translated into action. There will have to be steadfast commitment from various sectors and stakeholders in order to foster preparedness, resilience, and response during this opportune window of time.

Sally Huang *is Biodefense Ph.D. Student at Georgetown University.*

Source: https://cip-association.org/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.

This Emergency Response Tech May Just Save Your Life in a Shooting

By Naama Barak

Source: http://www.homelandsecuritynewswire.com/dr20201013-this-emergency-response-tech-may-just-save-your-life-in-a-shooting

Oct 13 – The terror attack at the Sarona Market in Tel Aviv in June 2016 was followed only a few days later by the deadly shooting at the Pulse nightclub in Orlando, Florida. The sequence of events got Yoni Sherizen thinking about the vulnerability of soft targets. "These two incidents got me looking at a question of unfortunately not if, but when, they would happen again," he says.

Originally from the US, Sherizen moved to Israel from the UK in 2009. When the two attacks took place, he was transitioning from the field of education and welfare into the tech world and was looking for opportunities that would not only deliver a profit but also add value.

Such an opportunity arose as he and his partners developed Gabriel, an emergency-response system that can be installed in schools, places of worship, workplaces and elsewhere to help save lives in cases of shootings and other attacks.

"The solution has three components," he explains. "No. 1, we have a physical device that we stick inside the buildings. It looks like a cousin of the fire alarm – **a round, blue bell to press in case of emergency**.

"It looks to the average person like a smart panic button but it's actually more than that," he says, explaining that the button enables two-way communication and can sense its environment.

"Those first few seconds and first few minutes are really the difference between life and death for many people," he says. "We're all about stopping that chaos from occurring."

Recently, Gabriel added a gunshot detection feature, which sets off an alert even before someone presses a button. The sensors pinpoint the location of the shooting, enabling first responders to go directly to the scene.

"We're very quickly able to get situation awareness and take control of the situation," Sherizen notes.

"No. 2, we leverage all the smartphones as critical tools both to report and get information out to people and have real-time two-way communication," he says. "No. 3 is a very simple, easy-to-use dashboard."

This dashboard, Sherizen adds, allows those at the site and first responders to take charge of the situation and share it in realtime with emergency personnel so that everyone has the same information for decision-making.

"Most people think that once you've alerted police, once that call for help has gone out, you're okay," he notes. "It takes several minutes for the response to even arrive at the front door. Those tools give the onsite team the ability to very quickly take control of the situation."

A Guardian Angel

While developing Gabriel, Sherizen and his team tried to find a device already in the market that they could use as part of their system. They found nothing.

"We researched endless interviews with people, everyone from survivors of attacks to schoolteachers and principals to security experts to police officers, federal agents, special forces across multiple countries," he says. "We spoke to as many people as we could, and we continue to speak to as many people as possible."

Gabriel has so far been deployed by some Jewish community institutions in the States, but Sherizen has more global plans for the unique technology.

"We chose the name Gabriel because it's a concept that crosses all religions, cultures, languages – the idea of a protective angel that's there waiting to protect you," he notes.

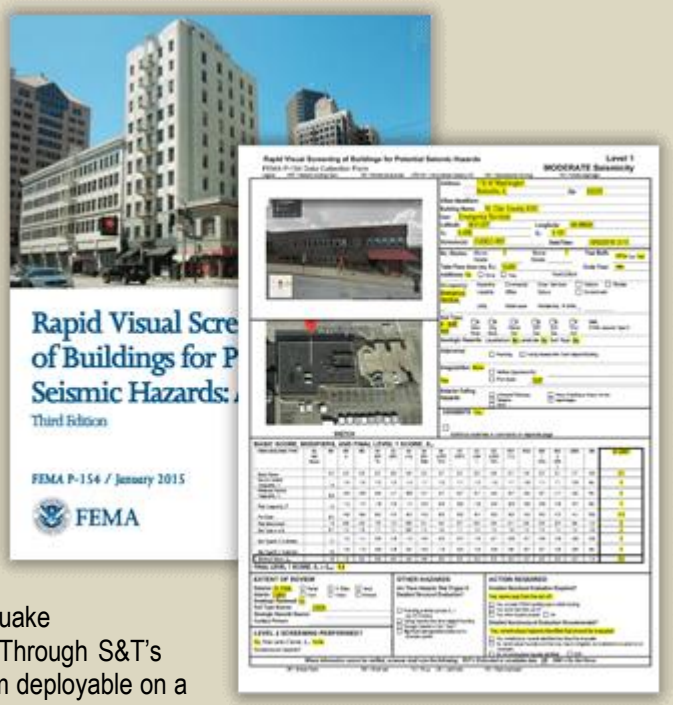
"We started with the Jewish community because they had a very real and immediate need and they understood the need for the product," he says. "We're already expanding beyond that. We're in talks with corporations for workplace violence and potential threats that arise in a corporate environment."
Wherever the device may be installed, Sherizen notes the importance of preparing for any kind of attack.
"I would say one thing is the importance of being prepared, of running drills and creating muscle memory," he notes. "We've built the system in order for people to become educated and drill and practice."
"We've created a system that intentionally creates best practices and helps people become prepared without the trauma," he says.
"You never really know who you are and how you are going to respond until you are under that pressure," he explains. "We also need to take into account the fact that there are people who are just going to be freaked out."
"We see this as a global issue," he concludes. "Every building that has a fire alarm today needs a Gabriel device and that's the vision we have here today."

***Naama Barak** is a writer at ISRAEL21c.*

Disaster Preparedness in the Palm of Your Hand

Source: http://www.homelandsecuritynewswire.com/dr20201021-disaster-preparedness-in-the-palm-of-your-hand

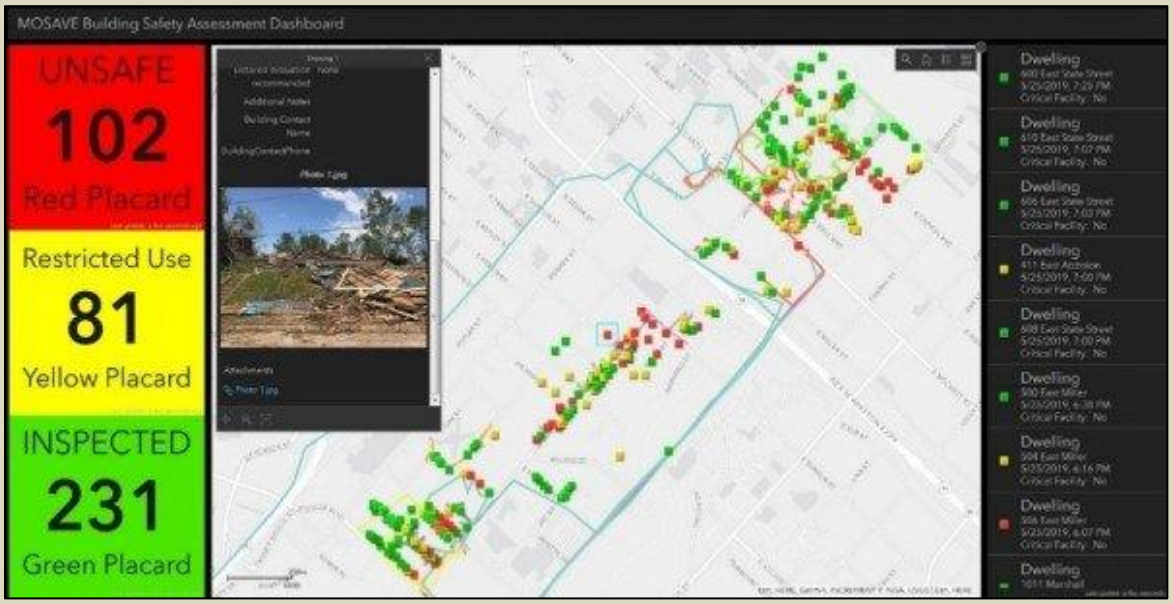
Oct 21 – Natural disasters like tornadoes and earthquakes can devastate communities and bring uncertainty in their aftermath when it comes to safely accessing buildings or homes. When an EF-3 tornado struck Jefferson City, Missouri, in May 2019, it killed three people and left over 600 buildings damaged, presenting first responders with an overwhelming response challenge. In tragic situations like this, facility owners and emergency planners play a key role in taking swift action to evaluate the damage done.
"Prior to the chaos of a disaster, it's imperative that emergency planners and building owners understand the status of their communities' facilities," said Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Program Manager Ron Langhelm. "Post-disaster, they need to have tools that can give them a clear picture of the damage, so they know how to address it."
This year, during National Preparedness Month in September, S&T highlighted several technologies designed to help with disaster preparation, response, and recovery efforts. But the conversation shouldn't end just because September did. We're going to continue on sharing resources, some of which fit right in the palm of your hand.
"This is a great opportunity to continue thinking about how your community is planning for the future and whether you have the necessary tools to respond," said Langhelm. "Through joint investments, S&T has been able to deploy preparedness and response tools to many localities for front-line use. Our hope, along with that of our partners, is that communities use and help us improve these tools."
For instance, Langhelm has led S&T's efforts to work with the Central United States Earthquake Consortium (CUSEC) to enhance **two GIS-based apps used for pre- and post-disaster assessment:** the Rapid Visual Screening (RVS) and Building Safety Assessment (BSA) apps. These tools adapted paper processes into a mobile format to deliver data quickly and easily to a wide array of stakeholders who need access in advance or in the wake of a disaster. CUSEC developed early iterations of the BSA and RVS apps with funding from FEMA's National Earthquake Hazards Reduction Program (NEHRP) and the Delta Regional Authority. Through S&T's support, CUSEC was able to significantly enhance the apps and make them deployable on a national scale. Both of the apps are free and available for use via the S&T-supported Regional Information Sharing Platform.



Assessing Vulnerable Facilities Before a Disaster
Part of S&T's partnership with CUSEC is to better equip the Central U.S. with decision-support technology that can be applied to earthquakes and other hazards, and the RVS

app directly supports these efforts. This region has a 25 percent to 40 percent probability that a magnitude 6.0 or greater earthquake could occur within any 50-year time period, making preparation paramount.

The RVS app helps screen buildings vulnerable to direct earthquake-induced damage prior to an event. Its data collection, visualization and reporting capabilities are adapted from FEMA's *P-154 Rapid Visual Screening of Buildings for Potential Seismic Hazards* (3rd ed.) (PDF, 388 pgs., 50 KB) methodology. FEMA's P-154 was first published in 1988 and has seen several updates that incorporate the evolving knowledge concerning seismic hazards and building structures, as well as new field data collection and reporting technologies.



"Together, FEMA, S&T and CUSEC have been able to modernize an existing methodology to improve mitigation efforts," said Langhelm. "By using the RVS app, building owners and emergency planners streamline the FEMA P-154 paper process, and can create a database of potentially vulnerable structures."

The RVS app uses commercially-available technologies from the Environmental Systems Research Institute (Esri). Information in the database can be viewed and edited using a built-in operations dashboard or can be displayed in a FEMA P-154 standard report format using the RVS app reporting tool. Data collected using the RVS app can also be exported to a spreadsheet or to FEMA's HAZUS loss estimation software.

Following a local assessment of buildings or facilities, the results can be used to identify and prioritize opportunities for mitigation efforts. Communities have already begun putting it into use. For example, the Northeast States Emergency Consortium used the app to screen critical facilities in Maine for potential vulnerabilities, and in 2021, Kentucky and Tennessee also will use the app to screen critical facilities. The Missouri Seismic Safety Commission has begun using the RVS app to conduct rapid visual screenings of schools as part of their initiative to improve earthquake safety.

BSA App Used After 2019 Missouri Tornadoes

The days following a disaster can be devastating for communities and can have lasting impacts on its economy and well-being. After the tornado in Jefferson City, the Missouri State Emergency Management Agency authorized the Missouri Structural Assessment and Visual Evaluation (MOSAVE) Coalition to assess homes in the affected area for safe occupancy.

The BSA app, developed in 2018, was deployed for use. Designed to speed data collection, the MOSAVE assessment teams, comprised of architects, engineers, and building construction professionals, used the app to conduct structural assessments to document the conditions observed within the affected area.

"This was the best data collection method I've used in all my deployments," said Michael Ash, MOSAVE member.

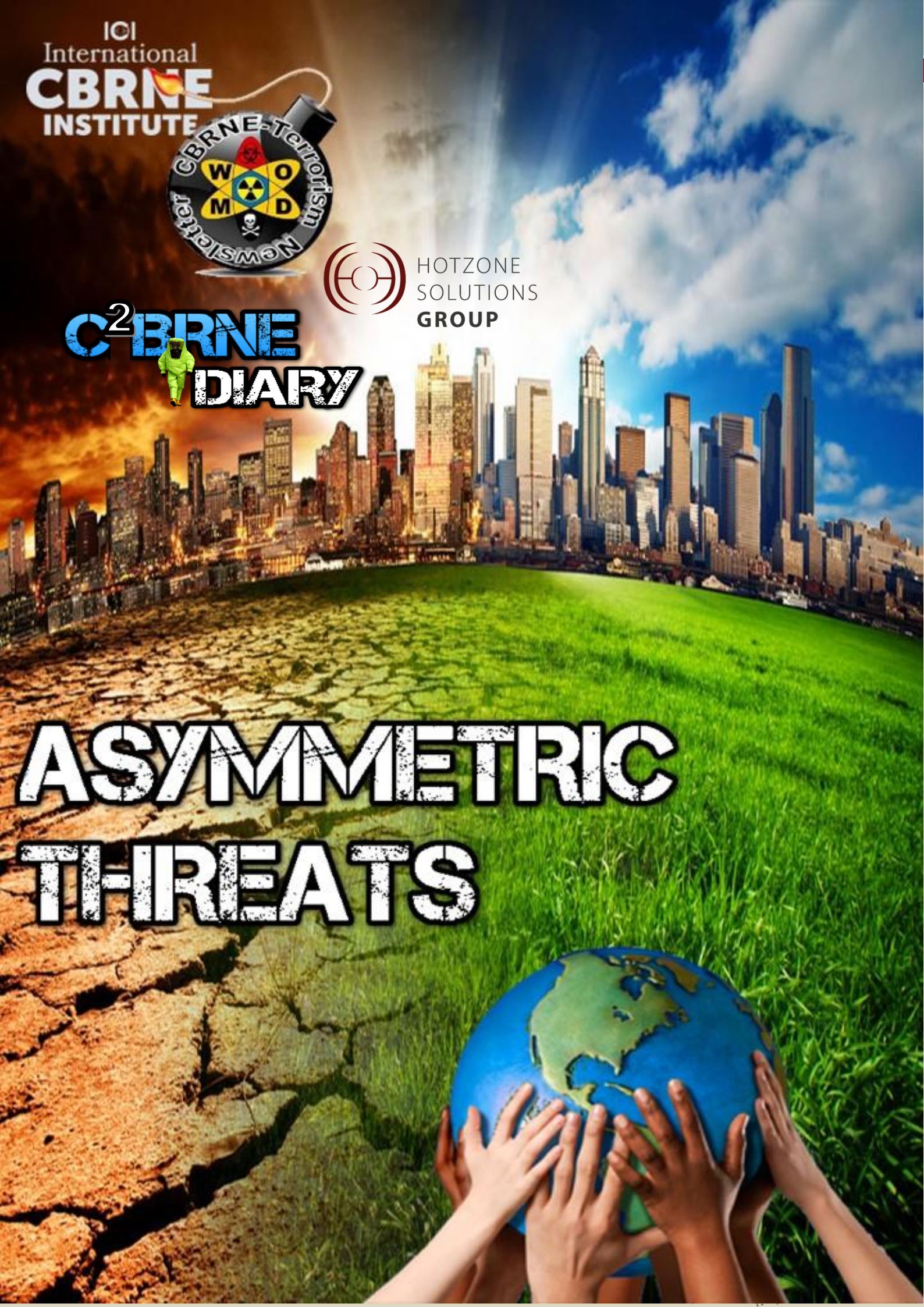
MOSAVE structural inspectors entered information as they assessed the buildings and structures in the field. That information was then used to update a dashboard at the emergency operations center, giving local authorities a clear picture of the tornado damage in a prompt and efficient way.

MOSAVE Chairman Ben Ross stated, "During the Cole County deployment, the app saved a lot of time updating leadership on our progress since people were able to look at the live dashboard for updates."

Like RVS, BSA was also developed with Esri technologies and includes data entry forms for field assessment teams and dashboards that provide real-time assessment results and situational awareness to emergency managers. For the Jefferson City tornado deployment, the app helped identify building safety issues, such as leaning structures, damage to building supports, or buildings off their foundation. According to MOSAVE team members, this was a significant time savings over

the standard paper process. Following the May 2019 tornado, MOSAVE provided feedback that validated the efficiency of using the BSA app to conduct safety assessments.
Not long after this tornado, the tool was further validated at FEMA's 2019 Shaken Fury exercise where it was one of several technology solutions demonstrated to enhance information sharing and situational awareness capabilities. Volunteers from the Tennessee Structural Assessment and Visual Evaluation Coalition simulated data collection and reporting to the Tennessee Emergency Operations Center, providing 51 reports during the exercise that tested the field app and populated a dashboard of results.

Taking the apps for a test drive
S&T notes that to try out the apps, bring them into your own ArcGIS organization, or just learn more about additional use cases, please visit CUSEC's RVS app and CUSEC's BSA app pages on the CUSEC Regional Information Sharing Platform.


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

Climate migration – How Many People Will Migrate Due to Rising Sea Levels? Our Best Guesses Aren't Good Enough

By Sonja Ayeb-Karlsson, Celia McMichael, Ilan Kelman, and Shouro Dasgupta

Source: http://www.homelandsecuritynewswire.com/dr20200926-how-many-people-will-migrate-due-to-rising-sea-levels-our-best-guesses-aren-t-good-enough

Sep 26 – An article in 2011 shocked many by suggesting that up to 187 million people could be forced to leave their homes as a result of two meters of sea level rise by 2100. Almost a decade on, some of the latest estimates suggest that as many as 630 million people may live on land below projected annual flood levels for the end of the century.

The idea that rising seas will force millions to move, unleashing a refugee crisis like no other, has now become commonplace. It's a narrative that the media are fond of, but that does not mean it is based on evidence.

The potential scale of sea level rise is becoming clearer, but this does not necessarily translate into population movements. Everything we have learned so far suggests that decisions to migrate are far more complex than a simple flight response.

In our new review article, we looked at 33 different studies that have estimated how sea level rise will affect migration patterns. Reliable estimates are important to help support vulnerable populations, but there is deep uncertainty around the amount of people who will be exposed to rising seas, and how they will respond.

Trapped Populations

We looked carefully at the methods and data sets of these studies to try and tease out uncertainties. One issue plaguing their estimates is assumptions about the number of people who will be living in vulnerable low-lying areas in the future.

Most of the studies we reviewed did note that the connections between migration and sea level rise are incredibly complex. Every person directly affected isn't guaranteed to move away as a result. People may be just as likely to try and protect their homes against the water, by building sea walls or elevating their houses.

It's impossible to predict how each person will respond, and there are countless reasons why someone might choose to stay in the place they call home rather than move or seek shelter elsewhere. Those who may be forced to migrate and resettle due to climate change receive far more attention than those left behind. These so-called "trapped" populations can be just as vulnerable as those on the move, if not more so.

Research suggests that the decision to stay or leave will have as much to do with emotional and social pressures as financial or practical reasons. People may feel afraid or find it unbearable to leave, while others lack the necessary support. Many may feel obliged to stay due to binding social ties and responsibilities.

How the health and wellbeing of those staying behind will be affected by rising seas is poorly investigated. More research is needed to understand the realities of staying put, for those who choose to stay and those who are unable to leave.

Where Do We Go from Here?

Research on sea level rise and migration has often tried to obtain global estimates of those likely to be affected. These are useful for drawing attention to the potential scale of future impacts, but they lack local insights that could help make the picture clearer for different areas.

Rising sea levels are just one of the many ways climate change is remaking our world. Understanding how sea level rise interacts with other environmental changes, such as increased temperatures and changing rainfall patterns will be important, but this stretches the ability to predict exact migration numbers.

Despite all the unknowns, we do know that coastal changes wrought by climate change will be significant, and they require action now. That means devising measures to prevent or reduce inundation, figuring out how to live with the water, and planning for successful ways to migrate and resettle. Evaluating options, developing scenarios, and making decisions around this must happen now, rather than waiting for the issue to become more urgent.

It is just as important to avoid repeating myths around climate change triggering vast flows of people from the so-called "Global South" seeking refuge in the so-called "Global North". We do know that people will not inevitably flee across borders in a warming world. Where migration does happen, movements within countries are often neglected on the likely flawed assumption that most migrants are crossing borders.

The narratives create unnecessary concern while shifting focus away from what really matters – helping vulnerable people. Not only do these myths reproduce xenophobic and outdated colonial power relations based on unfounded arguments, but they also create unnecessary fear and hostile environments for migrant populations around the world.

Sonja Ayeb-Karlsson *is Senior Researcher, Institute for Environment and Human Security (UNU-EHS), United Nations University.*
Celia McMichael *is Senior Lecturer in Geography, University of Melbourne.*
Ilan Kelman *is Professor of Disasters and Health, UCL.*
Shouro Dasgupta *is Lecturer in Environmental Economics, Università Ca'Foscari.*

HOTZONE SOLUTIONS GROUP

A holistic approach in CBRNe operations

Consultation
Products
Training

www.hotzonesolutions.org